SIEMENS

RUGGEDCOM ROX II v2.11

Benutzerhandbuch CLI

Für RX1400

Vorwort

Einleitung 1

Mit RUGGEDCOM ROX II arbeiten 2

Erste Schritte 3

Gerätemanagement 4

Systemverwaltung 5

Sicherheit 6

IP-Adresszuweisung 7

Layer 2 8

Serieller Server 9

Wireless 10

Tunnel und VPNs 11

Unicast- und Multicast-Routing 12

Netzwerkredundanz 13

Netzwerkerkennung und -management 14

Verkehrssteuerung und -klassifizierung 15

Fortsetzung auf der nächsten Seite

11/2017
RC1335-DE-01

SIEMENS

RUGGEDCOM ROX II v2.11

Benutzerhandbuch CLI

Für RX1400

11/2017
RC1335-DE-01

Fortsetzung

Uhrzeitdienste 16

Virtualisierung 17

Anwendungen 18

Fehlersuche 19

Copyright © 2018 Siemens Canada Ltd

Alle Rechte vorbehalten. Eine Verbreitung oder Vervielfältigung dieses Dokuments oder die Bewertung und Kommunikation seines Inhalts ist nicht zulässig, sofern nicht ausdrücklich erlaubt. Verstöße verpflichten zu Schadenersatz. Alle Rechte vorbehalten, insbesondere für den Fall der Patentanmeldung oder Markeneintragung.

Dieses Dokument enthält proprietäre Informationen, die urheberrechtlich geschützt sind. Alle Rechte vorbehalten. Kein Teil dieses Dokuments darf ohne vorherige schriftliche Zustimmung von Siemens Canada Ltd kopiert, vervielfältigt oder in eine andere Sprache übersetzt werden.

Haftungsausschluss

Siemens hat den Inhalt dieser Druckschrift auf Übereinstimmung mit der beschriebenen Hardware und Software geprüft. Dennoch können Abweichungen zwischen dem Produkt und der Dokumentation auftreten.

Siemens haftet nicht für Fehler oder hier enthaltene Auslassungen oder für Nebenschäden in Verbindung mit der Lieferung, Leistung oder Nutzung dieses Materials.

Die Angaben in diesem Dokument werden regelmäßig überprüft, notwendige Korrekturen sind in den nachfolgenden Auflagen enthalten. Für Verbesserungsvorschläge sind wir dankbar. Wir behalten uns das Recht vor, ohne vorherige Ankündigung technische Verbesserungen vorzunehmen.

Eingetragene Markenzeichen

RUGGEDCOM™ und ROS™ sind Markenzeichen von Siemens Canada Ltd.

Linux® ist ein eingetragenes Markenzeichen von Linus Torvalds in den Vereinigten Staaten und anderen Ländern.

Für das eingetragene Markenzeichen Linux® besteht eine Unterlizenz seitens LMI, dem ausschließlichen Lizenznehmer von Linus Torvalds, der das weltweite Eigentumsrecht an der Marke besitzt.

Die übrigen Bezeichnungen in diesem Handbuch sind möglicherweise Marken, deren Verwendung durch Dritte für deren Zwecke die Rechte der Inhaber verletzen kann.

Open Source

RUGGEDCOM ROX II basiert auf Linux®. Linux® wird unter den Bedingungen der GNU General Public License Version 2.0 [http://www.gnu.org/licenses/gpl-2.0.html] zur Verfügung gestellt.

RUGGEDCOM ROX II beinhaltet zusätzliche Open Source Software. Die Lizenzbedingungen finden Sie im relevanten Dokument *Lizenzbedingungen*.

Sicherheitshinweise

Siemens bietet Produkte und Lösungen mit Industrial-Security-Funktionen an, die den sicheren Betrieb von Anlagen, Maschinen, Geräten und/oder Netzwerken unterstützen. Sie sind wichtige Bausteine für ein ganzheitliches Industrial-Security-Konzept. Vor diesem Hintergrund werden die Produkte und Lösungen von Siemens einer fortlaufenden Weiterentwicklung unterzogen. Siemens empfiehlt Ihnen daher, dass Sie sich unbedingt regelmäßig über Produktaktualisierungen informieren.

Für den sicheren Betrieb von Produkten und Lösungen von Siemens ist es erforderlich, geeignete Schutzmaßnahmen (z. B. Zellenschutzkonzept) zu ergreifen und jede Komponente in ein ganzheitliches Industrial Security-Konzept zu integrieren, das dem aktuellen Stand der Technik entspricht. Dabei sind auch eingesetzte

Produkte von anderen Herstellern zu berücksichtigen. Weitergehende Informationen über Industrial Security finden Sie unter http://www.siemens.com/industrialsecurity.

Melden Sie sich für unseren produktspezifischen Newsletter an, damit Sie immer über Produktaktualisierungen informiert sind. Weitere Informationen hierzu finden Sie unter http://support.automation.siemens.com.

Gewährleistung

Die geltenden Garantiebedingungen sind in der Lizenzvereinbarung enthalten, sofern anwendbar.

Nähere Informationen zu den Garantiebestimmungen finden Sie unter https://www.siemens.com/ruggedcom oder kontaktieren Sie einen Mitarbeiter des Siemens Kundenservice.

Kontakt Siemens

Adresse
Siemens Canada Ltd
Industry Sector
300 Applewood Crescent
Concord, Ontario
Kanada L4K 5C7

Telefon
Gebührenfrei: + 1 888 264 0006
Tel: +1 905 856 5288
Fax: +1 905 856 1995

E-Mail
ruggedcom.info.i-ia@siemens.com

Internet
https://www.siemens.com/ruggedcom

Inhaltsverzeichnis

Vorwort xxxix
Konventionen xxxix
Zugehörige Dokumente xl
Systemvoraussetzungen xl
Zugriff auf Dokumentation xli
Lizenzbedingungen xli
Training xli
Kundensupport xlii

Kapitel 1
Einleitung 1
1.1 Produktmerkmale und Vorteile 1
1.2 Feature Keys 5
1.3 Sicherheitsempfehlungen 6
1.4 Am Port verfügbare Dienste 9
1.5 Benutzerberechtigungen 11
1.6 Entnehmbarer Speicher 14

Kapitel 2
Mit RUGGEDCOM ROX II arbeiten 15
2.1 Voreingestellte Benutzernamen und Passwörter 15
2.2 Anmelden 16
2.3 Abmelden 17
2.4 Mit den Netzwerkdienstprogrammen arbeiten 17
2.4.1 Senden von Ping-Anfragen an eine IPv4-Adresse oder einen Host 17
2.4.2 Eine IPv6-Adresse oder einen Host pingen 18
2.4.3 MPLS-Endpunkte pingen 18
2.4.4 VRF-Endpunkte pingen 18
2.4.5 Rückverfolgen einer Route zu einem IPv4-Host 19
2.4.6 Rückverfolgen einer Route zu einem IPv6-Host 19
2.4.7 Eine Route zu einem MPLS-Endpunkt verfolgen 20
2.4.8 Tracing einer Route zu einem VRF-Endpunkt 20
2.4.9 Erfassen von Paketen von einer Netzwerkschnittstelle 20
2.4.10 Erfassen von Paketen von einer VRF-Netzwerkschnittstelle 21
2.5 Mit der Befehlszeilenschnittstelle arbeiten 21

2.5.1 Auf die verschiedenen CLI-Modi zugreifen 22
2.5.2 Befehlszeilenergänzung verwenden 22
2.5.3 Verfügbare Befehle anzeigen 23
2.5.4 Bearbeiten von Befehlen 23
2.5.5 Verwendung doppelter Anführungszeichen 25
2.5.6 Ausgabeumleitung verwenden 25
2.5.7 Verwenden von regulären Ausdrücken 28
2.5.8 CLI-Dienstprogramme verwenden 29
2.5.9 Einen Bereich festlegen 30
2.5.10 Gängige Befehle 30
2.5.10.1 Grundlegende CLI-Befehle 30
2.5.10.2 Dateibefehle 32
2.5.10.3 Schnittstellen- und Dienstbefehle 34
2.5.10.4 Administrationsbefehle 35
2.5.10.5 Allgemeine Befehle für den Konfigurationsmodus 36
2.6 Konfigurieren der CLI-Schnittstelle 40
2.7 Auf die verschiedenen Modi zugreifen 41
2.7.1 Zugreifen auf den BIST-Modus 41
2.7.2 Zugreifen auf den Servicemodus 44
2.7.3 Auf den Wartungsmodus zugreifen 45

Kapitel 3
Erste Schritte 47
3.1 Verbindung mit RUGGEDCOM ROX II herstellen 47
3.1.1 Standard-IP-Adresse 47
3.1.2 Herstellen einer Direktverbindung 47
3.1.3 Herstellen einer entfernten Verbindung 48
3.2 Ein Basis-Netzwerk konfigurieren 49
3.2.1 Konfigurieren eines IPv4-Basis-Netzwerks 49
3.2.2 Konfigurieren eines IPv6-Basis-Netzwerks 50

Kapitel 4
Gerätemanagement 51
4.1 Geräte- und Softwareinformationen anzeigen 51
4.2 Die GPS-Position des Geräts bestimmen 52
4.3 Chassis-Informationen und -Status anzeigen 53
4.3.1 Anzeigen der Steckplatz-Hardware 53
4.3.2 Flash-Card-Speicherbelegung anzeigen 53
4.3.3 Anzeigen des Steckplatz-Status 54
4.3.4 Status des Steckplatzsensors anzeigen 55
4.4 Anzeigen der Teileliste 55

4.5 Das Gerät herunterfahren ... 56
4.6 Gerät neu booten ... 57
4.7 Auf Werkseinstellungen zurücksetzen ... 57
4.8 Außerbetriebnahme des Geräts ... 57
4.9 Anzeigen einer Liste der Line-Modul-Konfigurationen ... 58
4.10 Anzeigen von SFP-Informationen ... 59
4.11 Verwalten von Feature Keys ... 60
4.11.1 Inhalt eines Feature Key anzeigen ... 60
4.11.2 Installieren von Feature Keys ... 61
4.12 Dateien verwalten ... 62
4.12.1 Installieren von Dateien ... 62
4.12.2 Sichern von Dateien ... 63
4.13 Verwalten von Protokollen ... 64
4.13.1 Anzeigen von Protokollen ... 65
4.13.2 Protokolle löschen ... 66
4.13.3 Das sichere Remote Syslog konfigurieren ... 66
4.13.3.1 Aktivieren/Deaktivieren des sicheren Remote Syslog ... 66
4.13.3.2 Eine Liste der zulässigen Peers anzeigen ... 67
4.13.3.3 Einen erlaubten Peer hinzufügen ... 67
4.13.3.4 Einen erlaubten Peer löschen ... 68
4.13.3.5 Konfigurieren einer IP-Quelladresse für dezentrale Syslog-Meldungen ... 68
4.13.4 Diagnoseprotokolle verwalten ... 68
4.13.4.1 Das Entwicklerprotokoll aktivieren/deaktivieren ... 69
4.13.4.2 Das SNMP-Protokoll aktivieren/deaktivieren ... 70
4.13.4.3 Aktivieren/Deaktivieren des NETCONF-Summary-Protokolls ... 70
4.13.4.4 Aktivieren/Deaktivieren des NETCONF-Trace-Protokolls ... 71
4.13.4.5 Das XPATH-Trace-Protokoll aktivieren/deaktivieren ... 72
4.13.4.6 Das WebUI-Trace-Protokoll aktivieren/deaktivieren ... 72
4.13.5 Entfernte Syslog-Server verwalten ... 73
4.13.5.1 Eine Liste der entfernten Server anzeigen ... 73
4.13.5.2 Einen entfernten Server hinzufügen ... 74
4.13.5.3 Einen entfernten Server löschen ... 74
4.13.6 Selektoren für entfernte Server verwalten ... 75
4.13.6.1 Eine Liste der Selektoren für entfernte Server anzeigen ... 75
4.13.6.2 Einen Selektor zum Auswählen eines entfernten Servers hinzufügen ... 75
4.13.6.3 Einen Selektor zum Auswählen eines entfernten Servers löschen ... 76
4.14 Die Softwarekonfiguration verwalten ... 77
4.14.1 Die Konfiguration speichern ... 77
4.14.2 Eine Konfiguration laden ... 77
4.15 Ein Upgrade/Downgrade derRUGGEDCOM ROX II-Software ausführen ... 78

4.15.1 Die Quelle für Upgrades konfigurieren 78
4.15.2 Einrichten eines Upgrade-Servers 79
4.15.2.1 Konfigurieren des Upgrade-Servers 80
4.15.2.2 Ein Software-Release zum Upgrade-Server hinzufügen 80
4.15.2.3 Firmware-Releases im Upgrade-Server hinzufügen 81
4.15.3 Upgrade der Software RUGGEDCOM ROX II 81
4.15.4 Ein Software-Upgrade anhalten/ablehnen 83
4.15.5 Downgrade der RUGGEDCOM ROX II-Software durchführen 83
4.15.5.1 Ein Software-Upgrade rückgängig machen 83
4.15.5.2 Downgrade mittels ROXflash 84

Kapitel 5
Systemverwaltung 87
5.1 Systemname und Standort konfigurieren 87
5.2 Den Hostnamen konfigurieren 88
5.3 Benutzerspezifische Anpassung des Begrüßungsbildschirms 88
5.4 Die maximale Anzahl Sitzungen festlegen 88
5.5 Webschnittstellen-Sitzungen aktivieren und konfigurieren 89
5.6 Verwalten von Alarmen 90
5.6.1 Vorkonfigurierte Alarme 91
5.6.2 Eine Liste der aktiven Alarme anzeigen 91
5.6.3 Alarme löschen und quittieren 91
5.6.3.1 Alarme löschen 92
5.6.3.2 Alarme quittieren 92
5.6.4 Konfigurieren eines Alarms 93
5.7 Benutzer verwalten 94
5.7.1 Eine Liste der Benutzer anzeigen 94
5.7.2 Hinzufügen eines Benutzers 95
5.7.3 Einen Benutzer löschen 95
5.7.4 Benutzer überwachen 96
5.7.4.1 Benutzer aus dem Netzwerk abmelden 96
5.7.4.2 Meldungen an Benutzer senden 96
5.8 Verwalten von Passwörtern und Passphrasen 97
5.8.1 Komplexitätsregeln für Passwörter/Passphrasen konfigurieren 98
5.8.2 Ein Benutzer-Passwort/-Passphrase festlegen 99
5.8.3 Festlegen des Boot-Passworts bzw. der Boot-Passphrase 99
5.8.4 Festlegen des Wartungs-Passworts bzw. der Wartungs-Passphrase 100
5.8.5 Rücksetzen des Admin-Passworts bzw. der Admin-Passphrase 100
5.8.6 Boot-Passwort/-Passphrase zurücksetzen 102
5.8.7 Rücksetzen des Wartungs-Passworts bzw. der Wartungs-Passphrase 102
5.9 Aufträge planen 104

5.9.1 Eine Liste der geplanten Aufträge anzeigen 104
5.9.2 Einen geplanten Auftrag hinzufügen 104
5.9.3 Einen geplanten Auftrag löschen 106

Kapitel 6
Sicherheit 107
6.1 CLI-Sitzungen aktiveren und konfigurieren 107
6.2 SFTP-Sitzungen aktivieren und konfigurieren 108
6.3 Schutz vor Brute-Force-Angriffen aktivieren/deaktivieren 109
6.4 Port-Sicherheit verwalten 110
6.4.1 Port-Sicherheitskonzepte 111
6.4.1.1 Statische Authentifizierung anhand der MAC-Adresse 111
6.4.1.2 IEEE 802.1x-Authentifizierung 111
6.4.1.3 IEEE 802.1x-Authentifizierung mit Authentifizierung anhand der MAC-Adresse 112
6.4.1.4 Zuweisen von VLANs zu Tunnelattributen 113
6.4.2 Konfigurieren der Port-Sicherheit 113
6.4.3 Anzeigen des Sicherheitszustands von Switched-Ethernet-Ports 115
6.5 Benutzerauthentifizierungen verwalten 115
6.5.1 Einstellen des Benutzer-Authentifizierungsmodus 116
6.5.2 Benutzer-Authentifizierungsschlüssel verwalten 116
6.5.2.1 Die einem Benutzer zugewiesenen Schlüssel bestimmen 117
6.5.2.2 Hinzufügen eines Benutzer-Authentifizierungsschlüssels 117
6.5.2.3 Einen Benutzerauthentifizierungsschlüssel löschen 118
6.5.2.4 Zuweisen/Trennen eines Benutzer-Authentifizierungsschlüssels 118
6.5.3 Verwalten der RADIUS-Authentifizierung 119
6.5.3.1 Konfigurieren einer RADIUS-Authentifizierung für LOGIN-Services 121
6.5.3.2 Eine RADIUS-Authentifizierung für PPP-Services konfigurieren 122
6.5.3.3 Eine RADIUS-Authentifizierung für Switched-Ethernet-Ports konfigurieren 122
6.5.4 Konfigurieren der TACACS+-Authentifizierung 123
6.6 Zertifikate und Schlüssel verwalten 124
6.6.1 Den öffentlichen SSH/RSA-Schlüssel des lokalen Hosts anzeigen 125
6.6.2 Den Speicher für vertrauenswürdige Zertifikate verwalten 125
6.6.2.1 Den Speicher für vertrauenswürdige Zertifikate konfigurieren 126
6.6.2.2 Den Speicher für vertrauenswürdige Zertifikate aktivieren/deaktivieren 126
6.6.2.3 Liste der Stammzertifikate im Speicher der vertrauenswürdigen Zertifikate 127
6.6.3 Zertifikate von Zertifizierungsstellen (CA) im Speicher für vertrauenswürdige Zertifikate verwalten 153
6.6.3.1 Eine Liste der Zertifikate einer Zertifizierungsstelle (CA) im Speicher für vertrauenswürdige Zertifikate anzeigen 153
6.6.3.2 Ein Zertifikat von einer Zertifizierungsstelle zum Speicher für vertrauenswürdige Zertifikate hinzufügen 153

6.6.3.3 Ein Zertifikat einer Zertifizierungsstelle (CA) im Speicher für vertrauenswürdige Zertifikate löschen 154
6.6.4 Zertifikate von Zertifizierungsstellen (CA) und CRLs verwalten 154
6.6.4.1 Eine Liste der Zertifikate von Zertifizierungsstellen und CRLs anzeigen 154
6.6.4.2 Anzeigen des Status eines CA-Zertifikats und einer CRL 155
6.6.4.3 Hinzufügen eines CA-Zertifikats und der CRL 156
6.6.4.4 Ein CA-Zertifikat und eine CRL löschen 157
6.6.5 Private Schlüssel verwalten 157
6.6.5.1 Eine Liste der privaten Schlüssel anzeigen 157
6.6.5.2 Einen privaten Schlüssel hinzufügen 158
6.6.5.3 Einen privaten Schlüssel löschen 158
6.6.6 Öffentliche Schlüssel verwalten 159
6.6.6.1 Eine Liste der öffentlichen Schlüssel anzeigen 159
6.6.6.2 Hinzufügen eines öffentlichen Schlüssels 159
6.6.6.3 Hinzufügen eines IPSec-formatierten öffentlichen Schlüssels 160
6.6.6.4 Einen öffentlichen Schlüssel löschen 161
6.6.7 Zertifikate verwalten 161
6.6.7.1 Eine Liste der Zertifikate anzeigen 162
6.6.7.2 Den Status eines Zertifikats anzeigen 162
6.6.7.3 Hinzufügen eines Zertifikats 163
6.6.7.4 Ein Zertifikat löschen 163
6.7 Verwalten von Firewalls 164
6.7.1 Firewall-Konzepte 165
6.7.1.1 Zustandslose vs. zustandsorientierte Firewalls 165
6.7.1.2 Linux netfilter 165
6.7.1.3 Netzadressenübersetzung 166
6.7.1.4 Weiterleitung von Ports 166
6.7.1.5 Schutz gegen einen SYN-Flood-Angriff 167
6.7.1.6 Schutz gegen IP Spoofing 167
6.7.2 Eine Liste der Firewalls anzeigen 167
6.7.3 Hinzufügen einer Firewall 168
6.7.4 Eine Firewall löschen 169
6.7.5 Betrieb mit mehreren Firewallkonfigurationen 169
6.7.6 Konfigurieren der Firewall für ein VPN 170
6.7.7 Die Firewall für ein VPN in einer entmilitarisierten Zone (DMZ) konfigurieren 171
6.7.8 Zonen verwalten 172
6.7.8.1 Eine Liste der Zonen anzeigen 172
6.7.8.2 Eine Zone hinzufügen 173
6.7.8.3 Eine Zone löschen 173
6.7.9 Schnittstellen verwalten 174
6.7.9.1 Eine Liste der Schnittstellen anzeigen 174

6.7.9.2 Hinzufügen einer Schnittstelle 175
6.7.9.3 Eine Schnittstelle zu einer Zone zuweisen 176
6.7.9.4 Eine Broadcast-Adresse konfigurieren 176
6.7.9.5 Eine Schnittstelle löschen 177
6.7.10 Hosts verwalten 177
6.7.10.1 Eine Liste der Hosts anzeigen 178
6.7.10.2 Hinzufügen eines Hosts 178
6.7.10.3 Einen Host löschen 179
6.7.11 Verwalten von Grundregeln 179
6.7.11.1 Eine Liste der Grundregeln anzeigen 180
6.7.11.2 Eine Regel hinzufügen 181
6.7.11.3 Die Quellzone konfigurieren 181
6.7.11.4 Die Zielzone konfigurieren 182
6.7.11.5 Eine Regel löschen 182
6.7.12 NAT-Einstellungen verwalten 182
6.7.12.1 Eine Liste der NAT-Einstellungen anzeigen 183
6.7.12.2 Hinzufügen einer NAT-Einstellung 183
6.7.12.3 Eine NAT-Einstellung löschen 184
6.7.13 Maskierungs- oder SNAT-Einstellungen verwalten 184
6.7.13.1 Eine Liste der Maskierungs- oder SNAT-Einstellungen anzeigen 185
6.7.13.2 Hinzufügen von Maskierungs- oder SNAT-Einstellungen 185
6.7.13.3 Eine Maskierungs- oder SNAT-Einstellung löschen 186
6.7.14 Regeln verwalten 187
6.7.14.1 Eine Liste der Regeln anzeigen 187
6.7.14.2 Eine Regel hinzufügen 188
6.7.14.3 Die Quellzone konfigurieren 189
6.7.14.4 Die Zielzone konfigurieren 189
6.7.14.5 Eine Regel löschen 190
6.7.15 Eine Firewall-Konfiguration überprüfen 190
6.7.16 Eine Firewall aktivieren/deaktivieren 190

Kapitel 7
IP-Adresszuweisung 193
7.1 IP-Adressen für routingfähige Schnittstellen verwalten 193
7.1.1 Kalkulation für routingfähige Schnittstellen konfigurieren 193
7.1.2 Statistiken für routingfähige Schnittstellen anzeigen 194
7.1.3 IPv4-Adressen verwalten 195
7.1.3.1 Eine Liste der IPv4-Adressen anzeigen 195
7.1.3.2 Eine IPv4-Adresse hinzufügen 196
7.1.3.3 Eine IPv4-Adresse löschen 196
7.1.4 IPv6-Adressen verwalten 197

7.1.4.1 Eine Liste der IPv6-Adressen anzeigen 197
7.1.4.2 Eine IPv6-Adresse hinzufügen 197
7.1.4.3 Eine IPv6-Adresse löschen 198
7.1.5 Konfigurieren der IPv6 Neighbor Discovery 198
7.1.6 IPv6-Netzwerkpräfixe verwalten 200
7.1.6.1 Hinzufügen eines IPv6-Netzwerkpräfixes 200
7.1.6.2 Ein Ipv6-Netzwerkpräfix löschen 201
7.2 Verwalten des DHCP Relay Agent (IPv4) 202
7.2.1 Den DHCP Relay Agent (IPv4) konfigurieren 203
7.2.2 Eine Liste der DHCP-Client-Ports (IPv4) anzeigen 203
7.2.3 Einen DHCP-Client-Port (IPv4) hinzufügen 203
7.2.4 Einen DHCP-Client-Port (IPv4) löschen 204
7.3 Den DHCP-Server verwalten 204
7.3.1 Eine Liste der aktiven Leases anzeigen 205
7.3.2 Den DHCP-Server konfigurieren 206
7.3.3 Den DHCP-Server aktivieren/deaktivieren 206
7.3.4 Konfigurieren von Optionen für den DHCP-Server 206
7.3.5 DHCP-Client-Konfigurationsoptionen verwalten 208
7.3.5.1 Konfigurieren von Standard-Konfigurationsoptionen (IPv4) für DHCP-Clients 208
7.3.5.2 Konfigurieren von Standard-Konfigurationsoptionen (IPv6) für DHCP-Clients 209
7.3.5.3 Anzeigen einer Liste der kundenspezifischen Konfigurationsoptionen für DHCP-Clients 210
7.3.5.4 Hinzufügen einer kundenspezifischen Konfigurationsoption für DHCP-Clients 210
7.3.5.5 Löschen einer kundenspezifischen Konfigurationsoption für DHCP-Clients 211
7.3.6 Hörende DHCP-Schnittstellen verwalten 212
7.3.6.1 Eine Liste der hörenden DHCP-Schnittstellen anzeigen 212
7.3.6.2 Eine hörende DHCP-Schnittstelle hinzufügen 213
7.3.6.3 Eine hörende DHCP-Schnittstelle löschen 213
7.3.7 Gemeinsame Netzwerke verwalten 214
7.3.7.1 Eine Liste gemeinsamer Netzwerke anzeigen 214
7.3.7.2 Ein gemeinsames Netzwerk hinzufügen 215
7.3.7.3 Optionen für gemeinsame Netzwerke konfigurieren 215
7.3.7.4 Ein gemeinsames Netzwerk löschen 216
7.3.8 Subnetze verwalten 217
7.3.8.1 Eine Liste der Subnetze anzeigen 217
7.3.8.2 Hinzufügen eines Subnetzes 217
7.3.8.3 Optionen für Subnetze konfigurieren 218
7.3.8.4 Ein Subnetz löschen 220
7.3.9 Host-Gruppen verwalten 221
7.3.9.1 Eine Liste der Host-Gruppen anzeigen 221
7.3.9.2 Eine Hostgruppe hinzufügen 221

7.3.9.3 Konfigurieren von Optionen für eine Hostgruppe 222
7.3.9.4 Eine Hostgruppe löschen 223
7.3.10 DHCP-Hosts verwalten 224
7.3.10.1 Eine Liste der Hosts anzeigen 224
7.3.10.2 Einen Host hinzufügen 225
7.3.10.3 Konfigurieren von Optionen für einen Host 225
7.3.10.4 Hosts löschen 227
7.3.11 Adressen-Pools (IPv4) verwalten 227
7.3.11.1 Eine Liste der Adress-Pools (IPv4) anzeigen 227
7.3.11.2 Hinzufügen eines Adress-Pools (IPv4) 228
7.3.11.3 Einen Adress-Pool (IPv4) löschen 229
7.3.12 Adressen-Pools (IPv6) verwalten 229
7.3.12.1 Eine Liste der Adress-Pools (IPv6) anzeigen 230
7.3.12.2 Hinzufügen eines Adress-Pools (IPv6) 230
7.3.12.3 Einen Adress-Pool (IPv6) löschen 231
7.3.13 IP-Bereiche verwalten (IPv4) 231
7.3.13.1 Eine Liste der IP-Bereiche (IPv4) anzeigen 232
7.3.13.2 Hinzufügen eines IP-Bereichs (IPv4) 232
7.3.13.3 Löschen eines IP-Bereichs (IPv4) 233
7.3.14 IP-Bereiche verwalten (IPv6) 233
7.3.14.1 Eine Liste der IP-Bereiche (IPv6) anzeigen 234
7.3.14.2 Hinzufügen eines IP-Bereichs (IPv6) 234
7.3.14.3 Löschen eines IP-Bereichs (IPv6) 235
7.3.15 IPv6-Präfixe verwalten 235
7.3.15.1 Eine Liste der IPv6-Präfixe anzeigen 235
7.3.15.2 Ein IPv6-Präfix hinzufügen 236
7.3.15.3 Ein IPv6-Präfix löschen 237
7.3.16 Temporäre Subnetze verwalten 237
7.3.16.1 Eine Liste temporärer Subnetze anzeigen 237
7.3.16.2 Ein temporäres Subnetz hinzufügen 238
7.3.16.3 Ein temporäres Subnetz löschen 238
7.3.17 IPv6-Subnetze verwalten 239
7.3.17.1 Eine Liste der IPv6-Subnetze anzeigen 239
7.3.17.2 Ein IPv6-Subnetz hinzufügen 239
7.3.17.3 Ein IPv6-Subnetz löschen 240
7.3.18 Option 82-Klassen für Adress-Pools (IPv4) verwalten 240
7.3.18.1 Eine Liste von Option 82-Klassen für Adress-Pools (IPv4) anzeigen 241
7.3.18.2 Hinzufügen einer Option 82-Klasse zu einem Adress-Pool (IPv4) 241
7.3.18.3 Eine Option 82-Klasse aus einem Adress-Pool (IPv4) löschen 242
7.4 Statische DNS verwalten 242

7.4.1 Domainnamen verwalten 243
7.4.1.1 Eine Liste der Domain-Namen anzeigen 243
7.4.1.2 Einen Domain-Namen hinzufügen 243
7.4.1.3 Einen Domain-Namen löschen 244
7.4.2 Domain-Name-Server verwalten 244
7.4.2.1 Eine Liste der Domain-Name-Server anzeigen 244
7.4.2.2 Einen Domain-Name-Server hinzufügen 245
7.4.2.3 Einen Domain-Name-Server löschen 245
7.5 Dynamic DNS (DDNS) verwalten 245
7.5.1 Aktivieren und Konfigurieren von Dynamic DNS 246
7.5.2 Dynamische DNS-Server verwalten 247
7.5.2.1 Eine Liste der dynamischen DNS-Server anzeigen 247
7.5.2.2 Den Status eines DDNS-Servers anzeigen 247
7.5.2.3 Einen DDNS-Server hinzufügen 248
7.5.2.4 Einen dynamischen DNS-Server löschen 248
7.5.3 Hostnamen für dynamische DNS-Server verwalten 249
7.5.3.1 Eine Liste der Host-Namen anzeigen 249
7.5.3.2 Einen Hostnamen hinzufügen 249
7.5.3.3 Einen Hostnamen löschen 250

Kapitel 8
Layer 2 251
8.1 Switched-Ethernet-Ports verwalten 251
8.1.1 Eine Liste der Switched-Ethernet-Ports anzeigen 251
8.1.2 Einen Switched-Ethernet-Port konfigurieren 252
8.1.3 Statistiken der Switched-Ethernet-Ports anzeigen 258
8.1.4 Anzeigen der RMON-Portstatistik 259
8.1.5 Switched-Ethernet-Port-Statistiken löschen 262
8.1.6 Einen Switched-Ethernet-Port zurücksetzen 262
8.1.7 Kabel für Switched-Ethernet-Ports testen 263
8.1.7.1 Ausführen eines Kabeldiagnosetests 263
8.1.7.2 Anzeigen der Kabeldiagnosestatistik 264
8.1.7.3 Löschen der Kabeldiagnosestatistik 265
8.2 Ethernet-Trunk-Schnittstellen verwalten 265
8.2.1 Eine Liste der Ethernet-Trunk-Schnittstellen anzeigen 266
8.2.2 Hinzufügen einer Ethernet-Trunk-Schnittstelle 266
8.2.3 Eine Ethernet-Trunk-Schnittstelle löschen 268
8.2.4 Ethernet-Trunk-Ports verwalten 268
8.2.4.1 Eine Liste der Ethernet-Trunk-Ports anzeigen 269
8.2.4.2 Einen Ethernet-Trunk-Port hinzufügen 269
8.2.4.3 Einen Ethernet-Trunk-Port löschen 269

8.3 MAC-Adressen verwalten 270
8.3.1 Anzeigen der dynamischen Liste der MAC-Adressen 270
8.3.2 Die dynamische MAC-Adressliste leeren 271
8.3.3 Optionen für das MAC-Adressenlernen konfigurieren 271
8.3.4 Statische MAC-Adressen verwalten 272
8.3.4.1 Eine Liste der statischen MAC-Adressen anzeigen 272
8.3.4.2 Hinzufügen einer statischen MAC-Adresse 273
8.3.4.3 Eine statische MAC-Adresse löschen 273
8.4 Multicast-Filterung verwalten 274
8.4.1 Multicast-Filterkonzepte 274
8.4.1.1 IGMP 274
8.4.1.2 GMRP (GARP Multicast Registration Protocol) 278
8.4.2 GMRP aktivieren und konfigurieren 281
8.4.3 IGMP Snooping verwalten 281
8.4.3.1 IGMP Snooping konfigurieren 282
8.4.3.2 Eine Liste der Router-Ports anzeigen 282
8.4.3.3 Einen Router-Port hinzufügen 283
8.4.3.4 Einen Router-Port löschen 283
8.4.4 Die statische Multicast-Gruppen-Tabelle verwalten 283
8.4.4.1 Eine Liste statischer Multicast-Gruppeneinträge anzeigen 284
8.4.4.2 Einen Eintrag für eine statische Multicast-Gruppe hinzufügen 284
8.4.4.3 Einen Eintrag für eine statische Multicast-Gruppe löschen 284
8.4.5 Ausgehende (egress) Ports für Multicast-Gruppen verwalten 285
8.4.5.1 Eine Liste der ausgehenden (egress) Ports anzeigen 285
8.4.5.2 Hinzufügen eines ausgehenden (egress) Ports 286
8.4.5.3 Löschen eines ausgehenden (egress) Ports 286
8.4.6 Ein Übersicht der Multicast-Gruppen anzeigen 286
8.4.7 Eine Liste der IP-Multicast-Gruppen anzeigen 287
8.5 VLANs verwalten 288
8.5.1 VLAN-Konzepte 288
8.5.1.1 Getaggte und ungetaggte Frames 289
8.5.1.2 Natives VLAN 289
8.5.1.3 Edge- und Trunk-Porttypen 289
8.5.1.4 Eingangsfilterung 290
8.5.1.5 Liste verbotener Ports 290
8.5.1.6 VLAN-fähige Betriebsart 290
8.5.1.7 GARP VLAN Registration-Protokoll (GVRP) 291
8.5.1.8 PVLAN Edge 293
8.5.1.9 Vorteile von VLANs 293
8.5.2 Konfigurieren des internen VLAN-Bereichs 295

8.5.3 Eingangsfilterung aktivieren/deaktivieren ... 296
8.5.4 VLANs für Switched-Ethernet-Ports verwalten ... 297
8.5.4.1 VLAN-Zuweisungen für Switched-Ethernet-Ports anzeigen ... 297
8.5.4.2 VLANs für Switched-Ethernet-Ports konfigurieren ... 298
8.5.5 Statische VLANs verwalten ... 298
8.5.5.1 Eine Liste der statischen VLANs anzeigen ... 299
8.5.5.2 Hinzufügen eines statischen VLAN ... 299
8.5.5.3 Ein statisches VLAN löschen ... 300
8.5.6 Verbotene Ports verwalten ... 300
8.5.6.1 Eine Liste der verbotenen Ports ... 300
8.5.6.2 Einen verbotenen Port hinzufügen ... 301
8.5.6.3 Einen verbotenen Port löschen ... 301
8.5.7 VLANs für Schnittstellen und Tunnel verwalten ... 301
8.6 Spanning Tree Protocol (STP) verwalten ... 302
8.6.1 RSTP-Betrieb ... 302
8.6.1.1 RSTP-Zustände und -Funktionen ... 303
8.6.1.2 Edge-Ports ... 304
8.6.1.3 Punkt-zu-Punkt- und Mehrfachpunktverbindung ... 305
8.6.1.4 Pfad- und Portkosten ... 305
8.6.1.5 Bridge-Durchmesser ... 306
8.6.1.6 eRSTP ... 306
8.6.1.7 Fast Root Failover ... 307
8.6.2 RSTP-Anwendungen ... 308
8.6.2.1 RSTP in Konfigurationen mit strukturierter Verdrahtung ... 308
8.6.2.2 RSTP in Ring-Backbone-Konfigurationen ... 309
8.6.2.3 RSTP-Port-Redundanz ... 311
8.6.3 MSTP-Betrieb ... 311
8.6.3.1 MSTP-Regionen und -Interoperabilität ... 312
8.6.3.2 MSTP-Bridge- und -Port-Funktionen ... 313
8.6.3.3 Vorteile von MSTP ... 314
8.6.3.4 MSTP an einem überbrückten Netzwerk implementieren ... 315
8.6.4 Konfigurieren des STP (global) ... 316
8.6.5 Konfigurieren des STP für Switched-Ethernet-Ports und Ethernet-Trunk-Schnittstellen ... 318
8.6.6 MST-Instanzen global verwalten ... 320
8.6.6.1 Anzeigen der Statistik von Multiple Spanning Tree-Instanzen ... 320
8.6.6.2 Eine Liste der MST-Instanzen anzeigen ... 321
8.6.6.3 Hinzufügen einer Multiple Spanning Tree-Instanz ... 322
8.6.6.4 Eine MSTI (Multiple Spannung Tree Instance) löschen ... 323
8.6.7 MST-Instanzen nach Ports verwalten ... 323
8.6.7.1 Statistiken für MST-Instanzen je Port anzeigen ... 323

8.6.7.2 Anzeigen einer Liste der Multiple Spanning Tree-Instanzen (MSTI) pro Port 325
8.6.7.3 Hinzufügen einer portspezifischen Multiple Spanning Tree-Instanz 326
8.6.7.4 Löschen von portspezifischen Multiple Spanning Tree-Instanzen 327
8.6.8 Anzeigen des Status eines RSTP 328
8.6.9 RSTP-Statistiken je Port anzeigen 330
8.6.10 Statistiken für STP (Spanning Tree Protocol) löschen 332

Kapitel 9
Serieller Server 333
9.1 Serielle Ports verwalten 333
9.1.1 Eine Liste der seriellen Ports anzeigen 333
9.1.2 Anzeigen der Statistik für serielle Ports 334
9.1.3 Anzeigen der Statistik der Transportverbindungen 335
9.1.4 Statiken für DNP-Gerätetabellen anzeigen 336
9.1.5 Statistiken für serielle Ports löschen 336
9.1.6 Einen seriellen Port konfigurieren 337
9.1.7 Den seriellen Server neu starten 338
9.1.8 Einen seriellen Port zurücksetzen 338
9.2 Serielle Port-Protokolle verwalten 338
9.2.1 Konzepte serieller Port-Protokolle 339
9.2.1.1 Raw-Socket-Anwendungen 339
9.2.1.2 Modbus TCP-Anwendungen 340
9.2.1.3 DNP-Anwendungen 341
9.2.1.4 Ein-/ausgehende serielle Verbindungen 342
9.2.2 Eine Liste der Protokolle für serielle Ports anzeigen 342
9.2.3 Hinzufügen eines Protokolls des seriellen Ports 342
9.2.4 DNP-Protokoll konfigurieren 343
9.2.5 Das Modbus TCP-Protokoll konfigurieren 343
9.2.6 Konfigurieren des Raw-Socket-Protokolls 344
9.2.7 Ein Protokoll des seriellen Ports löschen 346
9.3 Geräteadressentabellen verwalten 346
9.3.1 Eine Liste der Tabellen mit Geräteadressen anzeigen 346
9.3.2 Hinzufügen einer Tabelle mit Geräteadressen 347
9.3.3 Löschen einer Tabelle mit Geräteadressen 347
9.4 Serielles Multicast-Streaming verwalten 348
9.4.1 Serielles Multicast-Streaming verstehen 348
9.4.1.1 Zielports (Sink) und Quellports (Source) 348
9.4.1.2 Beispiele für das Multicast-Streaming 349
9.4.2 Serielles Multicast-Streaming konfigurieren 349
9.4.3 Beispiel: Serielle Schnittstellen, die als "Sink"-Gerät für Multicast-Streams konfiguriert sind 350
9.4.4 Beispiel: Für Multicast-Streams als stromliefernd konfigurierte serielle Schnittstellen 352

9.4.5 Beispiel: Für Multicast-Streams als stromliefernd und stromziehend konfigurierte serielle Schnittstellen 355
9.5 Entfernte Hosts verwalten 358
9.5.1 Eine Liste der entfernten Hosts anzeigen 358
9.5.2 Hinzufügen eines entfernten Hosts 358
9.5.3 Einen entfernten Host löschen 359
9.6 Lokale Hosts verwalten 360
9.6.1 Eine Liste der lokalen Hosts anzeigen 360
9.6.2 Hinzufügen eines lokalen Hosts 360
9.6.3 Eine lokalen Host löschen 361
9.7 Entfernte Host-Schnittstellen verwalten 362
9.7.1 Anzeigen einer Liste der dezentralen Host-Schnittstellen 362
9.7.2 Hinzufügen einer Schnittstelle des entfernten Hosts 362
9.7.3 Eine Schnittstelle des entferntem Hosts löschen 363
9.8 Lokale Host-Schnittstellen verwalten 363
9.8.1 Anzeigen einer Liste der lokalen Host-Schnittstellen 364
9.8.2 Hinzufügen einer lokalen Host-Schnittstelle 364
9.8.3 Eine lokale Host-Schnittstelle löschen 365

Kapitel 10
Wireless 367
10.1 Die WLAN-Schnittstelle verwalten 367
10.1.1 Aktivieren und Konfigurieren der WLAN-Schnittstelle 367
10.1.2 WAP (Wireless Access Points) verwalten 369
10.1.2.1 Eine Liste der Wireless Access Points (WAP) anzeigen 369
10.1.2.2 Den Status der drahtlosen Zugangspunkte anzeigen 370
10.1.2.3 Status der WLAN-Client-Zuordnungen anzeigen 371
10.1.2.4 Hinzufügen eines Wireless Access Point 371
10.1.2.5 Einen WAP (Wireless Access Point) löschen 373
10.1.3 WLAN-Clients verwalten 373
10.1.3.1 Eine Liste der WLAN-Clients anzeigen 373
10.1.3.2 Status der WLAN-Clients anzeigen 374
10.1.3.3 Hinzufügen eines WLAN-Clients 374
10.1.3.4 Einen WLAN-Client löschen 375
10.1.3.5 Suchen nach WLAN-Clients 376
10.1.4 Beispiel: Konfigurieren eines WLAN mit einer Firewall 376
10.2 Mobilfunkmodem-Schnittstellen verwalten 379
10.2.1 Dual-SIM-Karten aktivieren 379
10.2.2 Eine Liste der Mobilfunkmodem-Schnittstellen anzeigen 380
10.2.3 Anzeigen des Status einer Mobilfunkmodem-Schnittstelle 380
10.2.4 Statistiken zu PPP-Schnittstellen anzeigen 381

10.2.5 Eine Mobilfunkmodem-Schnittstelle konfigurieren 382
10.3 AT-Befehle ausführen 382
10.4 Herstellen einer Verbindung als PPP-Client 382
10.5 Mobilfunkmodem-Profile verwalten 383
10.5.1 Eine Liste der GSM-Profile anzeigen 383
10.5.2 Hinzufügen eines GSM-Profils 384
10.5.3 Ein GSM-Profil löschen 385
10.6 Das LTE-Modem verwalten 386
10.6.1 Aktivieren/Deaktivieren des LTE-Modems 386
10.6.2 LTE-Modem konfigurieren 387
10.6.3 Das Mobilfunkmodem zurücksetzen 387
10.6.4 Aktivieren/Deaktivieren von GPS 387
10.6.5 NMEA-GPS-Datenströme aktivieren und konfigurieren 388
10.6.6 Ändern der aktiven SIM-Karte 389
10.6.7 Firmware-Updates verwalten 389
10.6.7.1 Den Firmware-Update-Status anzeigen 390
10.6.7.2 Konfigurieren des Firmware-Update-Modus und der -Quelle 390
10.6.7.3 Firmware-Update durchführen 391

Kapitel 11
Tunnel und VPNs 393
11.1 Verwalten von virtuellen Switches 393
11.1.1 Eine Liste virtueller Switches anzeigen 394
11.1.2 Hinzufügen eines virtuellen Switch 395
11.1.3 Einen virtuellen Switch löschen 396
11.1.4 Schnittstellen für virtuelle Switches verwalten 396
11.1.4.1 Eine Liste von Schnittstellen für virtuelle Switches anzeigen 396
11.1.4.2 Hinzufügen einer Schnittstelle des virtuellen Switch 397
11.1.4.3 Eine Schnittstelle des virtuellen Switch löschen 398
11.1.5 Verkehr über einen virtuellen Switch filtern 398
11.1.5.1 Aktivieren/Deaktivieren der Filterung für virtuelle Switches 398
11.1.5.2 Eine Liste von Filtern für virtuelle Switches anzeigen 399
11.1.5.3 Hinzufügen eines Filters für den virtuellen Switch 399
11.1.5.4 Einen Filter des virtuellen Switch löschen 400
11.1.6 Filterregeln verwalten 400
11.1.6.1 Eine Liste der Regeln anzeigen 400
11.1.6.2 Eine Liste von Regeln zum Filter des virtuellen Switch anzeigen 401
11.1.6.3 Eine Regel hinzufügen 401
11.1.6.4 Eine Regel zum Filter des virtuellen Switch hinzufügen 402
11.1.6.5 Eine Regel löschen 403
11.1.6.6 Eine Regel aus einem Filter des virtuellen Switches löschen 403

11.1.7 In/Out-Schnittstellen verwalten 403
11.1.7.1 Eine Liste der IN/OUT-Interfaces anzeigen 404
11.1.7.2 Ein IN/OUT-Interface hinzufügen 404
11.1.7.3 Ein IN/OUT-Interface löschen 405
11.1.8 VLANs für virtuelle Switches verwalten 405
11.1.8.1 Eine Liste von VLANs für virtuelle Switches anzeigen 405
11.1.8.2 Ein VLAN auf Basis eines virtuellen Switch hinzufügen 406
11.1.8.3 Ein VLAN auf Basis von virtuellen Switches löschen 406
11.2 Den Layer-2-Tunnel-Daemon verwalten 407
11.2.1 RTT-Statistiken anzeigen 407
11.2.2 Konfigurieren des Layer-2-Tunnel-Daemon 408
11.3 L2TP-Tunnel verwalten 409
11.3.1 Konfigurieren von L2TP-Tunneln 409
11.3.2 DNS-Server konfigurieren 410
11.3.3 PPP-Optionen konfigurieren 410
11.3.4 WINS-Server konfigurieren 411
11.4 L2TPv3-Tunnel verwalten 411
11.4.1 L2TPv3-Tunnelszenarien 412
11.4.2 Einen L2TPv3-Tunnel erstellen 413
11.4.3 Statische L2TPv3-Tunnel verwalten 414
11.4.3.1 Statische L2TPv3-Tunnel aktivieren/deaktivieren 414
11.4.3.2 Eine Liste der statischen L2TPv3-Tunnel anzeigen 414
11.4.3.3 Hinzufügen eines statischen L2TPv3-Tunnels 415
11.4.3.4 Einen statischen L2TPv3-Tunnel löschen 416
11.4.4 Dynamische L2TPv3-Tunnel verwalten 416
11.4.4.1 Dynamische L2TPv3-Tunnel aktivieren und konfigurieren 417
11.4.4.2 Eine Liste der dynamischen L2TPv3-Tunnel anzeigen 417
11.4.4.3 Hinzufügen eines dynamischen L2TPv3-Tunnels 418
11.4.4.4 Einen dynamischen L2TPv3-Tunnel löschen 420
11.4.5 Sitzungen für L2TPv3-Tunnel verwalten 420
11.4.5.1 Eine Liste der Sitzungen anzeigen 420
11.4.5.2 Hinzufügen einer Sitzung 421
11.4.5.3 Eine Sitzung löschen 422
11.4.6 VLANs für L2TPv3-Tunnel verwalten 423
11.4.6.1 Eine Liste der VLANs anzeigen 423
11.4.6.2 Ein VLAN hinzufügen 423
11.4.6.3 Ein VLAN löschen 424
11.5 Verwalten von GOOSE-Tunneln 424
11.5.1 Statistik der GOOSE-Tunnel anzeigen 425
11.5.2 Eine Liste der GOOSE-Tunnel anzeigen 426

11.5.3 Einen GOOSE-Tunnel hinzufügen ... 427
11.5.4 Einen GOOSE-Tunnel löschen ... 427
11.5.5 Entfernte Daemons für GOOSE-Tunnel verwalten ... 428
11.5.5.1 Eine Liste der entfernten Daemons anzeigen ... 428
11.5.5.2 Einen entfernten Daemon hinzufügen ... 428
11.5.5.3 Einen entfernten Daemon löschen ... 429
11.6 Generische Tunnel verwalten ... 429
11.6.1 Statistik generischer Tunnel anzeigen ... 429
11.6.2 Eine Liste generischer Tunnel anzeigen ... 430
11.6.3 Hinzufügen eines generischen Tunnels ... 431
11.6.4 Einen generischen Tunnel löschen ... 431
11.6.5 IP-Adressen entfernter Daemons für generische Tunnel verwalten ... 432
11.6.5.1 Eine Liste der IP-Adressen anzeigen ... 432
11.6.5.2 Eine IP-Adresse hinzufügen ... 432
11.6.5.3 Eine IP-Adresse löschen ... 433
11.6.6 Ausgehende (egress) Schnittstellen entfernter Daemons für generische Tunnel verwalten ... 433
11.6.6.1 Eine Liste der ausgehenden (egress) Schnittstellen anzeigen ... 433
11.6.6.2 Eine ausgehende (egress) Schnittstelle hinzufügen ... 434
11.6.6.3 Eine ausgehende (egress) Schnittstelle löschen ... 434
11.6.7 Ethernet-Typen für generische Tunnel verwalten ... 435
11.6.7.1 Eine Liste der Ethernet-Typen anzeigen ... 435
11.6.7.2 Einen Ethernet-Typ hinzufügen ... 435
11.6.7.3 Einen Ethernet-Typ löschen ... 436
11.7 GRE (Generic Routing Encapsulation)-Tunnel verwalten ... 436
11.7.1 Statistiken für GRE-Tunnel anzeigen ... 437
11.7.2 Eine Liste der GRE-Tunnel anzeigen ... 438
11.7.3 Hinzufügen eines GRE-Tunnels ... 438
11.7.4 Konfigurieren einer DSCP-Kennzeichnung für den GRE-Tunnelverkehr ... 440
11.7.5 Einen GRE-Tunnel löschen ... 440
11.8 IPsec-Tunnel verwalten ... 441
11.8.1 IPsec-Tunneling-Konzepte ... 441
11.8.1.1 IPsec-Betriebsarten ... 442
11.8.1.2 Unterstützte Verschlüsselungsprotokolle ... 442
11.8.1.3 Kryptografie von öffentlichen und geheimen Schlüsseln ... 442
11.8.1.4 X.509-Zertifikate ... 443
11.8.1.5 NAT Traversal ... 443
11.8.1.6 Unterstützung eines entfernten IPsec-Clients ... 443
11.8.1.7 IPsec- und Router-Schnittstellen ... 444
11.8.2 Konfigurieren von IPsec-Tunneln ... 444
11.8.3 Konfigurieren von Zertifikaten und Schlüsseln ... 445

11.8.4 Anzeigen des Status des IPSec-Tunnels ... 446
11.8.5 Vorher vereinbarte (pre-shared) Schlüssel verwalten ... 447
11.8.5.1 Eine Liste der vorher vereinbarten Schlüssel anzeigen ... 447
11.8.5.2 Einen vorher vereinbarten Schlüssel hinzufügen ... 447
11.8.5.3 Einen vorher vereinbarten Schlüssel löschen ... 448
11.8.6 Verbindungen verwalten ... 448
11.8.6.1 Eine Liste der Verbindungen anzeigen ... 449
11.8.6.2 Hinzufügen einer Verbindung ... 449
11.8.6.3 Konfigurieren der Dead Peer Detection ... 451
11.8.6.4 Eine Verbindung löschen ... 452
11.8.7 Das IKE-(Internet Key Exchange)-Protokoll verwalten ... 452
11.8.7.1 Eine Liste der IKE-Algorithmen anzeigen ... 453
11.8.7.2 Hinzufügen eines IKE-Algorithmus ... 453
11.8.7.3 Löschen eines IKE-Algorithmus ... 453
11.8.8 Ein ESP-Protokoll (Encapsulated Security Payload) verwalten ... 454
11.8.8.1 Konfigurieren der ESP-Verschlüsselung ... 454
11.8.8.2 Eine Liste der ESP-Algorithmen anzeigen ... 455
11.8.8.3 Einen ESP-Algorithmus hinzufügen ... 455
11.8.8.4 Einen ESP-Algorithmus löschen ... 456
11.8.9 Konfigurieren der Verbindungsenden ... 456
11.8.10 Private Subnetze verwalten ... 458
11.8.10.1 Private Subnetze für Verbindungsenden konfigurieren ... 458
11.8.10.2 Eine Adressliste für private Subnetze anzeigen ... 459
11.8.10.3 Eine Adresse für ein privates Subnetz hinzufügen ... 459
11.8.10.4 Löschen einer Adresse für ein privates Subnetz ... 460
11.9 6in4- und 4in6-Tunnel verwalten ... 460
11.9.1 6in4- oder 4in6-Tunnel aktivieren/deaktivieren ... 460
11.9.2 Eine Liste der 6in4- oder 4in6-Tunnel anzeigen ... 461
11.9.3 Den Status von 6in4/4in6-Tunneln anzeigen ... 461
11.9.4 Einen 6in4- oder 4in6-Tunnel hinzufügen ... 461
11.9.5 Einen 6in4- oder 4in6-Tunnel löschen ... 462
11.10 DMVPN verwalten ... 462
11.10.1 Beschreibung des DMVPN ... 463
11.10.2 Konfigurieren von DMVPN ... 464
11.10.3 DMVPN-Schnittstellen verwalten ... 465
11.10.3.1 Eine Liste der DMVPN-Schnittstellen anzeigen ... 465
11.10.3.2 Eine DMVPN-Schnittstelle hinzufügen ... 465
11.10.3.3 Eine DMVPN-Schnittstelle löschen ... 466
11.10.4 Anzeigen des Status von DMVPN ... 466

Kapitel 12
Unicast- und Multicast-Routing 469
12.1 Den Status der IPv4-Routen anzeigen 469
12.2 Den Status von IPv6-Routen anzeigen 470
12.3 Speicherstatistik anzeigen 471
12.4 Konfigurieren von ICMP 472
12.5 Event-Tracker verwalten 473
12.5.1 Eine Liste der Event-Tracker anzeigen 473
12.5.2 Statistiken für Event-Tracker anzeigen 474
12.5.3 Einen Event Tracker hinzufügen 474
12.5.4 Einen Event-Tracker löschen 475
12.6 IS-IS verwalten 476
12.6.1 IS-IS-Konzepte 476
12.6.1.1 IS-IS-Router 477
12.6.1.2 NET-(Network Entity Title)-Adressen 477
12.6.1.3 Vor- und Nachteile der Verwendung von IS-IS 478
12.6.2 Konfigurieren von IS-IS 478
12.6.3 Anzeigen des Status von Nachbarn 479
12.6.4 Anzeigen des Status einer Link-State-Datenbank 480
12.6.5 Bereichsvariablen verwalten 481
12.6.5.1 Eine Liste der Bereichsvariablen anzeigen 481
12.6.5.2 Hinzufügen einer Bereichsvariablen 482
12.6.5.3 Eine Bereichsvariable löschen 483
12.6.6 Schnittstellen verwalten 484
12.6.6.1 Eine Liste der Schnittstellen anzeigen 484
12.6.6.2 Konfigurieren einer Schnittstelle 485
12.6.7 LSP-Generierung verwalten 486
12.6.7.1 Eine Liste der Intervalle zur LSP-Generierung anzeigen 486
12.6.7.2 Hinzufügen eines LSP-Generierungsintervalls 487
12.6.7.3 Ein Intervall zur LSP-Generierung löschen 487
12.6.8 SPF-Berechnungen verwalten 487
12.6.8.1 Eine Liste der SPF-Berechnungsintervalle anzeigen 488
12.6.8.2 Ein SPF-Berechnungsintervall hinzufügen 488
12.6.8.3 Ein SPF-Berechnungsintervall löschen 488
12.6.9 Die Lebensdauer von LSPs verwalten 489
12.6.9.1 Eine Liste der LSP-Lebensdauerintervalle anzeigen 489
12.6.9.2 Hinzufügen eines LSP-Lebensdauerintervalls 490
12.6.9.3 Ein LSP-Lebensdauer-Intervall löschen 490
12.6.10 LSP-Auffrischungsintervalle verwalten 491
12.6.10.1 Eine Liste der LSP-Aktualisierungsintervalle anzeigen 491

12.6.10.2 Hinzufügen eines LSP-Aktualisierungsintervalls ... 491
12.6.10.3 Ein LSP-Aktualisierungsintervall löschen ... 492
12.6.11 Verwalten von Network Entity Titles (NETs) ... 492
12.6.11.1 Eine Liste der NETs anzeigen ... 493
12.6.11.2 Eine NET hinzufügen ... 493
12.6.11.3 Eine Network Entity Title löschen ... 494
12.6.12 Umverteilungsmetriken verwalten ... 494
12.6.12.1 Eine Liste der Umverteilungsmetriken anzeigen ... 495
12.6.12.2 Eine Umverteilungsmetrik hinzufügen ... 495
12.6.12.3 Eine Umverteilungsmetrik löschen ... 496
12.7 Verwalten des RIP ... 496
12.7.1 Konfigurieren des RIP ... 497
12.7.2 Anzeigen des Status von dynamischen RIP-Routen ... 498
12.7.3 Präfix-Listen und -Einträge verwalten ... 499
12.7.3.1 Eine Liste der Präfixeinträge anzeigen ... 500
12.7.3.2 Eine Liste der Präfixeinträge anzeigen ... 500
12.7.3.3 Eine Präfixliste hinzufügen ... 500
12.7.3.4 Einen Präfixeintrag hinzufügen ... 501
12.7.3.5 Eine Präfixliste löschen ... 502
12.7.3.6 Einen Präfixeintrag löschen ... 502
12.7.4 Netzwerke verwalten ... 502
12.7.4.1 Ein Netzwerk konfigurieren ... 503
12.7.4.2 Nachverfolgen von Befehlen ... 503
12.7.5 Netzwerk-IP-Adressen verwalten ... 504
12.7.5.1 Eine Liste der Netzwerk-IP-Adressen anzeigen ... 504
12.7.5.2 Eine Netzwerk-IP-Adresse hinzufügen ... 504
12.7.5.3 Eine Netzwerk-IP-Adresse löschen ... 505
12.7.6 Netzwerkschnittstellen verwalten ... 505
12.7.6.1 Eine Liste der Netzwerkschnittstellen anzeigen ... 505
12.7.6.2 Eine Netzwerkschnittstelle hinzufügen ... 506
12.7.6.3 Eine Netzwerkschnittstelle löschen ... 506
12.7.7 Nachbarn verwalten ... 506
12.7.7.1 Eine Liste der Nachbarn anzeigen ... 506
12.7.7.2 Einen Nachbarn hinzufügen ... 507
12.7.7.3 Einen Nachbarn löschen ... 507
12.7.8 Verteilung der Präfix-Liste verwalten ... 507
12.7.8.1 Eine Liste der Präfixlisten-Verteilerpfade anzeigen ... 508
12.7.8.2 Hinzufügen eines Präfixlisten-Verteilpfads ... 508
12.7.8.3 Einen Präfixlisten-Verteilpfad löschen ... 508
12.7.9 Schlüsselbunde und Schlüssel verwalten ... 509

12.7.9.1 Eine Liste der Schlüsselbunde (Key Chains) anzeigen 509
12.7.9.2 Eine Liste der Schlüssel anzeigen 510
12.7.9.3 Ein Schlüsselbund hinzufügen 510
12.7.9.4 Hinzufügen eines Schlüssels 511
12.7.9.5 Ein Schlüsselbund (Key Chain) löschen 512
12.7.9.6 Einen Schlüssel löschen 512
12.7.10 Umverteilungsmetriken verwalten 513
12.7.10.1 Eine Liste der Umverteilungsmetriken anzeigen 513
12.7.10.2 Eine Umverteilungsmetrik hinzufügen 513
12.7.10.3 Eine Umverteilungsmetrik löschen 513
12.7.11 Routing-Schnittstellen verwalten 514
12.7.11.1 Eine Liste der Routing-Schnittstellen anzeigen 514
12.7.11.2 Eine Routing-Schnittstelle konfigurieren 514
12.8 BGP verwalten 515
12.8.1 Konfigurieren von BGP 516
12.8.2 Anzeigen des Status von dynamischen BGP-Routen 517
12.8.3 Routen-Karten verwalten 519
12.8.3.1 Eine Liste der Route-Map-Filter anzeigen 520
12.8.3.2 Eine Liste der Einträge im Route-Map-Filter anzeigen 520
12.8.3.3 Einen Route-Map-Filter hinzufügen 521
12.8.3.4 Einen Eintrag für einen Route-Map-Filter hinzufügen 521
12.8.3.5 Einen Route-Map-Filter löschen 522
12.8.3.6 Einen Eintrag im Route-Map-Filter löschen 522
12.8.3.7 Konfigurieren von Übereinstimmungsregeln 522
12.8.3.8 Konfigurieren eines Satzes 523
12.8.4 Vorgelagerte und ausgegliederte autonome Systempfadfilter verwalten 524
12.8.4.1 Eine Liste der vorgelagerten autonomen Systempfadfilter anzeigen 524
12.8.4.2 Eine Liste der ausgegliederten autonomen Systempfade anzeigen 524
12.8.4.3 Einen vorgelagerten autonomen Systempfadfilter hinzufügen 525
12.8.4.4 Einen ausgegliederten autonomen Systempfadfilter hinzufügen 525
12.8.4.5 Einen vorgelagerten autonomen Systempfadfilter löschen 526
12.8.4.6 Einen ausgegliederten autonomen Systempfadfilter löschen 526
12.8.5 Präfix-Listen und -Einträge verwalten 527
12.8.5.1 Eine Liste der Präfixeinträge anzeigen 527
12.8.5.2 Eine Liste der Präfixeinträge anzeigen 527
12.8.5.3 Eine Präfixliste hinzufügen 528
12.8.5.4 Einen Präfixeintrag hinzufügen 528
12.8.5.5 Eine Präfixliste löschen 529
12.8.5.6 Einen Präfixeintrag löschen 529
12.8.6 Autonome Systempfade und Einträge verwalten 530

12.8.6.1 Eine Liste der autonomen Systempfade anzeigen 530
12.8.6.2 Eine Liste der autonomen Systempfadeinträge anzeigen 530
12.8.6.3 Einen autonomen Systempfadfilter hinzufügen 531
12.8.6.4 Hinzufügen eines Eintrags für einen autonomen Systempfadfilter 531
12.8.6.5 Einen autonomen Systempfadfilter löschen 531
12.8.6.6 Einen Eintrag für einen autonomen Systempfadfilter löschen 532
12.8.7 Nachbarn verwalten 532
12.8.7.1 Eine Liste der Nachbarn anzeigen 533
12.8.7.2 Einen Nachbarn hinzufügen 533
12.8.7.3 Konfigurieren der Verteilung von Präfixlisten 534
12.8.7.4 Nachverfolgen von Befehlen für BGP-Nachbarn 534
12.8.7.5 Einen Nachbarn löschen 535
12.8.8 Netzwerke verwalten 535
12.8.8.1 Eine Liste der Netzwerke anzeigen 536
12.8.8.2 Ein Netzwerk hinzufügen 536
12.8.8.3 Nachverfolgen von Befehlen für ein BGP-Netzwerk 537
12.8.8.4 Ein Netzwerk löschen 537
12.8.9 Sammeladressen verwalten 538
12.8.9.1 Eine Liste der Sammeladressen anzeigen 538
12.8.9.2 Eine Sammeladresse hinzufügen 538
12.8.9.3 Eine Sammeladresse löschen 539
12.8.10 Optionen für Sammeladressen verwalten 539
12.8.10.1 Eine Liste der Optionen für Sammeladressen anzeigen 539
12.8.10.2 Eine Option für Sammeladressen hinzufügen 540
12.8.10.3 Eine Option für Sammeladressen löschen 540
12.8.11 Umverteilungsmetriken verwalten 540
12.8.11.1 Eine Liste der Umverteilungsmetriken anzeigen 540
12.8.11.2 Eine Umverteilungsmetrik hinzufügen 541
12.8.11.3 Eine Umverteilungsmetrik löschen 541
12.9 Verwalten von OSPF 541
12.9.1 OSPF-Grundlagen 542
12.9.2 Konfigurieren des OSPF 543
12.9.3 Anzeigen des Status von dynamischen OSPF-Routen 544
12.9.4 Präfix-Listen und -Einträge verwalten 546
12.9.4.1 Eine Liste der Präfixlisten anzeigen 546
12.9.4.2 Eine Liste der Präfixeinträge anzeigen 547
12.9.4.3 Hinzufügen einer Präfixliste 547
12.9.4.4 Hinzufügen eines Präfixeintrags 548
12.9.4.5 Eine Präfixliste löschen 549
12.9.4.6 Einen Präfixeintrag löschen 549

12.9.5 Bereiche verwalten 550
12.9.5.1 Eine Liste der Bereiche anzeigen 550
12.9.5.2 Hinzufügen eines Bereichs 551
12.9.5.3 Einen Bereich löschen 551
12.9.6 Routen-Karten verwalten 552
12.9.6.1 Eine Liste der Route-Map-Filter anzeigen 552
12.9.6.2 Anzeigen einer Liste der Einträge für einen Route-Map-Filter 553
12.9.6.3 Hinzufügen eines Route-Map-Filters 553
12.9.6.4 Einen Eintrag für einen Route-Map-Filter hinzufügen 554
12.9.6.5 Einen Route-Map-Filter löschen 555
12.9.6.6 Löschen eines Eintrags im Route-Map-Filter 555
12.9.6.7 Konfigurieren von Übereinstimmungsregeln 556
12.9.7 Filter für eingehende Routen verwalten 556
12.9.7.1 Liste der Filter für eingehende Routen anzeigen 557
12.9.7.2 Hinzufügen eines Filters für eingehende Routen 557
12.9.7.3 Einen Filter für eingehende Routen löschen 558
12.9.8 Umverteilungsmetriken verwalten 558
12.9.8.1 Anzeigen Liste mit Umverteilungsmetriken 558
12.9.8.2 Hinzufügen einer Umverteilungsmetrik 559
12.9.8.3 Eine Umverteilungsmetrik löschen 559
12.9.9 Routing-Schnittstellen verwalten 560
12.9.9.1 Eine Liste der Routing-Schnittstellen anzeigen 560
12.9.9.2 Eine Routing-Schnittstelle konfigurieren 560
12.9.10 Message Digest Keys verwalten 563
12.9.10.1 Eine Liste der Message Digest Keys anzeigen 563
12.9.10.2 Hinzufügen eines Message Digest Key 564
12.9.10.3 Einen Message Digest Key löschen 564
12.10 MPLS verwalten 565
12.10.1 Status des IP Binding anzeigen 565
12.10.2 Status der Forwarding-Tabelle anzeigen 566
12.10.3 MPLS aktivieren/deaktivieren 566
12.10.4 MPLS-Schnittstellen verwalten 567
12.10.4.1 Status der MPLS-Schnittstellen anzeigen 567
12.10.4.2 Eine Liste der MPLS-Schnittstellen anzeigen 568
12.10.4.3 Eine MPLS-Schnittstelle aktivieren/deaktivieren 568
12.10.5 Statisches Label Binding verwalten 569
12.10.5.1 Den Status statischer Label Bindings anzeigen 569
12.10.5.2 Eine Liste der statischen Label anzeigen 569
12.10.5.3 Hinzufügen eines statischen Labels 570
12.10.5.4 Ein statisches Label 571

12.10.6 Statische Crossconnects verwalten 571
12.10.6.1 Status der statischen Crossconnects anzeigen 571
12.10.6.2 Eine Liste der statischen Crossconnects anzeigen 572
12.10.6.3 Einen statischen Crossconnect hinzufügen 572
12.10.6.4 Einen statischen Crossconnect löschen 573
12.10.7 LDP verwalten 573
12.10.7.1 Status des LDP Binding anzeigen 574
12.10.7.2 Status der LDP-Erkennungsschnittstellen anzeigen 575
12.10.7.3 Status der lokalen Knoten des LDP-Nachbarn anzeigen 575
12.10.7.4 Status der LDP-Nachbarverbindungsinformationen anzeigen 576
12.10.7.5 Status der LDP-Nachbarerkennungsinformationen anzeigen 577
12.10.7.6 Das LDP konfigurieren 577
12.10.7.7 Neighbor Discovery konfigurieren 578
12.10.7.8 Eine Liste der LDP-Schnittstellen anzeigen 579
12.10.7.9 Eine LDP-Schnittstelle aktivieren/deaktivieren 579
12.11 Verwalten von VRF (Virtual Routing and Forwarding) 579
12.11.1 VRF-Konzepte 580
12.11.1.1 VRF und VRF-Lite 580
12.11.1.2 Vor- und Nachteile der Verwendung von VRF 581
12.11.2 Statistiken zu VRF-Schnittstellen anzeigen 581
12.11.3 Konfigurieren von VRF 583
12.11.4 Eine VRF-Schnittstelle konfigurieren 584
12.11.5 VRF-Definitionen verwalten 584
12.11.5.1 Eine Liste der VRF-Definitionen anzeigen 585
12.11.5.2 Hinzufügen einer VRF-Definition 585
12.11.5.3 Löschen einer VRF-Definition 586
12.11.6 Routenziele verwalten 586
12.11.6.1 Eine Liste der Routenziele anzeigen 586
12.11.6.2 Ein Routenziel hinzufügen 587
12.11.6.3 Ein Routenziel löschen 587
12.11.7 VRF-Instanzen und OSPF verwalten 588
12.11.7.1 Eine Liste der VRF-Instanzen anzeigen 588
12.11.7.2 Hinzufügen einer VRF-Instanz und Konfigurieren von OSPF 588
12.11.7.3 Eine VRF-Instanz löschen 590
12.11.8 IP/VPN-Tunnel verwalten 590
12.11.8.1 Eine Liste der IP/VPN-Tunnel anzeigen 591
12.11.8.2 Einen IP-/VPN-Tunnel hinzufügen 591
12.11.8.3 Einen IP/VPN-Tunnel löschen 591
12.11.9 VPNv4-Nachbarn verwalten 592
12.11.9.1 Eine Liste der Nachbarn anzeigen 592

12.11.9.2 Einen Nachbarn hinzufügen 592
12.11.9.3 Einen Nachbarn löschen 593
12.11.10 IPv4-Adressfamilien verwalten 593
12.11.10.1 Eine Liste der IPv4-Adressfamilien anzeigen 593
12.11.10.2 Eine Familie von IPv4-Adressen hinzufügen 594
12.11.10.3 Eine Familie von IPv4-Adressen löschen 594
12.11.11 Umverteilung für IPv4-Adressfamilien verwalten 595
12.11.11.1 Eine Liste der Umverteilungen anzeigen 595
12.11.11.2 Eine Umverteilung hinzufügen 595
12.11.11.3 Eine Umverteilung löschen 596
12.11.12 Nachbarn für IPv4-Adressfamilien verwalten 596
12.11.12.1 Eine Liste der Nachbarn anzeigen 597
12.11.12.2 Einen Nachbarn hinzufügen 597
12.11.12.3 Konfigurieren der Verteilung von Präfixlisten 598
12.11.12.4 Nachverfolgen von Befehlen 599
12.11.12.5 Einen Nachbarn löschen 599
12.11.13 Statische VRF-Routen verwalten 600
12.11.13.1 Eine Liste der statischen VRF-Routen anzeigen 600
12.11.13.2 Hinzufügen einer statischen VRF-Route 600
12.11.13.3 Eine Black-Hole-Verbindung für eine statische VRF-Route konfigurieren 601
12.11.13.4 Eine statische VRF-Route löschen 602
12.11.14 Gateways für statische VRF-Routen verwalten 602
12.11.14.1 Eine Liste der Gateways für statische VRF-Routen anzeigen 602
12.11.14.2 Hinzufügen eines Gateway für eine statische VRF-Route 603
12.11.14.3 Ein Gateway für eine statische VRF-Route löschen 603
12.11.15 Schnittstellen für statische VRF-Routen verwalten 604
12.11.15.1 Eine Liste der Schnittstellen für statische VRF-Routen anzeigen 604
12.11.15.2 Hinzufügen eines Gateway für eine statische VRF-Route 604
12.11.15.3 Ein Gateway für eine statische VRF-Route löschen 605
12.12 Statische Routen verwalten 605
12.12.1 Eine Liste der statischen Routen anzeigen 606
12.12.2 Hinzufügen einer statischen IPv4-Route 606
12.12.3 Eine statische IPv6-Route hinzufügen 607
12.12.4 Eine statische Route löschen 607
12.12.5 Eine Black-Hole-Verbindung für eine statische IPv4-Route konfigurieren 608
12.12.6 Gateways für statische Routen verwalten 608
12.12.6.1 Gateways für statische IPv6-Routen konfigurieren 608
12.12.6.2 Eine Liste der Gateways für statische IPv4-Routen anzeigen 609
12.12.6.3 Ein Gateway für eine statische IPv4-Route hinzufügen 609
12.12.6.4 Ein Gateway für eine statische IPv4-Route löschen 610

12.12.7 Schnittstellen für statische Routen verwalten 610
12.12.7.1 Schnittstellen für statische Ipv6-Routen konfigurieren 610
12.12.7.2 Eine Liste der Schnittstellen für statische IPv4-Routen anzeigen 611
12.12.7.3 Eine Schnittstelle für eine statische IPv4-Route hinzufügen 611
12.12.7.4 Eine Schnittstelle für eine statische IPv4-Route löschen 612
12.13 Statisches Multicast-Routing verwalten 612
12.13.1 Statisches Multicast-Routing aktivieren/deaktivieren 612
12.13.2 Statische Multicast-Gruppen verwalten 613
12.13.2.1 Eine Liste statischer Multicast-Gruppen anzeigen 613
12.13.2.2 Hinzufügen einer statischen Multicast-Gruppe 614
12.13.2.3 Eine statische Multicast-Gruppe löschen 614
12.13.3 Out-Schnittstellen verwalten 615
12.13.3.1 Eine Liste der Out-Schnittstellen anzeigen 615
12.13.3.2 Ein OUT-Interface hinzufügen 615
12.13.3.3 Ein Out-Interface löschen 616
12.14 Verwalten des dynamischen Multicast-Routing 616
12.14.1 PIM-SM-Grundlagen 617
12.14.2 Anzeigen des Status von PIM-SM 618
12.14.3 Status des dynamischen Multicast-Routings anzeigen 619
12.14.4 PIM-SM konfigurieren 619
12.14.5 Das Gerät als BSR-Kandidat einstellen 620
12.14.6 Das Gerät als RP-Kandidat einstellen 620
12.14.7 PIM-SM-Schnittstellen verwalten 621
12.14.7.1 Eine Liste der PIM-SM-Schnittstellen anzeigen 621
12.14.7.2 Aktivieren/Deaktivieren einer PIM-SM-Schnittstelle 621
12.14.8 Statische RP-Adressen verwalten 622
12.14.8.1 Eine Liste der statischen RP-Adressen anzeigen 622
12.14.8.2 Eine statische RP-Adresse hinzufügen 623
12.14.8.3 Eine statische RP-Adresse löschen 623
12.14.9 Multicast-Gruppen-Präfixe verwalten 624
12.14.9.1 Eine Liste der Multicast-Gruppen-Präfixe anzeigen 624
12.14.9.2 Ein Präfix für eine Multicast-Gruppe hinzufügen 624
12.14.9.3 Ein Präfix für eine Multicast-Gruppe löschen 625

Kapitel 13
Netzwerkredundanz 627
13.1 VRRP verwalten 627
13.1.1 VRRP-Konzepte 628
13.1.1.1 Statisches Routing vs. VRRP 628
13.1.1.2 VRRP-Terminologie 628
13.1.1.3 Verbindungssynchronisation 631

13.1.2 Status des VRRP anzeigen 631
13.1.3 VRRP aktivieren/deaktivieren 632
13.1.4 VRRP-Tracker verwalten 632
13.1.4.1 Eine Liste der VRRP-Tracker anzeigen 633
13.1.4.2 Einen VRRP-Tracker hinzufügen 633
13.1.4.3 Einen VRRP-Tracker löschen 634
13.1.5 VRRP-Gruppen verwalten 635
13.1.5.1 Eine Liste der VRRP-Gruppen anzeigen 635
13.1.5.2 Eine VRRP-Gruppe hinzufügen 635
13.1.5.3 Eine VRRP-Gruppe löschen 636
13.1.6 VRRP-Instanzen verwalten 636
13.1.6.1 Eine Liste der VRRP-Instanzen anzeigen 636
13.1.6.2 Hinzufügen einer VRRP-Instanz 637
13.1.6.3 Eine VRRP-Instanz löschen 638
13.1.7 VRRP-Überwachungen verwalten 639
13.1.7.1 Eine Liste der VRRP-Überwachungen anzeigen 639
13.1.7.2 Eine VRRP-Überwachung hinzufügen 639
13.1.7.3 Eine VRRP-Überwachung löschen 640
13.1.8 Track Scripts verwalten 640
13.1.8.1 Eine Liste der Track Scripts anzeigen 640
13.1.8.2 Ein Track-Skript hinzufügen 641
13.1.8.3 Ein Track-Skript löschen 641
13.1.9 Virtuelle IP-Adressen verwalten 642
13.1.9.1 Eine Liste virtueller IP-Adressen anzeigen 642
13.1.9.2 Eine virtuelle IP-Adresse hinzufügen 642
13.1.9.3 Eine virtuelle IP-Adresse löschen 643
13.1.10 Verbindungssynchronisation verwalten 643
13.1.10.1 Verbindungssynchronisation konfigurieren 643
13.1.10.2 Verbindungssynchronisation aktivieren/deaktivieren 644
13.1.10.3 Eine Liste fest zugeordneter Links anzeigen 644
13.1.10.4 Einen fest zugeordneten Link hinzufügen 645
13.1.10.5 Einen fest zugeordneten Link löschen 645
13.1.10.6 Einen fest zugeordneten Link auswählen 646
13.1.10.7 Anzeigen des Status von jedem fest zugeordneten Link 646
13.2 Schutz vor Verbindungs-Failover verwalten 647
13.2.1 Anzeigen des Verbindungs-Failover-Protokolls 648
13.2.2 Den Status des Verbindungs-Failover anzeigen 649
13.2.3 Parameter für Verbindungs-Failover verwalten 649
13.2.3.1 Eine Liste der Parameter für Verbindungs-Failover anzeigen 650
13.2.3.2 Hinzufügen eines Parameters für Verbindungs-Failover 650

13.2.3.3 Einen Parameter für Verbindungs-Failover löschen 651
13.2.4 Backup-Schnittstellen für Verbindungs-Failover verwalten 651
13.2.4.1 Eine Liste der Backup-Schnittstellen für Verbindungs-Failover anzeigen 652
13.2.4.2 Hinzufügen einer Backup-Schnittstelle für Verbindungs-Failover 652
13.2.4.3 Eine Backup-Schnittstelle für Verbindungs-Failover löschen 653
13.2.5 Ping-Ziele für Verbindungs-Failover verwalten 654
13.2.5.1 Eine Liste der Ping-Ziele für Verbindungs-Failover anzeigen 654
13.2.5.2 Hinzufügen eines Ping-Ziels für Verbindungs-Failover 654
13.2.5.3 Ein Ping-Ziel für Verbindungs-Failover löschen 655
13.2.6 Testen des Verbindungs-Failovers 655
13.2.7 Einen Verbindungs-Failover-Test abbrechen 656

Kapitel 14
Netzwerkerkennung und -management 657
14.1 Verwalten von LLDP 657
14.1.1 Das LLDP konfigurieren 658
14.1.2 Anzeigen der globalen Statistik und bekanntgegebener Systeminformationen 659
14.1.3 Statistiken für LLDP-Nachbarn anzeigen 661
14.1.4 Anzeigen der Statistik für LLDP-Ports 662
14.2 Verwalten von SNMP 663
14.2.1 MIB-Dateien und SNMP-Traps 664
14.2.2 Aktivieren und Konfigurieren von SNMP-Sitzungen 666
14.2.3 Statistiken für SNMP anzeigen 667
14.2.4 IDs von SNMP-Protokoll-Engines finden 668
14.2.5 SNMP-Communities verwalten 668
14.2.5.1 Eine Liste der SNMP-Communities anzeigen 669
14.2.5.2 Eine SNMP-Community hinzufügen 669
14.2.5.3 Eine SNMP-Community löschen 670
14.2.6 SNMP-Zieladressen verwalten 670
14.2.6.1 Eine Liste der SNMP-Zieladressen anzeigen 670
14.2.6.2 Eine SNMP-Zieladresse hinzufügen 671
14.2.6.3 Eine SNMP-Zieladresse löschen 672
14.2.7 SNMP-Benutzer verwalten 672
14.2.7.1 Eine Liste der SNMP-Benutzer anzeigen 672
14.2.7.2 Hinzufügen eines SNMP-Benutzers 673
14.2.7.3 Einen SNMP-Benutzer löschen 674
14.2.8 Zuordnung des SNMP-Sicherheitsmodells verwalten 674
14.2.8.1 Eine Liste der SNMP-Sicherheitsmodelle anzeigen 674
14.2.8.2 Hinzufügen eines SNMP-Sicherheitsmodells 675
14.2.8.3 Ein SNMP-Sicherheitsmodell löschen 675
14.2.9 SNMP-Gruppenzugang verwalten 676

14.2.9.1 Eine Liste der SNMP-Gruppen anzeigen 676
14.2.9.2 Hinzufügen einer SNMP-Gruppe 676
14.2.9.3 Eine SNMP-Gruppe löschen 677
14.3 NETCONF verwalten 677
14.3.1 Aktivieren und Konfigurieren von NETCONF-Sitzungen 678
14.3.2 NETCONF-Statistiken anzeigen 679

Kapitel 15
Verkehrssteuerung und -klassifizierung 681
15.1 Verwalten der Port-Spiegelung 681
15.1.1 Port-Spiegelung konfigurieren 682
15.1.2 Ausgehende Quellports verwalten 682
15.1.2.1 Eine Liste ausgehender (egress) Quellports anzeigen 682
15.1.2.2 Einen ausgehenden (egress) Quellport hinzufügen 683
15.1.2.3 Einen ausgehenden (egress) Quellport löschen 683
15.1.3 Eingehende (ingress) Quellports verwalten 684
15.1.3.1 Eine Liste der eingehenden (ingress) Quellports anzeigen 684
15.1.3.2 Einen eingehenden (ingress) Quellport hinzufügen 684
15.1.3.3 Einen eingehenden (ingress) Quellport löschen 685
15.2 Verkehrssteuerung verwalten 685
15.2.1 Aktivieren und Konfigurieren der Verkehrssteuerung 686
15.2.2 Verkehrssteuerungsschnittstellen verwalten 687
15.2.2.1 Eine Liste der Verkehrssteuerungsschnittstellen anzeigen 687
15.2.2.2 Eine Verkehrssteuerungsschnittstelle hinzufügen 688
15.2.2.3 Eine Verkehrssteuerungsschnittstelle löschen 689
15.2.3 Verkehrssteuerungsprioritäten verwalten 689
15.2.3.1 Eine Liste der Verkehrssteuerungsprioritäten anzeigen 690
15.2.3.2 Eine Verkehrssteuerungspriorität hinzufügen 690
15.2.3.3 Eine Verkehrssteuerungspriorität löschen 691
15.2.4 Verkehrssteuerungsklassen verwalten 692
15.2.4.1 Eine Liste der Verkehrssteuerungsklassen anzeigen 692
15.2.4.2 Hinzufügen einer Verkehrssteuerungsklasse 693
15.2.4.3 Eine Verkehrssteuerungsklasse löschen 694
15.2.5 Verkehrssteuerungsgeräte verwalten 694
15.2.5.1 Eine Liste der Verkehrssteuerungsgeräte anzeigen 695
15.2.5.2 Ein Verkehrssteuergerät hinzufügen 695
15.2.5.3 Ein Verkehrssteuergerät löschen 696
15.2.6 Verkehrssteuerungsregeln verwalten 696
15.2.6.1 Eine Liste der Verkehrssteuerungsregeln anzeigen 697
15.2.6.2 Hinzufügen einer Verkehrssteuerungsregel 697
15.2.6.3 QoS-Kennzeichnungen konfigurieren 698

15.2.6.4 Eine Verkehrsteuerungsregel löschen 702
15.2.7 QoS-Mapping für VLANs verwalten 702
15.2.7.1 Anzeigen einer Liste der QoS-Maps für VLANs 703
15.2.7.2 Hinzufügen einer QoS-Map 703
15.2.7.3 Löschen einer QoS-Map 704
15.2.8 Egress-Marker für QoS-Maps verwalten 704
15.2.8.1 Anzeigen einer Liste der ausgehenden (egress) Kennzeichnungen 705
15.2.8.2 Hinzufügen einer ausgehenden (egress) Kennzeichnung 705
15.2.8.3 Löschen einer ausgehenden (egress) Kennzeichnung 706
15.2.9 QoS-Statistiken anzeigen 707
15.3 Verwalten von Berechtigungsklassen 708
15.3.1 Berechtigungsklassen (Classes of Service, CoS) konfigurieren 709
15.3.2 Priority-to-CoS-Mapping verwalten 709
15.3.2.1 Eine Liste der Priority-to-CoS-Mapping-Einträge anzeigen 709
15.3.2.2 Einen Priority-zu-CoS Mapping-Eintrag hinzufügen 710
15.3.2.3 Einen Priority-zu-CoS Mapping-Eintrag löschen 710
15.3.3 DSCP-to-CoS-Mapping verwalten 711
15.3.3.1 Eine Liste der DSCP-to-CoS-Mapping-Einträge anzeigen 711
15.3.3.2 Hinzufügen eines DSCP-zu-CoS Mapping-Eintrags 711
15.3.3.3 Einen DSCP-zu-CoS Mapping-Eintrag löschen 712

Kapitel 16
Uhrzeitdienste 713
16.1 Die Einstellungen zur Zeitsynchronisation konfigurieren 713
16.2 Systemzeit und -datum konfigurieren 714
16.3 Die Systemzeitzone konfigurieren 714
16.4 Ortszeit-Einstellungen konfigurieren 715
16.5 Den NTP-Service aktivieren und konfigurieren 715
16.6 Anzeigen des Status des NTP-Diensts 716
16.7 Status der Referenzuhren anzeigen 717
16.8 NTP-Server verwalten 718
16.8.1 Eine Liste der NTP-Server anzeigen 718
16.8.2 Überwachen von Subscribern 719
16.8.3 Hinzufügen eines NTP-Servers 720
16.8.4 Einen NTP-Server löschen 721
16.8.5 Serverschlüssel verwalten 721
16.8.5.1 Eine Liste der Serverschlüssel anzeigen 722
16.8.5.2 Einen Server-Schlüssel hinzufügen 722
16.8.5.3 Einen Server-Schlüssel löschen 723
16.8.6 Server-Einschränkungen verwalten 723
16.8.6.1 Eine Liste der Servereinschränkungen anzeigen 723

16.8.6.2 Hinzufügen einer Servereinschränkung 723
16.8.6.3 Eine Servereinschränkung löschen 724
16.9 NTP-Broadcast-/Multicast-Clients verwalten 725
16.9.1 NTP-Multicast-Clients aktivieren und konfigurieren 725
16.9.2 NTP-Broadcast-Clients aktivieren und konfigurieren 726
16.9.3 NTP-Broadcast-/Multicast-Adressen verwalten 726
16.9.3.1 Eine Liste der Broadcast-/Multicast-Adressen anzeigen 726
16.9.3.2 Eine Broadcast-/Multicast-Adresse hinzufügen 727
16.9.3.3 Eine Broadcast-/Multicast-Adresse löschen 728

Kapitel 17
Virtualisierung 729
17.1 Virtualisierung konfigurieren 730
17.2 Eine Imagedatei für eine virtuelle Maschine aufbauen/abrufen 731
17.3 Den Virtualisierungsdienst aktivieren oder deaktivieren 731
17.4 Die aktive virtuelle Maschine bestimmen 731
17.5 Globale Einstellungen konfigurieren 732
17.6 Eine Liste von Namen virtueller Maschinen anzeigen 733
17.7 Hinzufügen einer virtuellen Maschine 733
17.8 Ein Archiv der virtuellen Maschine extrahieren 734
17.9 Image einer vorhandenen virtuellen Maschine laden 734
17.10 Eine virtuelle Maschine löschen 735
17.11 Ein Archiv der virtuellen Maschine löschen 735
17.12 Eine virtuelle Maschine starten 736
17.13 Eine virtuelle Maschine stoppen 736
17.14 VM-Befehle absetzen 736
17.15 Zuweisen eines seriellen Ports 737
17.16 Zuordnung eines seriellen Ports löschen 737
17.17 Die VPE-Netzwerkschnittstelle aktivieren/deaktivieren 737
17.18 Eine virtuelle Schnittstelle hinzufügen 738
17.19 Eine virtuelle Schnittstelle löschen 738
17.20 Zuweisen einer Netzwerkschnittstelle 739
17.21 Auf die aktive virtuelle Maschine zugreifen 740
17.22 Abfragen der Seriennummer des Geräts 740

Kapitel 18
Anwendungen 743
18.1 Eine Liste der installierten Applikationen anzeigen 743
18.2 Eine Anwendung installieren 744
18.3 Ein Upgrade für eine Anwendung ausführen 744
18.4 Eine Anwendung deinstallieren 744

18.5 Applikations-Repositories verwalten 745
18.5.1 Eine Liste der Repositories anzeigen 745
18.5.2 Die Repository-Verbindung überprüfen 745
18.5.3 Ein Repository hinzufügen 746
18.5.4 Ein Repository löschen 746

Kapitel 19
Fehlersuche 747
19.1 Ethernet-Ports 747
19.2 Multicast-Filterung 748
19.3 Spanning Tree 749
19.4 VLANs 750
19.5 Fehlerbehebung bei Firmware-Updates 751

Vorwort

Dieser Leitfaden beschreibt die CLI Benutzeroberfläche für RUGGEDCOM ROX II v2.11 auf dem RUGGEDCOM RX1400. Er enthält Anweisungen und Richtlinien für die Arbeit mit der Software sowie einige allgemeine theoretische Erläuterungen.

Er richtet sich an Mitarbeiter des technischen Netzwerk-Supports, die mit den Abläufen in Netzwerken vertraut sind. Ferner ist er für Netzwerk- und Systemplaner, Systemprogrammierer und Anlagentechniker hilfreich.

INHALT

- "Konventionen"
- "Zugehörige Dokumente"
- "Systemvoraussetzungen"
- "Zugriff auf Dokumentation"
- "Lizenzbedingungen"
- "Training"
- "Kundensupport"

Konventionen

Dieses Benutzerhandbuch CLI verwendet folgende Konventionen zur eindeutigen und effizienten Bereitstellung von Informationen.

Alarmmeldungen

Die folgenden Arten von Alarmmeldungen werden falls erforderlich angezeigt, um wichtige Informationen hervorzuheben.

GEFAHR!
Alarme des Typs „GEFAHR" beschreiben unmittelbare Gefährdungssituationen, die, wenn sie nicht vermiedene werden, zu Tod oder schweren Verletzungen führt.

WARNHINWEIS!
Alarme des Typs „WARNUNG" beschreiben Gefährdungssituationen, die, wenn sie nicht vermieden werden, zu schweren Verletzungen und/oder Schäden an den Geräten führt.

ACHTUNG!
Alarme des Typs „ACHTUNG" beschreiben Gefährdungssituationen, die, wenn sie nicht vermieden werden, zu Tod oder schweren Verletzungen führt.

WICHTIG!
Alarme des Typs „WICHTIG“ geben wichtige Auskünfte, die man kennen sollte, bevor ein Verfahren oder Schritt durchgeführt oder eine Funktion genutzt wird.

HINWEIS
Ein „HINWEIS“ stellt zusätzliche Informationen bereit, zum Beispiel Fakten, Tipps und Einzelheiten.

» CLI-Befehlssyntax

Der Befehlssyntax in einem Command Line Interface (CLI) wird gemäß den folgenden Konventionen beschrieben:

Beispiel	Beschreibung
command	Befehle („Commands“) sind fettgedruckt.
command parameter	Parameter sind in Klartext geschrieben.
command parameter1 parameter2	Die Parameter werden in der Reihenfolge aufgelistet, in der sie eingegeben werden müssen.
command parameter1 *parameter2*	Kursiv geschriebene Parameter müssen mit einem benutzerdefinierten Wert ersetzt werden.
command [parameter1 | parameter2]	Alternative Parameter werden von einem vertikalen Balken getrennt (|). Eckige Klammern zeigen eine erforderliche Auswahl zwischen einem oder mehr Parametern.
command { parameter3 | parameter4 }	Geschwungene Klammern zeigen optionale Parameter an.
command parameter1 parameter2 { parameter3 | parameter4 }	Alle Befehle und Parameter sind in der Reihenfolge, in der sie eingegeben werden müssen.

Zugehörige Dokumente

Weitere Dokumente, die hilfreich sein können, sind:

- *RUGGEDCOM RX1400 Installationsanleitung*
- *Baugruppenkatalog für die RUGGEDCOM RX1400-Serie*
- *RUGGEDCOM RX1400 Datenblatt*
- *RUGGEDCOM ROX II v2.11 Freigabehinweise*

Die meisten Dokumente stehen auf dem Siemens Industry Online Support Portal [https://support.industry.siemens.com] oder als mobile Applikation zur Verfügung. Für weitere Dokumente wenden Sie sich an einen Siemens Händler oder an den Siemens Kundensupport.

Systemvoraussetzungen

Jede Workstation, die für die Verbindung mit der RUGGEDCOM ROX II Rugged CLI-Benutzeroberfläche verwendet wird, muss die folgenden Systemvoraussetzungen erfüllen:

- Es muss eine funktionsfähige Ethernet-Schnittstelle vorhanden sein, die mit mindestens einem der Port-Typen des RUGGEDCOM RX1400 kompatibel ist
- Es muss möglich sein, eine IP-Adresse und Netzmaske auf der Ethernet-Schnittstelle des Rechners zu konfigurieren
- Ein geeignetes Ethernet-Kabel
- Eine auf einem Rechner installierte SSH-Client-Anwendung

Zugriff auf Dokumentation

Die aktuelle Benutzerdokumentation für RUGGEDCOM ROX II v2.11 ist online abrufbar unter https://www.siemens.com/ruggedcom. Wenn Sie ein Benutzerdokument anfordern möchten bzw. Fragen dazu haben, wenden Sie sich bitte an den Siemens Kunden-Support.

Lizenzbedingungen

RUGGEDCOM ROX II enthält Open-Source-Software. Lesen Sie die Lizenzbedingungen für Open-Source-Software sorgfältig durch, bevor Sie mit diesem Produkt arbeiten.

Die Lizenzbedingungen sind in einem getrennten Dokument beschrieben, das über RUGGEDCOM ROX II erhältlich ist. Für den Zugriff auf die Lizenzbedingungen melden Sie sich bei RUGGEDCOM ROX II CLI an und geben den folgenden Befehl ein:

```
file show-license LicenseSummary.txt
```

Training

Siemens bietet ein umfangreiches Schulungsprogramm an, das vom Inhouse Training mit Standardkursen über Netzwerktechnologie, Ethernet Switches und Router bis hin zu individuellen Kursen beim Kunden reicht, die auf dessen Bedarf, Erfahrung und Anwendung abgestimmt sind.

Das Educational Services Team von Siemens vermittelt unseren Kunden die wesentlichen praktischen Fertigkeiten, damit sie über die erforderlichen Kenntnisse verfügen, um die verschiedenen Technologien zu verstehen, auf denen die Infrastruktur von Netzwerken für die geschäftskritische Kommunikation basiert.

Dank Siemens' einzigartigem Mix aus Sachkenntnissen im Bereich IT/Telekommunikation und dem in den Märkten Energieversorgung, Transport und Industrie erforderlichen Fachwissen kann Siemens ein auf die Anwendung des Kunden zugeschnittenes Training anbieten.

Weitere Informationen über das Trainingsangebot und die Verfügbarkeit von Kursen finden Sie unter https://www.siemens.com/ruggedcom oder wenden Sie sich an einen Siemens-Vertriebshändler.

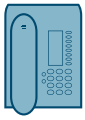
Kundensupport

Der Kundensupport steht allen Siemens-Kunden 24 Stunden am Tag und 7 Tage die Woche zur Verfügung. Falls Sie technische Unterstützung oder allgemeine Informationen benötigen, können Sie den Siemens Kundensupport über die folgenden Kanäle kontaktieren:



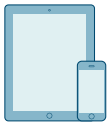
Online

Besuchen Sie http://www.siemens.com/automation/support-request, um eine Supportanfrage (SR) einzureichen oder den Status einer offenen Anfrage einzusehen.



Telefon

Rufen Sie ein Hotline-Zentrum in Ihrer Nähe an, um eine Supportanfrage (SR) zu stellen. Hier finden Sie ein Hotline-Zentrum in Ihrer Nähe: http://www.automation.siemens.com/mcms/aspa-db/de/automatisierungstechnik/Seiten/default.aspx .



Mobilgeräte-App

Installieren Sie die Industry Online Support-App der Siemens AG auf Ihrem Mobilgerät (Betriebssystem Android, Apple iOS oder Windows) und:

- Greifen Sie auf die umfangreiche Bibliothek von Siemens mit Hilfe-Dokumentationen einschließlich FAQs und Handbüchern zu.
- Reichen Sie eine Supportanfrage (SR) ein oder sehen Sie den Status einer offenen Anfrage ein.
- Kontaktieren Sie einen lokalen Siemens-Vertreter aus den Abteilungen Vertrieb, Technischer Support, Schulung usw.
- Stellen Sie Fragen oder teilen Sie Ihr Wissen mit anderen Kunden von Siemens und den Support-Mitarbeitern.

1 Einleitung

Willkommen beim RUGGEDCOM ROX II (Rugged Operating System für Linux®) v2.11 Benutzerhandbuch CLI für RUGGEDCOM RX1400. Dieses Dokument beschreibt, wie Sie RX1400 über RUGGEDCOM ROX II die Befehlszeilenschnittstelle (Command Line Interface, CLI) konfigurieren können. RUGGEDCOM ROX II enthält eine Webschnittstelle, die in einem eigenen Benutzerhandbuch CLI beschrieben ist.

WICHTIG!
Dieser Benutzerhandbuch CLI beschreibt alle Merkmale vonRUGGEDCOM ROX II, einige Funktionen können jedoch nur über die Webschnittstelle konfiguriert werden. Dies wird ggf. im Benutzerhandbuch CLI entsprechend vermerkt.

INHALT

- Abschnitt 1.1, „Produktmerkmale und Vorteile“
- Abschnitt 1.2, „Feature Keys“
- Abschnitt 1.3, „Sicherheitsempfehlungen“
- Abschnitt 1.4, „Am Port verfügbare Dienste“
- Abschnitt 1.5, „Benutzerberechtigungen“
- Abschnitt 1.6, „Entnehmbarer Speicher“

Abschnitt 1.1

Produktmerkmale und Vorteile

Im Folgenden werden die zahlreichen in RUGGEDCOM ROX II verfügbaren Produktmerkmale und ihre jeweiligen Vorteile beschrieben:

- **Cyber-Sicherheit**
  Cyber-Sicherheit ist ein wichtiges Thema in vielen Branchen, in denen Automatisierungs- und Kommunikationsnetzwerke eine Schlüsselrolle für aufgabenkritische Anwendungen spielen und hohe Zuverlässigkeit von überragender Bedeutung ist. Zu den wesentlichen Produktmerkmalen in RUGGEDCOM ROX II, die sich den Sicherheitsbedrohungen auf der Ebene lokaler Netzwerke widmen, gehören:

Passwörter	Mehrstufige Benutzerpasswörter schützen vor unbefugter Konfiguration
SSH/SSL	Erweitert den Passwortschutz um die Möglichkeit, Passwörter und Daten bei der Übertragung innerhalb des Netzwerks zu verschlüsseln
Ports aktivieren/deaktivieren	Möglichkeit der Deaktivierung von Ports zum Unterbinden des Datenverkehrs
802.1Q VLAN	Bietet die logische Trennung des Datenverkehrs zwischen an Switches befindlichen vordefinierten Ports
SNMPv3	Verschlüsselte Authentifizierung und Zugriffssicherheit

HTTPS	Sicherer Zugriff auf die Webschnittstelle
Firewall	Eine integrierte zustandsorientierte Firewall gewährleistet geschützte Netzwerkzonen
VPN/IPSEC	Ermöglicht die Erstellung sicherer verschlüsselter und authentifizierter Tunnel

- **Enhanced Rapid Spanning Tree Protocol (eRSTP)™**
  Das eRSTP von Siemens ermöglicht die Erstellung fehlertoleranter Ring- und Maschennetzwerke, die redundante Links einbinden, welche *zurückgeschnitten* werden, um Schleifen zu verhindern. Durch das eRSTP werden sowohl STP als auch RSTP implementiert, um im Gegensatz zu anderen proprietären *Ring*-Lösungen die Interoperabilität mit herkömmlichen Switches zu fördern. Die Fast-Root-Failover-Funktion von eRSTP sorgt in einer Maschentopologie bei einem Ausfall der RSTP-Root-Bridge für schnelle Netzwerkkonvergenz.
- **Dienstgüte (Quality of Service, IEEE 802.1p):**
  Einige Netzwerkanwendungen wie Echtzeitsteuerung oder VoIP (Voice over IP) benötigen vorhersagbare Ankunftszeiten für Ethernet-Frames. Switches können bei starkem Netzwerkverkehr aufgrund von internen Warteschlangen, die Frames puffern und sie dann in der Reihenfolge, in der sie eingegangen sind, übermitteln, Latenz verursachen. RUGGEDCOM ROX II unterstützt *Berechtigungsklassen*, die es zeitkritischem Datenverkehr ermöglichen, an den Anfang der Warteschlange zu springen, was wiederum Latenz minimiert und *Jitter* reduziert, damit solche anspruchsvollen Anwendungen korrekt betrieben werden können. RUGGEDCOM ROX II ermöglicht die Klassifizierung der Priorität nach Port, Tags, MAC-Adresse oder IP-ToS (Type of Service). Ein konfigurierbarer Algorithmus nach der Methode *Weighted Fair Queuing* steuert, in welcher Reihenfolge die Frames die Warteschlangen verlassen.
- **VLAN (IEEE 802.1Q)**
  Virtual Local Area Networks (VLAN) ermöglichen die Unterteilung eines physischen Netzwerks in einzelne logische Netzwerke mit unabhängigen Broadcast-Domänen. Eine Sicherheitsmaßnahme wird dadurch bereitgestellt, dass Hosts nur auf andere Hosts im selben VLAN zugreifen können und Traffic-Stürme isoliert werden. RUGGEDCOM ROX II unterstützt nach 802.1Q getaggte Ethernet-Frames und VLAN-Trunks. Durch die portbasierte Klassifizierung können Legacy-Geräte dem korrekten VLAN zugeordnet werden. Ferner wird GVRP unterstützt, um die Konfiguration der Switches im VLAN zu vereinfachen.
- **Simple Network Management Protocol (SNMP)**
  SNMP bietet ein standardisiertes Verfahren für Netzwerkmanagementstationen, um Geräte unterschiedlicher Hersteller abzufragen. RUGGEDCOM ROX II unterstützt v1, v2c und v3. Im Allgemeinen wird SNMPv3 empfohlen, da es Sicherheitsfunktionen (wie Authentifizierung, Datenschutz und Zugriffskontrolle) umfasst, die in früheren SNMP-Versionen nicht vorhanden sind.

  RUGGEDCOM ROX II unterstützt auch zahlreiche Standard-MIBs (Management Information Base) für die einfache Anbindung an jedes beliebige Network Management System (NMS). Eine von RUGGEDCOM ROX II unterstützte Funktion von SNMP ist die Möglichkeit, bei Systemereignissen *Traps* zu erstellen. RUGGEDCOM NMS, die Managementlösung von Siemens, kann Traps mehrerer Geräte aufzeichnen und stellt somit ein leistungsstarkes Werkzeug für die Fehlerbehebung im Netzwerk dar. Das Tool stellt ferner eine grafische Visualisierung des Netzwerks bereit und lässt sich vollständig in alle anderen Produkte von Siemens integrieren.
- **Fernüberwachung und Fernkonfiguration mit RUGGEDCOM NMS**
  RUGGEDCOM NMS (RNMS) ist das Netzwerkmanagementsystem von Siemens für die Erkennung, Überwachung und Verwaltung von RUGGEDCOM-Produkten und anderen IP-fähigen Geräten in einem Netzwerk. Dieses hoch konfigurierbare, voll umfängliche Produkt erfasst und meldet die Verfügbarkeit und Leistung von Netzwerkkomponenten und -diensten. Geräte-, Netzwerk- und Dienstausfälle werden schnell erkannt und gemeldet, um Ausfallzeiten zu verringern.

  RNMS eignet sich insbesondere für die Fernüberwachung und Fernkonfiguration von RUGGEDCOM Routern, Switches, seriellen Servern und WiMAX-Funknetzgeräten. Weitere Informationen erhalten Sie von einem Siemens-Vertriebsmitarbeiter.

- **NETCONF-Konfigurationsoberfläche**
  In der NETCONF-Konfigurationsoberfläche können Administratoren mithilfe von XML-basierten Befehlen Geräteparameter einstellen und Geräte-Updates empfangen. Dieser Standard, der von mehreren Herstellern unterstützt wird, ermöglicht die starke Vereinfachung der Aufgaben im Netzwerkmanagement.

  Weitere Informationen zur Verwendung von NETCONF für die Konfiguration von RUGGEDCOM ROX II finden Sie im *RUGGEDCOM RUGGEDCOM ROX II NETCONF-Referenzhandbuch* unter https://www.siemens.com/ruggedcom.
- **NTP (Network Time Protocol)**
  NTP synchronisiert automatisch die interne Uhr sämtlicher RUGGEDCOM ROX II-Geräte im Netzwerk. Hierdurch wird die Übereinstimmung zeitgestempelter Ereignisse für die Fehlerbehebung möglich.
- **Portratenbegrenzung**
  RUGGEDCOM ROX II unterstützt die konfigurierbare Ratenbegrenzung je Port, um den Unicast- und Multicast-Verkehr zu begrenzen. Dies kann für Dienstleistungsanbieter bei der Verwaltung wertvoller Netzwerkbandbreite entscheidend sein. Ferner wird Edge-Security für DoS-Angriffe (Denial of Service) geboten.
- **Filtern von Broadcast-Stürmen**
  Broadcast-Stürme verursachen verheerende Schäden im Netzwerk und können die Fehlfunktion angeschlossener Geräte auslösen. Dies kann in einem Netzwerk mit aufgabenkritischen Geräten katastrophal sein. RUGGEDCOM ROX II begrenzt dies durch die Filterung von Broadcast-Stürmen mit einem benutzerdefinierten Schwellwert.
- **Port-Spiegelung**
  RUGGEDCOM ROX II kann so konfiguriert werden, dass sämtlicher Datenverkehr eines Ports an einem dafür bestimmten Spiegelport dupliziert wird. In Kombination mit einem Netzwerkanalysator kann sich diese Funktion als leistungsstarkes Fehlerbehebungswerkzeug erweisen.
- **Portkonfiguration und -status**
  In RUGGEDCOM ROX II können Eigenschaften wie Geschwindigkeit, Duplex, Auto-Negotiation, Flusskontrolle und andere an einzelnen Ports *fest* konfiguriert werden. Dies ermöglicht die ordnungsgemäße Verbindung mit Geräten, die keine Negotiation betreiben oder ungewöhnliche Einstellungen haben. Ein ausführlicher Status von Ports mit Alarm- und SNMP-Trap hilft bei Verbindungsproblemen enorm zur Fehlerbehebung im System.
- **Portstatistik und RMON (Remote Monitoring)**
  RUGGEDCOM ROX II bietet kontinuierlich aktualisierte Statistiken für jeden Port mit Ingress- und Egress-Paket- und Byte-Zählern sowie ausführlichen Fehlerzahlen.

  Ferner werden RMON-Statistiken voll unterstützt. RMON ermöglicht eine äußerst moderne Datenerfassung, Analyse und Erkennung von Mustern im Datenverkehr.
- **Ereignisprotokollierung und Alarme**
  RUGGEDCOM ROX II erfasst alle signifikanten Ereignisse in einem nicht-flüchtigen Systemprotokoll und ermöglicht somit die forensische Fehlerbehebung. Zu den Ereignissen gehören Link-Ausfall und Link-Wiederherstellung, unbefugter Zugriff, Erkennung von Broadcast-Stürmen und Selbsttest-Diagnose. Die Alarme bieten eine Momentaufnahme neuester Ereignisse, die vom Netzwerkadministrator noch quittiert werden müssen. Bei Vorhandensein kritischer Alarme wird ein externes Hardware-Relais stromlos geschaltet, damit, wenn gewünscht, ein externer Controller reagieren kann.
- **HTML-Webbrowser-Benutzeroberfläche**
  RUGGEDCOM ROX II bietet eine einfache, intuitive Benutzeroberfläche für die Konfiguration und Überwachung über einen standardmäßigen grafischen Webbrowser oder über eine standardmäßige Telekom-Bedienoberfläche. Alle Systemparameter umfassen eine ausführliche Online-Hilfe für die einfache Einrichtung und Konfiguration. RUGGEDCOM ROX II zeigt sich in einer vertrauten Darstellung und bietet standardisierte Konfigurationsvorgänge, damit eine einfache Migration zu anderen von RUGGEDCOM verwalteten Produkten möglich ist.

- **Befehlszeilenschnittstelle (Command Line Interface, CLI)**
  Eine Befehlszeilenschnittstelle in Verbindung mit Remote Shell wird verwendet, um Datenabruf, Konfigurations-Updates und Firmware-Upgrades zu automatisieren. Eine leistungsstarke Command Line Interface (CLI) im Stil des Telekomstandards gibt Expertenbenutzern die Möglichkeit, sämtliche Parameter, die das Gerät anbietet, selektiv abzurufen oder zu bearbeiten.
- **Link-Backup**
  Das Link-Backup ist eine leicht konfigurierbare Möglichkeit, bei Ausfall einer festgelegten Hauptverbindung eine Backup-Verbindung herzustellen. Bei den Haupt- und Backup-Verbindungen kann es sich um Ethernet oder Mobilfunk handeln. Die Funktion kann eine Sicherung an mehreren entfernten Standorten auslösen und mehrere Haupt-/ Backup-Verbindungsbeziehungen verwalten. Die Funktion kann auch einen permanenten Highspeed-WAN-Link in einem permanenten Lowspeed-WAN-Link sichern und kann dazu verwendet werden, die Standardroute von der Hauptverbindung zur Backup-Verbindung zu migrieren.
- **OSPF (Open Shortest Path First)**
  OSPF ist ein Routingprotokoll, das den besten Pfad für das Routing von IP-Verkehr über ein TCP/IP-Netzwerk basierend auf den Verbindungszuständen zwischen den Knoten sowie verschiedenen Qualitätsparametern bestimmt. OSPF ist ein Interior Gateway Protocol (IGP), das so aufgebaut ist, dass es innerhalb eines autonomen Systems arbeitet. Zudem handelt es sich um ein Verbindungsstatusprotokoll, was bedeutet, dass die beste Route anhand des Typs und der Geschwindigkeit der Verbindungen zwischen den Routern ermittelt wird und nicht anhand der Anzahl der Router-Hops, die zwischen den einzelnen Routern liegen (wie bei Distanzvektor-Routingprotokollen wie RIP).
- **BGP (Border Gateway Protocol)**
  BGPv4 ist ein Pfadvektor-Routingprotokoll, bei dem Routing-Entscheidungen anhand der vom Netzwerkadministrator vorgegebenen Richtlinien oder Regeln getroffen werden. Es wird typischerweise dann eingesetzt, wenn Netzwerke bei mehreren Internet-Serviceanbietern untergebracht sind, oder bei sehr großen internen Netzwerken, wo interne Gateway-Protokolle keine ausreichende Skalierung bieten.
- **RIP (Routing Information Protocol)**
  RIP Version 1 und Version 2 sind Distanzvektor-Routingprotokolle, die bei der Ermittlung des besten Routingpfads die Anzahl der Router-Hops auf 15 begrenzen. Dieses Protokoll wird üblicherweise bei kleinen, in sich geschlossenen Netzwerken eingesetzt, da jeder Router über 15 Hops hinaus als unerreichbar betrachtet wird.
- **IS-IS (Intermediate System - Intermediate System)**
  IS-IS ist ein Protokoll aus einer Suite von Routingprotokollen, das Routinginformationen unter den Routern freigeben soll. Die Aufgabe des Routers ist es, die effiziente Bewegung von Daten über manchmal komplexe Netzwerke zu ermöglichen. Die Routingprotokolle sind so aufgebaut, dass die Routinginformationen in diesen Netzwerken freigegeben werden, und sie verwenden moderne Algorithmen, um zu entscheiden, welches die kürzeste Route für die Informationen von Punkt A nach Punkt B ist. Eines der ersten Verbindungsstatus-Routingprotokolle war IS-IS. Es wurde 1985 entwickelt und 1998 von der ISO übernommen (ISO/IEC 10589:2002). Später wurde es als IETF-Standard (RFC 1142 [http://tools.ietf.org/html/rfc1142]) neu veröffentlicht.
- **Verhinderung von Brute-Force-Angriffen**
  Schutz vor Brute-Force-Angriffen (BFAs) gehört in RUGGEDCOM ROX II zum Standard. Wenn es ein externer Host nicht schafft, sich innerhalb einer vorgegebenen Anzahl von Versuchen an der CLI-, NETCONF- oder Webschnittstelle anzumelden, wird die IP-Adresse des Hosts eine Zeit lang gesperrt. Dieser Zeitraum wird verlängert, wenn die Anmeldung des Hosts bei nachfolgenden Versuchen erneut fehlschlägt.
- **Unterstützung für MicroSD/MicroSDHC**
  Verwenden Sie ein steckbares microSD- oder microSDHC-Flash-Laufwerk, um wichtige Dateien zu verwalten und RUGGEDCOM ROX II zu konfigurieren.
  - Upgrade/Downgrade von Firmware – Verwenden Sie das microSD- oder microSDHC-Flash-Laufwerk als tragbares Repository für neue oder Legacy-Versionen der RUGGEDCOM ROX II-Firmware.

- Dateien sichern – Konfigurieren Sie RUGGEDCOM ROX II so, dass wichtige Informationen auf dem microSD- oder microSDHC-Flash-Laufwerk gesichert werden, so z. B. Rollbacks, Protokolldateien, Feature Keys und Konfigurationsdateien.
- Dateien freigeben – Mit einem microSD/microSDHC-Flash-Laufwerk können Sie rasch andere RUGGEDCOM RX1400-Geräte konfigurieren oder schnell ein Upgrade durchführen.

WICHTIG!
Entfernen Sie das microSD- bzw. microSDHC-Flash-Laufwerk während einer Dateiübertragung nicht.

HINWEIS
Auf dem microSD/microSDHC-Flash-Laufwerk wird nur eine Partition unterstützt.

- **Unterstützung für virtuelle Maschinen**
  Verwenden Sie die integrierte Virtualisierungsumgebung, um ein Linux-Gastbetriebssystem und Fremdanwendungen auf dem Gerät auszuführen und dadurch Intelligenz am Netzwerkrand zu ermöglichen.

Abschnitt 1.2
Feature Keys

Feature Keys ergänzen eine vorhandene Installation des RUGGEDCOM ROX II um weitere Funktionen. Diese können zu einem beliebigen Zeitpunkt erworben und installiert werden.

Aktuell sind drei Feature Keys erhältlich: L2STD, L3STD und L3SEC. Jeder neue RX1400 wird standardmäßig mit einem Basis-Feature-Key ausgeliefert, der dauerhaft auf dem Gerät installiert ist. Zusätzliche Feature Keys können auf der microSD/microSDHC-Speicher gespeichert werden, um sie bei Bedarf auf andere Geräte zu übertragen.

HINWEIS
Jeder Feature Key wird mit der Seriennummer des Geräts signiert, in dem er verwendet werden soll. Feature Keys können in anderen RUGGEDCOM ROX II-Geräten verwendet werden, jedoch wird ein Alarm generiert, der auf eine Nichtübereinstimmung hinsichtlich der Hardware hinweist.

Feature Keys besitzen u.a. folgende Funktionen:

Funktion	Feature Key		
	Layer 2 Standard Edition (L2STD)	Layer 3 Standard Edition (L3STD)	Layer 3 Security Edition (L3SEC)
VLANs (802.1Q)	✓	✓	✓
QoS (802.1p)	✓	✓	✓
MSTP (802.1Q-2005)[a]	✓	✓	✓
RSTP	✓	✓	✓
eRSTP™	✓	✓	✓
NTP	✓	✓	✓
L2TPv2 und L2TPv3	✓	✓	✓
Portratenbegrenzung	✓	✓	✓
"Broadcast-Storm"-Filterung	✓	✓	✓

Funktion	Feature Key		
	Layer 2 Standard Edition (L2STD)	Layer 3 Standard Edition (L3STD)	Layer 3 Security Edition (L3SEC)
Port-Spiegelung	✓	✓	✓
SNMP v1/v2/v3	✓	✓	✓
RMON	✓	✓	✓
CLI	✓	✓	✓
HTML-Benutzeroberfläche	✓	✓	✓
MPLS	×	✓	✓
DHCP	×	✓	✓
VRRPv2 und VRRPv3	×	✓	✓
PIM-SM	×	✓	✓
Firewall	×	✓	✓
OSPF	×	✓	✓
BGP	×	✓	✓
RIP v1/v2	×	✓	✓
IS-IS	×	✓	✓
Datenverkehrspriorisierung	×	✓	✓
VPN	×	×	✓
IPSec	×	×	✓
Virtualisierung	✓	✓	✓

[a] *Vormals 802.1s*

Informationen über das Installieren und Anzeigen von Feature Keys finden Sie in Abschnitt 4.11, „Verwalten von Feature Keys“.

Abschnitt 1.3

Sicherheitsempfehlungen

Um unbefugten Zugriff auf das Gerät zu verhindern, beachten Sie die folgenden Sicherheitsempfehlungen:

» Authentifizierung

ACHTUNG!
Zugriffsrisiko - Gefahr von Datenverlust. Verlegen Sie nicht die Passwörter für das Gerät. Wenn Sie sowohl das Wartungs- als auch das Boot-Passwort verlegen, muss das Gerät zur Reparatur an Siemens Canada Ltd eingesendet werden. Diese Dienstleistung fällt nicht unter die Gewährleistung. Je nach Maßnahme, die erforderlich ist, um den Zugriff auf das Gerät wiederherzustellen, können Daten verloren gehen.

- Ändern Sie die Standard-Passwörter für alle Benutzerkonten, Zugriffsarten (z. B. Wartungsbetrieb) und Prozesse (sofern zutreffend), bevor das Gerät bereitgestellt wird.
- Verwenden Sie starke Passwörter. Vermeiden Sie schwache Passwörter (z. B. *Passwort1*, *123456789*, *abcdefgh*) oder wiederholte Zeichen (z. B. *abcabc*). Weitere Informationen zum Erstellen starker Passwörter finden Sie in den Voraussetzungen für Passwörter unter Abschnitt 5.8, „Verwalten von Passwörtern und Passphrasen“.

  Diese Empfehlung gilt auch für auf dem Gerät konfigurierte Pre-Shared Keys (PSK).
- Achten Sie darauf, Ihre Passwörter zu schützen, und teilen Sie sie keinen unbefugten Personen mit.
- Verwenden Sie nicht für mehrere Benutzernamen und Systeme die gleichen Passwörter und verwenden Sie die Passwörter nach ihrem Ablauf nicht erneut.
- Bewahren Sie Passwörter an einem sicheren Ort auf, damit Sie sie bei Verlust zur Hand haben.
- Wenn die RADIUS oder TACACS+ Benutzerauthentifizierung entfernt ausgeführt wird, vergewissern Sie sich, dass sämtliche Kommunikation innerhalb des Sicherheitsumfelds oder auf einem sicheren Kanal durchgeführt wird.
- TACACS+ verwendet den MD5-Algorithmus für die Key-Verschlüsselung. Achten Sie darauf, dass Sie die Sicherheitsempfehlungen in der Benutzeranleitung befolgen und die Umgebung entsprechend den Best Practices für *Defense-in-Depth* einrichten.
- PAP (Password Authentication Protocol) gilt nicht als sicheres Protokoll und sollte nur, wenn erforderlich, aktiviert werden. Verwenden Sie nach Möglichkeit CHAP (Challenge-Handshake Authentication Protocol).
- Für erhöhte Sicherheit verwenden Sie IPsec in Verbindung mit dem L2TP-Protokoll.

» Physischer/entfernter Zugriff

- Es ist unbedingt empfehlenswert, den Schutz vor Brute-Force-Angriffen (BFA) aktiviert zu lassen, um zu verhindern, dass sich Dritte unbefugten Zugriff auf das Gerät verschaffen. Weitere Informationen finden Sie unter Abschnitt 6.3, „Schutz vor Brute-Force-Angriffen aktivieren/deaktivieren“.
- SSH- und SSL-Schlüssel stehen Benutzern zur Verfügung, die sich über die serielle Konsole mit dem Gerät verbinden. Achten Sie darauf, dass Sie angemessene Sicherheitsvorkehrungen ergreifen, wenn Sie das Gerät außerhalb der vertrauten Umgebung versenden:
  - Ersetzen Sie die SSH- und SSL-Schlüssel vor dem Versand mit *Wegwerf*-Schlüsseln.
  - Nehmen Sie die vorhandenen SSH- und SSL-Schlüssel außer Betrieb. Erstellen und programmieren Sie bei Rückkehr des Geräts neue Schlüssel für das Gerät.
- Ersetzen Sie alle standardmäßigen und automatisch generierten SSL-Zertifikate mit von einer vertrauenswürdigen Zertifikatstelle (CA) signierten Zertifikaten und Schlüsseln. Standardmäßig und automatisch generierte Zertifikate sind von RUGGEDCOM ROX II selbst signiert.
- Beschränken Sie den physischen Zugriff auf das Gerät ausschließlich auf vertrauenswürdiges Personal. Eine Person mit bösartigen Absichten, die im Besitz der Flash-Karte ist, könnte kritische Informationen wie Zertifikate, Schlüssel usw. extrahieren (Benutzerpasswörter sind durch Hash-Codes geschützt) oder die Karte neu programmieren.
- Passwörter/Passphrasen für Servicebetrieb und Wartungsbetrieb sollten nur einer begrenzten Anzahl vertrauenswürdiger Benutzer mitgeteilt werden. Diese Betriebsarten bieten Zugriff auf private Schlüssel und Zertifikate.
- Kontrollieren Sie den Zugriff auf die serielle Konsole in dem gleichen Umfang wie jeden physischen Zugriff auf das Gerät. Der Zugriff auf die serielle Konsole ermöglicht unter Umständen den Zugriff auf den BIST-Modus, der über Tools verfügt, die dazu verwendet werden können, sich vollständigen Zugriff auf das Gerät zu verschaffen.
- Bei der Verwendung von SNMP (Simple Network Management Protocol):

  - Begrenzen Sie die Anzahl der IP-Adressen, die eine Verbindung zum Gerät herstellen können, und ändern Sie die Community-Namen. Konfigurieren Sie SNMP außerdem so, dass bei Authentifizierungsfehlern ein Trap erstellt wird. Weitere Informationen finden Sie unter Abschnitt 14.2, „Verwalten von SNMP“.
  - Achten Sie darauf, dass die Standard-Community-Strings in eindeutige Werte geändert werden.
- Achten Sie bei Verwendung von RUGGEDCOM ROX II als Client für eine sichere Verbindung mit einem Server (beispielsweise für ein sicheres Upgrade oder eine sichere Syslog-Übertragung) darauf, dass serverseitig starke Verschlüsselungsverfahren und Protokolle konfiguriert sind.
- Begrenzen Sie die maximale Anzahl gleichzeitig zulässiger Webserver-, CLI-, SFTP- und NETCONF-Sitzungen.
- Wenn eine Firewall erforderlich ist, konfigurieren und starten Sie die Firewall, bevor Sie das Gerät mit einem öffentlichen Netzwerk verbinden. Vergewissern Sie sich, dass die Firewall so konfiguriert ist, dass sie Verbindungen einer spezifischen Domäne akzeptiert. Weitere Informationen finden Sie unter Abschnitt 6.7, „Verwalten von Firewalls“.
- Modbus ist in RUGGEDCOM ROX II standardmäßig deaktiviert. Wenn Modbus erforderlich ist, vergewissern Sie sich, dass Sie die Sicherheitsempfehlungen im Benutzerhandbuch CLI befolgen und die Umgebung entsprechend den Best Practices für Defense-in-Depth einrichten.
- Konfigurieren Sie die sichere Protokollierung des entfernten Systems, um alle Protokolle an einen zentralen Ort weiterzuleiten. Weitere Informationen finden Sie unter Abschnitt 4.13, „Verwalten von Protokollen“.
- Konfigurationsdateien werden für die einfache Verwendung entweder im NETCONF- oder im CLI-Format zur Verfügung gestellt. Vergewissern Sie sich, dass die Konfigurationsdateien angemessen geschützt sind, wenn sie außerhalb des Geräts vorhanden sind. Verschlüsseln Sie die Dateien beispielsweise, speichern Sie sie an einem sicheren Ort und übertragen Sie sie nicht über unsichere Kommunikationskanäle.
- Es ist unbedingt empfehlenswert, kritische Anwendungen auf private Netzwerke zu begrenzen oder sie zumindest nur über sichere Dienste wie IPsec verfügbar zu machen. Die Verbindung eines RUGGEDCOM ROX II-Geräts mit dem Internet ist möglich. Es ist jedoch allergrößte Sorgfalt geboten, um das Gerät und das Netzwerk dahinter mit sicheren Maßnahmen wie einer Firewall oder IPsec zu schützen. Nähere Informationen zum Konfigurieren von Firewalls und IPsec finden Sie unter Abschnitt 6.7, „Verwalten von Firewalls“ und Abschnitt 11.8, „IPsec-Tunnel verwalten“.
- Die Verwaltung der Zertifikate und Schlüssel liegt in der Verantwortung des Gerätebesitzers. Ziehen Sie die Verwendung von RSA-Schlüsselgrößen mit einer Länge von 2048 Bits für erhöhte kryptografische Stärke in Betracht. Bevor Sie das Gerät zur Reparatur an Siemens Canada Ltd einsenden, ersetzen Sie die aktuellen Zertifikate und Schlüssel mit temporären *Wegwerf*-Zertifikaten und Schlüsseln, die bei Rückgabe des Geräts vernichtet werden können.
- Achten Sie auf mögliche nicht sichere Protokolle, die im Gerät aktiviert sind. Während einige Protokolle wie HTTPS, SSH und 802.1x sicher sind, sind andere wie etwa Telnet und RSTP nicht für diesen Zweck ausgelegt. Um den unbefugten Zugriff auf das Gerät/Netzwerk zu verhindern, sind geeignete Sicherheitsmaßnahmen gegen nicht sichere Protokolle zu treffen.
- Vergewissern Sie sich, dass das Gerät vollständig außer Betrieb gesetzt wurde, bevor Sie es aus dem Betrieb nehmen. Weitere Informationen finden Sie unter Abschnitt 4.8, „Außerbetriebnahme des Geräts“.
- Konfigurieren Sie Port-Sicherheitsfunktionen an Zugriffsports, um zu verhindern, dass unbefugte Dritte eine physische Verbindung zum Gerät herstellen. Weitere Informationen finden Sie unter Abschnitt 6.4.2, „Konfigurieren der Port-Sicherheit“.
- Achten Sie auf unsichere WLAN-Protokolle wie Open und WEP. Verwenden Sie bei Einsatz von WLAN nur sichere Protokolle wie Wi-Fi Protected Access 2 (WPA2).

Virtualisierung

- Die Integrität jedes auf einer virtuellen Maschine installierten Betriebssystems muss vom Benutzer vor der Nutzung überprüft werden und alle relevanten Sicherheits-Patches müssen installiert sein. Das installierte Betriebssystem liegt in der Verantwortung des Benutzers und nicht von Siemens Canada Ltd.
- Vergewissern Sie sich, dass alle Dateien im Image einer virtuellen Maschine frei von bösartigen Inhalten und bösartigem Code sind. Schnittstellen, die die virtuelle Maschine mit dem Internet verbinden, müssen unter Berücksichtigung der Best Practices für Sicherheitsmaßnahmen geschützt werden.
- Verwenden Sie ein VLAN oder einen physischen Port – einen anderen als den RUGGEDCOM ROX II-Management-Port – um auf einer virtuellen Maschine auf eine Bridge-Schnittstelle zuzugreifen. Der für den Zugriff auf die virtuelle Maschine verwendete Port sollte sich in einem getrennten VLAN befinden.

Hardware/Software

ACHTUNG!
Konfigurationsgefahr - Gefahr der Datenbeschädigung. Der Wartungsmodus dient zur Fehlersuche und sollte nur von Siemens Canada Ltd-Technikern verwendet werden. Daher ist dieser Modus nicht vollständig dokumentiert. Eine falsche Anwendung der in diesem Wartungsmodus verfügbaren Befehle kann den Betriebszustand des Geräts beschädigen und es unzugänglich machen.

- Vergewissern Sie sich, dass die neueste Firmware-Version einschließlich aller sicherheitsbezogenen Patches installiert ist. Aktuelle Informationen zu Sicherheits-Patches für Siemens-Produkte finden Sie auf der Industrial Security Website [http://www.industry.siemens.com/topics/global/de/industrial-security/news-alerts/Seiten/alerts.aspx] oder der ProductCERT Security Advisories Website [http://www.siemens.com/innovation/de/technologiefokus/siemens-cert/cert-security-advisories.htm]. Updates für Siemens Product Security Advisories sind durch Anmelden beim RSS-Feed auf der Siemens ProductCERT Security Advisories Website oder durch Folgen von @ProductCert auf Twitter erhältlich.
- Aktivieren Sie nur die Dienste, die auf dem Gerät verwendet werden, einschließlich physischer Ports. Freie physische Ports können potenziell dazu verwendet werden, Zugriff auf das Netzwerk hinter dem Gerät zu erlangen.
- Für optimale Sicherheit verwenden Sie SNMPv3, wann immer möglich, und nutzen starke Passwörter.

Richtlinien

- Überprüfen Sie regelmäßig das Gerät, um sicherzustellen, dass diese Empfehlungen und/oder sämtliche internen Sicherheitsrichtlinien erfüllt werden.
- Überprüfen Sie die Benutzerdokumentation anderer Siemens-Produkte, die zusammen mit dem Gerät verwendet werden, nach weiteren Sicherheitsempfehlungen.

Abschnitt 1.4

Am Port verfügbare Dienste

Die folgende Tabelle führt die vom Gerät zur Verfügung gestellten Dienste, einschließlich folgender Informationen, auf:

- **Dienste**
  Der vom Gerät unterstützte Dienst

- **Portnummer**
  Die mit dem Dienst verbundene Portnummer
- **Port offen**
  Der Zustand des Ports; entweder er ist immer offen und kann nicht geschlossen werden, oder er ist nur offen und kann konfiguriert werden.
- **Port-Standard**
  Der voreingestellte Zustand des Ports (d.h. offen oder geschlossen)
- **Zugriff autorisiert**
  Gibt an, ob die Ports/Dienste während des Zugriffs authentifiziert werden

Dienste	Portnummer	Port offen	Port-Standard	Zugriff autorisiert
SSH	TCP/22	Offen (falls mit Login konfiguriert)	Offen	Ja
SSH (Servicemodus)	TCP/222	Offen (falls mit Login konfiguriert)	Geschlossen	Ja
NETCONF	TCP/830	Offen (falls mit Login konfiguriert)	Offen	Ja
SFTP	TCP/2222	Offen (falls mit Login konfiguriert)	Geschlossen	Ja
HTTP	TCP/80	Offen (falls mit Login konfiguriert)	Offen	-/-
NTP	UDP/123	Offen (falls konfiguriert)	Geschlossen	Nein
SNMP	UDP/161	Offen (falls mit Login konfiguriert)	Geschlossen	Ja
HTTPS	TCP/443	Offen (falls mit Login konfiguriert)	Offen	Ja
TCP Modbus	TCP/502	Offen (falls konfiguriert)	Geschlossen	Nein
IPSec IKE	UDP/500	Offen (falls konfiguriert)	Geschlossen	Ja
IPSec NAT-T	UDP/4500	Offen (falls konfiguriert)	Geschlossen	Ja
DNPv3	TCP/20000	Offen (falls konfiguriert)	Geschlossen	Nein
RawSocket	TCP/konfiguriert	Offen (falls konfiguriert)	Geschlossen	Nein
DHCP Agent	UDP/67	Offen (falls konfiguriert)	Geschlossen	Nein
DHCP Server	UDP/67 hörend, 68 antwortend	Offen (falls konfiguriert)	Geschlossen	Nein
RADIUS	UDP/1812 zum Senden, öffnet zufälligen Port zum Hören	Offen (falls konfiguriert)	Geschlossen	Ja
TACACS+	TCP/49 zum Senden, öffnet zufälligen Port zum Hören	Offen (falls konfiguriert)	Geschlossen	Ja
L2TP	Zufälliger Port	Offen (falls konfiguriert)	Geschlossen	Ja
BGP	TCP/179	Offen (falls konfiguriert)	Geschlossen	Nein
RIP	UDP/520	Offen (falls konfiguriert)	Geschlossen	Nein
MPLS-Ping	UDP/3503	Offen (falls konfiguriert)	Geschlossen	Nein
LDP	TCP/646 und UDP/646	Offen (falls konfiguriert)	Geschlossen	Nein
L2TPv3	UDP/1701	Offen (falls konfiguriert)	Geschlossen	Nein

Abschnitt 1.5

Benutzerberechtigungen

In der folgenden Tabelle werden die Bedien-, Konfigurations- und Aktionsbefehle aufgeführt, die Administrator-, Bediener- und Gast-Benutzer ausführen dürfen.

Arten des Benutzerzugriffs:

- **Erstellen (Create, C)** - kann optionale Parameter erstellen und entfernen
- **Ausführen (Execute, E)** - kann eine Aktion oder einen Befehl ausführen
- **Nein/No** - kein Zugriff
- **Lesen (Read, R)** - Lesezugriff
- **Aktualisieren (Update, U)** - kann vorhandene Parameter ändern

Zulässige Befehle/Pfade	Zugriff			Hinweise
	Administrator	Bediener	Gast	
config private | exclusive | no-confirm	Zulässig	Zulässig	Nein	
/admin/software-upgrade	R/U	R	Nein	
/admin/rox-imaging	R/U	R	Nein	
/admin/authentication	R/U	Nein	Nein	
/admin/authentication/password-complexity	R/U	Nein	Nein	
/admin/logging	C/R/U	Nein	Nein	
/admin/alarms (Status)	R	R	Nein	Administrator und Bediener können den Status von active-alarms sehen, Alarme quittieren und löschen
/admin/alarms-config/	R/U	R/U	Nein	Administrator und Bediener können Alarmlisten weder erstellen noch löschen
/admin/users	C/R/U	Nein	Nein	
/admin/users/userid	R/U	R/U	Nein	Der Bediener kann nur das eigene Passwort ändern und keine Benutzer erstellen.
/admin/cli	R/U	R/U	Nein	
/admin/snmp	C/R/U	Nein	Nein	
/admin/netconf	R/U	Nein	Nein	
/admin/dns	C/R/U	Nein	Nein	
/admin/webui	R/U	R/U	Nein	
/admin/scheduler	C/R/U	Nein	Nein	
/admin/contact	R/U	Nein	Nein	
/admin/hostname	R/U	Nein	Nein	
/admin/location	R/U	Nein	Nein	
/admin/session-limits	R/U	Nein	Nein	

Zulässige Befehle/Pfade	Zugriff			Hinweise
	Administrator	Bediener	Gast	
/admin/session-security	R/U	Nein	Nein	
/admin/sftp	R/U	Nein	Nein	
/admin/time (Status)	R	R	Nein	
/admin/switch-config (Status)	R/U	R	Nein	
/admin/system	R/U	Nein	Nein	
/admin/system-name	R/U	Nein	Nein	
/admin/timezone	R/U	Nein	Nein	
/admin/clear-all-alarms (Aktion)	E	C/R/U	Nein	
/admin/backup-files (Aktion)	E/R/U	Nein	Nein	
/admin/delete-all-ssh-known-hosts (Aktion)	E	Nein	Nein	
/admin/delete-logs (Aktion)	E	Nein	Nein	
/admin/delete-ssh-known-host (Aktion)	E	Nein	Nein	
/admin/full-configuration-load (Aktion)	E/U	Nein	Nein	
/admin/full-configuration-save (Aktion)	E/U	Nein	Nein	
/admin/install-files (Aktion)	E/U	Nein	Nein	
/admin/reboot (Aktion)	E	E	Nein	
/admin/restore-factory-defaults (Aktion)	E/U	Nein	Nein	
/admin/set-system-clock (Aktion)	E/U	Nein	Nein	
/admin/shutdown (Aktion)	E	E	Nein	
/apps	C/R/U	C/R/U	R	
/chassis/part-list	R/U	R	R	
/chassis/fixed-modules	C/R/U	Nein	R	
/chassis/line-module-list	R/U	R	R	
/chassis/line-modules/line-module	R/U	Nein	R	
/interfaces	R	C/R/U	R	
/interface	C/R/U	R/U	R	
/routing	C/R/U	C/R/U	R	
/routing/dynamic/ospf/interface	C/R/U	C/R/U	R	
/routing/dynamic/rip/interface	C/R/U	C/R/U	R	
/routing/multicast/dynamic/pim-sm/interface	C/R/U	C/R/U	R	
/routing/dynamic/isis/interface	C/R/U	C/R/U	R	
/security/firewall	C/R/U	C/R/U	R	

Zulässige Befehle/Pfade	Zugriff			Hinweise
	Administrator	Bediener	Gast	
/security/crypto	C/R/U	R	R	
/security/crypto/private-key	C/R/U	Nein	Nein	
/services	C/R/U	C/R/U	R	
/services/time/ntp/key/	C/R/U	Nein	Nein	
/tunnel/ipsec	C/R/U	Nein	Nein	
/ip	C/R/U	C/R/U	R	
/mpls	C/R/U	C/R/U	R	
/mpls/interface-mpls	C/R/U	C/R/U	R	
/mpls/ldp/interface-ldp	C/R/U	C/R/U	R	
/switch	C/R/U	C/R/U	R	
/switch/vlans/all-vlans	C/R/U	C/R/U	R	
/switch/port-security	R/U	Nein	Nein	
/qos	C/R/U	C/R/U	R	
/global	C/R/U	Nein	Nein	
hints	E	E	E	
monitor	E	E	Nein	
mpls-ping	E	E	Nein	
mpls-traceroute	E	E	Nein	
ping	E	E	Nein	
ping6	E	E	Nein	
reportstats	E	E	Nein	
ssh	E	Nein	Nein	
tcpdump	E	E	Nein	
telnet	E	E	Nein	
traceroute	E	E	Nein	
traceroute6	E	E	Nein	
traceserial	E	E	Nein	
wizard	E	Nein	Nein	

Abschnitt 1.6

Entnehmbarer Speicher

Der RUGGEDCOM RX1400 ist mit einem für den Benutzer zugänglichen Speichersteckplatz ausgestattet, der einen microSD- oder microSDHC-Flash-Speicher unterstützt. Der Speicher kann zum Verwalten von Konfigurations-, Firmware- oder sonstigen Dateien auf dem Gerät oder einer Geräteflotte verwendet werden.

- Upgrade/Downgrade der Firmware – Verwenden Sie den microSD- oder microSDHC-Flash-Speicher als tragbares Repository für neue oder alte Versionen der RUGGEDCOM ROX II-Firmware.
- Sichern von Dateien – Konfigurieren Sie den RUGGEDCOM ROX II so, dass er wichtige Informationen auf dem microSD- oder microSDHC-Flash-Speicher (z. B. Rollbacks, Protokolldateien, Feature Keys und Konfigurationsdateien) sichert.
- Teilen von Dateien – Konfigurieren oder upgraden Sie andere RUGGEDCOM RX1400-Geräte, indem Sie Dateien mithilfe desselben microSD-/microSDHC-Flash-Speicher kopieren.

WICHTIG!
Entfernen Sie den microSD- oder microSDHC-Flash-Speicher nicht während einer Dateiübertragung.

HINWEIS
Nur eine Partition wird auf dem microSD-/microSDHC-Flash-Speicher unterstützt.

Nur folgende Dateisysteme werden auf dem microSD-/microSDHC-Flash-Speicher unterstützt: VFAT (empfohlen), ext2, ext3, ext4, FAT16 oder FAT32. Der Vorteil bei der Verwendung dieser Dateisystemtypen für den entnehmbaren Speicher besteht darin, dass deren Inhalt auf jedem beliebigen Computer mit microSD/microSDHC-Schnittstelle geändert werden kann.

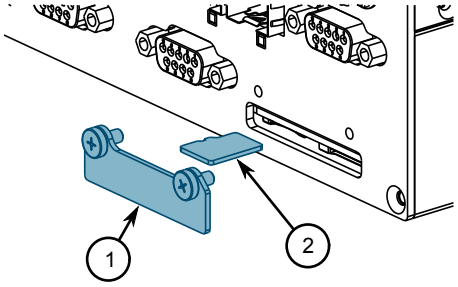


Abbildung 1: Installation der Speicherkarte

1. Abdeckplatte **2.** microSD-/microSDHC-Flash-Speicher

Informationen zum Installieren oder Entfernen des microSD-/microSDHC-Flash-Speicher finden Sie in der *Installationsanleitung* zum RUGGEDCOM RX1400.

2 Mit RUGGEDCOM ROX II arbeiten

Dieses Kapitel beschreibt, wie Sie die RUGGEDCOM ROX II-Schnittstelle verwenden können.

INHALT

- Abschnitt 2.1, „Voreingestellte Benutzernamen und Passwörter“
- Abschnitt 2.2, „Anmelden“
- Abschnitt 2.3, „Abmelden“
- Abschnitt 2.4, „Mit den Netzwerkdienstprogrammen arbeiten“
- Abschnitt 2.5, „Mit der Befehlszeilenschnittstelle arbeiten“
- Abschnitt 2.6, „Konfigurieren der CLI-Schnittstelle“
- Abschnitt 2.7, „Auf die verschiedenen Modi zugreifen“

Abschnitt 2.1

Voreingestellte Benutzernamen und Passwörter

Die folgenden voreingestellten Passwörter sind auf dem Gerät für jede Zugriffsart vorkonfiguriert:

ACHTUNG!
Sicherheitsgefahr – Risiko eines unberechtigten Zugriffs und/oder einer unberechtigten Nutzung
Um einen unbefugten Zugriff auf das Gerät zu verhindern, ändern Sie vor der Inbetriebnahme des Geräts die voreingestellten Passwörter. Für weitere Informationen siehe Abschnitt 5.8, „Verwalten von Passwörtern und Passphrasen“.

WICHTIG!
Die für die Zugriffsarten Administrator und Bediener voreingestellten Passwörter gelten nicht für WLAN-fähige Geräte, die zur Nutzung in den USA zertifiziert sind. In Übereinstimmung mit den FCC-Vorschriften sind diese voreingestellten Passwörter ausschließlich direkt von Siemens erhältlich. Nach der ersten Nutzung und vor der Inbetriebnahme können und sollten diese Passwörter geändert werden, um unberechtigten Zugriff zu verhindern.

Für weitere Informationen darüber, wie Sie die voreingestellten Passwörter für WLAN-fähige Geräte erhalten, wenden Sie sich an den Siemens-Kundensupport.

Modus	Benutzername	Passwort
Service	root	admin
Wartung	root	admin
Administrator	admin	admin
Bediener	oper	oper

Modus	Benutzername	Passwort
Gast	guest	guest

Abschnitt 2.2
Anmelden

Um sich bei RUGGEDCOM ROX II anzumelden, gehen Sie wie folgt vor:

1. Stellen Sie eine Verbindung zum Gerät her. Weitere Informationen über verschiedene Verfahrensweisen zum Herstellen einer Verbindung zum Gerät finden Sie in Abschnitt 3.1, „Verbindung mit RUGGEDCOM ROX II herstellen “.
2. Sobald die Verbindung zum Gerät hergestellt ist, drücken Sie auf **Enter**. Die Anmeldeaufforderung wird angezeigt.

   HINWEIS
   Der RUGGEDCOM ROX II besitzt drei voreingestellte Benutzerkonten: Admin, Bediener und Gast. Weitere Benutzerkonten können hinzugefügt werden. Informationen über das Hinzufügen von Benutzerkonten finden Sie in Abschnitt 5.7.2, „Hinzufügen eines Benutzers“.

3. Geben Sie den Benutzernamen ein und drücken Sie auf **Enter**. Sie werden aufgefordert, ein Passwort einzugeben.

   HINWEIS
   Falls kein eindeutiges Passwort bzw. keine eindeutige Passphrase konfiguriert wurde, verwenden Sie das werkseitig eingestellte Passwort. Weitere Informationen finden Sie unter Abschnitt 2.1, „Voreingestellte Benutzernamen und Passwörter“.

   WICHTIG!
   Der RUGGEDCOM ROX II ist mit einem System zum Schutz vor Brute-Force-Angriffen (BFA) ausgestattet, um potenziell böswillige Zugriffsversuche auf das Gerät zu erkennen. Sofern aktiviert, blockiert das Schutzsystem eine IP-Adresse nach 15 fehlgeschlagenen Anmeldeversuchen für eine Dauer von 10 Minuten. Die IP-Adresse wird erstmalig für 720 Sekunden bzw. 12 Minuten gesperrt. Wenn mit derselben IP-Adresse erneut 15 fehlgeschlagene Anmeldeversuche innerhalb eines Zeitraums von 10 Minuten erkannt werden, dann wird diese erneut gesperrt, jedoch beträgt die Sperrdauer diesmal das 1,5-fache der vorherigen Sperrdauer.

   Siemens empfiehlt dringend, den BFA-Schutz zu aktivieren. Weitere Informationen über das Aktivieren des BFA-Schutzes finden Sie in Abschnitt 6.3, „Schutz vor Brute-Force-Angriffen aktivieren/deaktivieren“.

   Der BFA-Schutz ist bei Neuinstallationen des RUGGEDCOM ROX II standardmäßig aktiviert.

4. Geben Sie das zum Benutzernamen zugehörige Passwort ein und drücken Sie auf **Enter**.

```
login as: admin admin@127.0.0.1's password: Welcome to Rugged CLI admin connected from 127.0.0.1
 using console on ruggedcom ruggedcom#
```

Abschnitt 2.3
Abmelden

Zum Abmelden von einem Gerät geben Sie **exit** auf der Root-Ebene ein.

```
ruggedcom#  exit
```

Abschnitt 2.4
Mit den Netzwerkdienstprogrammen arbeiten

RUGGEDCOM ROX II ist mit integrierten Tools für das Pingen von Hosts, die Verfolgung von Routen und die Analyse von Datenpaketen ausgestattet.

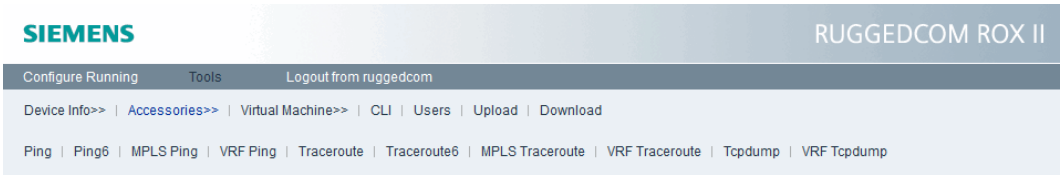


Abbildung 2: Menü "Accessories"

INHALT

- Abschnitt 2.4.1, „Senden von Ping-Anfragen an eine IPv4-Adresse oder einen Host“
- Abschnitt 2.4.2, „Eine IPv6-Adresse oder einen Host pingen“
- Abschnitt 2.4.3, „MPLS-Endpunkte pingen“
- Abschnitt 2.4.4, „VRF-Endpunkte pingen“
- Abschnitt 2.4.5, „Rückverfolgen einer Route zu einem IPv4-Host“
- Abschnitt 2.4.6, „Rückverfolgen einer Route zu einem IPv6-Host“
- Abschnitt 2.4.7, „Eine Route zu einem MPLS-Endpunkt verfolgen“
- Abschnitt 2.4.8, „Tracing einer Route zu einem VRF-Endpunkt“
- Abschnitt 2.4.9, „Erfassen von Paketen von einer Netzwerkschnittstelle“
- Abschnitt 2.4.10, „Erfassen von Paketen von einer VRF-Netzwerkschnittstelle“

Abschnitt 2.4.1
Senden von Ping-Anfragen an eine IPv4-Adresse oder einen Host

Um Ping-Anfragen an eine IPv4-Adresse oder einen Host zu senden, gehen Sie wie folgt vor:

1. Geben Sie in der Eingabeaufforderung Folgendes ein:

```
ping address
```

Erläuterung: *address* ist die IPv4-Zieladresse oder der Hostname.

Die Ergebnisse der Ping-Anfrage werden angezeigt. Beispiel:

```
ruggedcom# ping 192.168.0.7
PING 192.168.0.7 (192.168.0.7) 56(84) bytes of data.
64 bytes from 192.168.0.7: icmp_seq=1 ttl=60 time=0.639 ms
64 bytes from 192.168.0.7: icmp_seq=2 ttl=60 time=0.730 ms
64 bytes from 192.168.0.7: icmp_seq=3 ttl=60 time=0.591 ms
64 bytes from 192.168.0.7: icmp_seq=4 ttl=60 time=0.596 ms
```

2. Drücken Sie **Ctrl-C**, um die Ping-Anfrage zu beenden.

Abschnitt 2.4.2

Eine IPv6-Adresse oder einen Host pingen

Um eine IPv6-Adresse oder einen Host zu pingen, geben Sie Folgendes ein:

- **Für Hosts mit IPv4-Adressen**

  ping *address* iface *interface* count *attempts* wait *seconds*

- **Für Hosts mit IPv6-Adressen**

  ping6 *address* iface *interface* count *attempts* wait *seconds*

Erläuterung:

- *address* ist die IP-Adresse des Hosts
- *attempts* ist die Anzahl der Ping-Versuche
- *interface* ist die zu verwendende Schnittstelle
- *seconds* ist die maximale Anzahl an Sekunden für eine Reaktion des Hosts

Abschnitt 2.4.3

MPLS-Endpunkte pingen

Um einen MPLS-Endpunkt zu pingen, geben Sie Folgendes ein:

mpls-ping *address number*

Erläuterung:

- *address* ist die IPv4-Adresse und das Präfix des MPLS-Endpunkts
- *number* ist die Anzahl Ping-Versuche

Abschnitt 2.4.4

VRF-Endpunkte pingen

Um einen VRF-Endpunkt zu pingen, geben Sie Folgendes ein:

vrf-ping address *address* count *attempts* vrfname *name*

Erläuterung:

- *address* ist die IPv4-Adresse und das Präfix des VRF-Endpunkts
- *attempts* ist die Anzahl Ping-Versuche
- *name* ist das Ziel-VRF

Abschnitt 2.4.5
Rückverfolgen einer Route zu einem IPv4-Host

Um eine Route zu einem IPv4-Host zurückzuverfolgen, gehen Sie wie folgt vor:

```
traceroute host
```

Erläuterung:

- *host* ist die Bezeichnung oder IP-Adresse des dezentralen Hosts.

Die Ergebnisse der Rückverfolgung werden angezeigt. Beispiel:

```
ruggedcom# traceroute 192.168.0.7
traceroute to 192.168.0.7 (192.168.0.7), 30 hops max, 60 byte packets
 1  * * *
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 .
 .
 .
```

Abschnitt 2.4.6
Rückverfolgen einer Route zu einem IPv6-Host

Um eine Route zu einem IPv6-Host zurückzuverfolgen, gehen Sie wie folgt vor:

```
traceroute6 address
```

Erläuterung: *address* ist die Bezeichnung oder IP-Adresse des dezentralen Hosts.

Die Ergebnisse der Rückverfolgung werden angezeigt. Beispiel:

```
ruggedcom# traceroute6 2001:0db8:85a3:0000:0000:8a2e:0370:7334
traceroute to 2001:0db8:85a3:0000:0000:8a2e:0370:7334 (2001:0db8:85a3:0000:0000:8a2e:0370:7334), 30
 hops max, 60 byte packets
 1  * * *
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 .
 .
 .
```

Abschnitt 2.4.7
Eine Route zu einem MPLS-Endpunkt verfolgen

Um eine Route zu einem MPLS-Endpunkt zu verfolgen, gehen Sie wie folgt vor:

```
mpls-traceroute address
```

Erläuterung: *address* ist die IPv4-Adresse der MPLS-Routenverfolgung

Abschnitt 2.4.8
Tracing einer Route zu einem VRF-Endpunkt

Um eine Route zu einem VRF-Endpunkt zu tracen, gehen Sie wie folgt vor:

```
vrf-traceroute vrfname name
```

Erläuterung: *name* ist der VRF-Endpunkt

Abschnitt 2.4.9
Erfassen von Paketen von einer Netzwerkschnittstelle

Tcpdump ist ein Paketanalyseprogramm für TCP/IP und andere Pakete. Es kann zum Erfassen von Paketen an einer spezifizierten Netzwerkschnittstelle und zum Ablegen in einem Terminal oder in einer Datei verwendet werden.

Um Pakete zu erfassen, geben Sie **tcpdump** ein und konfigurieren folgende Parameter:

Parameter	Beschreibung
address	Zeigt die Quell-IP für jedes Paket an.
count	Die Anzahl an zu erfassenden Paketen
hex	Konvertiert die Daten in Hexadezimal- oder ASCII-Zeichen.
host	Der zu ignorierende bzw. zuzulassende Hostname.
interface	Die Schnittstelle von der abzulegenden IP-Liste.
linkheader	Zeigt den Link-Level-Header an.
port	Die zu beobachtenden Ports.
proto { tCP | uDP | iCMP | aRP | vRRP | IqMP | oSPF | eSP | Ah }	Das bzw. die herauszufilternden Protokolle. Um mehr als ein Protokoll auszuwählen, fügen Sie die Kleinbuchstaben in einer Zeichenfolge zusammen. Beispiel: "tui" filtert TCP-, UDP- und ICMP-Pakete heraus. Um ein Protokoll zu ignorieren, setzen Sie ein "n" vor den Protokollnamen (z. B. ntui).
verbosity	Die Verbositätsstufe. Geben Sie "v", "vv", oder "vvv" ein, um die Stufe festzulegen.

Abschnitt 2.4.10

Erfassen von Paketen von einer VRF-Netzwerkschnittstelle

VRF Tcpdump ist ein Paketanalyseprogramm für TCP/IP und andere Pakete. Es kann zum Erfassen von Paketen an einer spezifizierten VRF-Netzwerkschnittstelle und zum Ablegen in einem Terminal oder in einer Datei verwendet werden.

Um Pakete zu erfassen, geben Sie **`vrf-tcpdump`** ein und konfigurieren folgende Parameter:

Parameter	Beschreibung
vrfname	Zeigt die Quell-IP für jedes Paket an.
`address`	Zeigt die Quell-IP für jedes Paket an.
`count`	Die Anzahl an zu erfassenden Paketen
`hex`	Konvertiert die Daten in Hexadezimal- oder ASCII-Zeichen.
`host`	Der zu ignorierende bzw. zuzulassende Hostname.
`interface`	Die Schnittstelle von der abzulegenden IP-Liste.
`linkheader`	Zeigt den Link-Level-Header an.
`port`	Die zu beobachtenden Ports.
`proto` { `tCP` | `uDP` | `iCMP` | `aRP` | `vRRP` | `IqMP` | `oSPF` | `eSP` | `Ah` }	Das bzw. die herauszufilternden Protokolle. Um mehr als ein Protokoll auszuwählen, fügen Sie die Kleinbuchstaben in einer Zeichenfolge zusammen. Beispiel: "tui" filtert TCP-, UDP- und ICMP-Pakete heraus. Um ein Protokoll zu ignorieren, setzen Sie ein "n" vor den Protokollnamen (z. B. ntui).
`verbosity`	Die Verbositätsstufe. Geben Sie "v", "vv", oder "vvv" ein, um die Stufe festzulegen.

Abschnitt 2.5

Mit der Befehlszeilenschnittstelle arbeiten

Dieser Abschnitt beschreibt das Arbeiten mit der CLI (Command Line Interface) für RUGGEDCOM ROX II. Er umfasst gängige Befehle, Konventionen und hilfreiche Techniken.

INHALT

- Abschnitt 2.5.1, „Auf die verschiedenen CLI-Modi zugreifen“
- Abschnitt 2.5.2, „Befehlszeilenergänzung verwenden“
- Abschnitt 2.5.3, „Verfügbare Befehle anzeigen“
- Abschnitt 2.5.4, „Bearbeiten von Befehlen“
- Abschnitt 2.5.5, „Verwendung doppelter Anführungszeichen“
- Abschnitt 2.5.6, „Ausgabeumleitung verwenden“
- Abschnitt 2.5.7, „Verwenden von regulären Ausdrücken“
- Abschnitt 2.5.8, „CLI-Dienstprogramme verwenden“
- Abschnitt 2.5.9, „Einen Bereich festlegen“
- Abschnitt 2.5.10, „Gängige Befehle“

Abschnitt 2.5.1
Auf die verschiedenen CLI-Modi zugreifen

RUGGEDCOM ROX II bietet Befehle zur Überwachung und Konfigurierung der Software, Hardware und Netzwerkkonnektivität. Die Befehlszeilenschnittstelle (Command Line Interface, CLI) unterstützt die folgenden Modi:

Modus	Beschreibung
Betriebsmodus	Bei dem Betriebsmodus handelt es sich um den voreingestellten Modus, nachdem sich ein Benutzer am Gerät anmeldet. In diesem Modus können die Benutzer allgemeine Gerätemanagement-Aktionen ausführen sowie Fehlersuche- und Wartungsfunktionen nutzen. Er dient zur Anzeige des Systemstatus, zur Steuerung der CLI-Umgebung, zur Überwachung und Fehlerbehebung der Netzwerkkonnektivität und zum Starten des Konfigurationsmodus.
Konfigurationsmodus	Der Konfigurationsmodus wird aus dem Betriebsmodus gestartet. Hierin kann der Benutzer die Ist-Konfiguration des Gerätes ändern. Alle Änderungen an der Konfiguration werden an einer Kopie der aktiven Konfiguration vorgenommen, dem so genannten Kandidaten. Die Änderungen müssen erst bestätigt werden, damit sie in Kraft treten.

In beiden Modi zeigt die CLI-Aufforderung den aktuellen Modus an. Im Betriebsmodus lautet die Aufforderung:

```
ruggedcom#
```

Im Konfigurationsmodus lautet die Aufforderung:

```
ruggedcom(config)#
```

Wenn ein Benutzer durch die Hierarchie der Konfigurationsdaten navigiert, zeigt die Aufforderung die Position des Benutzers in der Konfiguration an. Nach der Navigation zu ***interface » serial » serport » 1***, ist die CLI-Aufforderung beispielsweise:

```
ruggedcom(config-serial-serport/1)#
```

Abschnitt 2.5.2
Befehlszeilenergänzung verwenden

Befehle und Parameter müssen nicht vollständig eingegeben werden, damit die CLI sie erkennt. Wenn Sie die ersten Buchstaben eines Befehls eingeben und auf **Tab** drücken, zeigt die CLI die möglichen Ergänzungen an. Wenn die ersten Buchstaben eines Befehls eindeutig sind, wird der vollständige Befehl automatisch angezeigt. Stimmen die ersten Buchstaben mit mehr als einem möglichen Befehl überein, erscheint eine Auflistung der möglichen Ergänzungen.

HINWEIS
Die automatische Vervollständigung in Anführungszeichen ist deaktiviert. Wenn die Bezeichnung eines Befehls oder Parameters ein Leerzeichen enthält, z. B. ein Dateiname, kann das Leerzeichen durch ein \ ersetzt werden oder die Zeichenfolge in Anführungszeichen gesetzt werden. Beispiel:

```
who file foo\ bar
```

oder

```
who file "foo bar"
```

HINWEIS
Die automatische Vervollständigung ist auch bei Dateinamen und Verzeichnissen möglich, kann aber nicht mit Leerzeichen eingeleitet werden. Die automatische Vervollständigung mit Leerzeichen wird deaktiviert, wenn Sie einen Datei- oder Verzeichnisnamen eingeben.

Abschnitt 2.5.3
Verfügbare Befehle anzeigen

Um jederzeit in der CLI eine Liste verfügbarer Befehle zu sehen, geben Sie **?** ein.

Im Betriebsmodus kann zum Beispiel durch Eingabe von **?** in der Eingabeaufforderung eine Liste aller Befehle für den Betriebsmodus aufgerufen werden.

```
ruggedcom# ?
Possible completions:
  admin               Configures the general device characteristics
  autowizard       Automatically query for mandatory elements
  clear                 Clear parameter
  commit              Confirm a pending commit
  compare           Compare running configuration to another configuration or a file
  .
  .
  .
  traceserial        Trace serial ports activities
  who                  Display currently logged on users
  write                 Write configuration
ruggedcom#
```

Abschnitt 2.5.4
Bearbeiten von Befehlen

Die folgenden Befehle können zum Bearbeiten der Befehlszeilen und zum Navigieren im Befehlsverlauf verwendet werden.

Bewegen des Cursors

Befehl	Beschreibung
Strg-B oder **Pfeil nach links**	Bewegt den Cursor ein Zeichen zurück
Strg-F oder **Pfeil nach rechts**	Bewegt den Cursor ein Zeichen vor
Esc-B oder **Alt-B**	Bewegt den Cursor ein Wort zurück
Esc-F oder **Alt-F**	Bewegt den Cursor ein Wort vor
Strg-A oder **Pos1**	Bewegt den Cursor an den Anfang der Befehlszeile
Strg-E oder **Ende**	Bewegt den Cursor an das Ende der Befehlszeile

Löschen von Zeichen

Befehl	Beschreibung
Strg-H, **Entf** oder **Rücktaste**	Löscht das Zeichen vor dem Cursor
Strg-D	Löscht das Zeichen nach dem Cursor
Strg-K	Löscht alle Zeichen vom Cursor bis zum Ende der Zeile
Strg-U oder **Strg-X**	Löscht die gesamte Zeile
Strg-W, **Esc-Rücktaste** oder **Alt-Rücktaste**	Löscht alle Zeichen vor dem Cursor
Esc-D oder **Alt-D**	Löscht alle Zeichen nach dem Cursor

Einfügen von kürzlich gelöschtem Text

Befehl	Beschreibung
Strg-Y	Fügt den zuletzt gelöschten Text an der Position des Cursors ein

Anzeigen zuvor eingegebener Befehle

Befehl	Beschreibung
Strg-P oder **Pfeil nach oben**	Zeigt den vorherigen Befehl im Befehlsverlauf an
Strg-N oder **Pfeil nach unten**	Zeigt den nächsten Befehl im Befehlsverlauf an
Strg-R	Dreht die Reihenfolge der Befehle im Befehlsverlauf um
`show history`	Zeigt eine Liste vorheriger Befehle an

Großschreibung

Befehl	Beschreibung
Esc-C	Schreibt den ersten Buchstaben des Wortes an der Position des Cursors groß und setzt alle anderen Zeichen auf Kleinschreibung
Esc-L	Ändert das gesamte Wort an der Position des Cursors in Kleinschreibung
Esc-U	Ändert das gesamte Wort an der Position des Cursors in Großschreibung

Besondere Aktionen

Befehl	Beschreibung
Strg-C	Bricht einen Befehl ab oder löscht die Befehlszeile
Strg-V oder **Esc-Q**	Behandelt das bzw. die nächsten Zeichen als Zeichendaten und nicht als Befehl
Strg-L	Zeichnet den Bildschirm neu
Strg-T	Transponiert Zeichen

Befehl	Beschreibung
Esc-M	Ruft den Multiline-Modus auf
Strg-D	Beendet den Multiline-Modus
Strg-Z	Beendet den Konfigurationsmodus

» Einfügen von harten Zeilenumbrüchen

Befehl	Beschreibung
Esc-M	Fügt einen harten Zeilenumbruch ein

Abschnitt 2.5.5

Verwendung doppelter Anführungszeichen

Wenn der Wert für einen Parameter Leerzeichen enthält, ist der Wert, sofern nicht anders angegeben ist, in doppelte Anführungszeichen ("") zu setzen.

Beispiel:

```
admin scheduler scheduled-jobs save-myconfig job-command "show running-config | save myconfig"
```

Abschnitt 2.5.6

Ausgabeumleitung verwenden

Über einen CLI-Befehl ausgegebene Daten können auf verschiedene Weise mithilfe eines Umleitungsausdrucks verarbeitet werden. Um eine Ausgabeumleitung anzugeben, geben Sie nach dem CLI-Befehl **|** und dann den Umleitungsausdruck ein. Um die verfügbaren Umleitungen anzuzeigen, geben Sie nach einem CLI-Befehl **| ?** ein. Beispiel:

```
ruggedcom# show admin | ?
Possible completions:
  append      Append output text to a file
  begin         Begin with the line that matches
  count         Count the number of lines in the output display
  exclude      Exclude lines that match
  include       Include lines that match
  linnum        Enumerate lines in the output
  more          Paginate output
  nomore      Suppress pagination
  notab         Suppress table output
  repeat        Repeat show term with a given interval
  save           Save output text to a file
  select         Select additional columns
  tab             Enforce table output
  until           End with the line that matches
```

Parameter	Beschreibung
append	Hängt den Ausgabetext an eine angegebene ASCII-Textdatei an. Beispielsweise werden durch Ausführung dieser beiden Befehle die Admin- und Chassis-Informationen an die angegebene Datei angehängt:

Parameter	Beschreibung

	`ruggedcom# show admin | append foo.txt ruggedcom# show interface | append foo.txt`
	
	Die resultierende Datei enthält die Ergebnisse von show interface angehängt an die Ergebnisse von show admin (mit ... abgeschnittene Zeilen wurden nur aus Darstellungsgründen gekürzt):
	
	`ruggedcom# file show-config foo.txt`
	`admin`
	`  time`
	`   gmtime    "Thu Oct  2 19:35:17 2014"`
	`   localtime "Thu Oct  2 15:35:17 2014"`
	`  rox-imaging`
	`   roxflash-progress`
	`    phase          Inactive`
	`    status message ""`
	`    image flashing 0`
	`  netconf`
	`   statistics`
	`    in bad hellos     0`
	`    in sessions       0`
	`    dropped sessions  0`
	`    in rpcs           0`
	`    in bad rpcs       0`
	`    out rpc errors    0`
	`    out notifications 0`
	`  software-upgrade`
	`   upgrade-progress`
	`    software partition   "Partition #1"`
	`    current version      "ROX 2.7.0-QA3.1 (2014-10-21 14:59)"`
	`    upgrade state        Inactive`
	`    status message       ""`
	`    filesystem copy      0`
	`    package download     0`
	`    package installation 0`
	`    last upgrade attempt "Thu Oct  2 09:57:46 EDT 2014"`
	`    last upgrade result  "Upgrade Successful"`

begin	Beginnt die Ausgabe mit der Zeile, die den angegebenen Text enthält. Bei dieser Umleitung können reguläre Ausdrücke verwendet werden. Weitere Informationen über reguläre Ausdrücke finden Sie unter Abschnitt 2.5.7, „Verwenden von regulären Ausdrücken“.
	
	Beispiel: **`show admin | begin netconf`** gibt alle **admin**-Daten zurück, die auf die Zeile `netconf` folgen:
	
	`ruggedcom# show admin | begin netconf`
	`  netconf`
	`   statistics`
	`    in sessions 0 in xml parse errs 0 in bad hellos 0 in rpcs 0 in bad rpcs 0 in not...`

count	Zeigt die Anzahl der durch den Ausdruck zurückgegebenen Zeilen an.
	
	Beispiel: show admin | count zeigt die Anzahl der Zeilen in den *admin*-Daten an.
	
	`ruggedcom# show admin | count`
	`Count: 9 lines`

exclude	Schließt Zeilen aus, die den angegebenen Text enthalten. Daten, die der ausgeschlossenen Zeile *untergeordnet* sind, werden ebenfalls ausgeschlossen. Mit dieser Umleitung können reguläre Ausdrücke verwendet werden. Weitere Informationen über reguläre Ausdrücke finden Sie unter Abschnitt 2.5.7, „Verwenden von regulären Ausdrücken“. Beispiel: show admin | exclude netconf zeigt die *admin*-Daten ausschließlich der Zeilen `netconf` an.

Parameter	Beschreibung
	``` ruggedcom# show admin | exclude netconf admin time gmtime "Tue Feb 15 08:25:27 2011\n" localtime "Tue Feb 15 03:25:27 2011\n" software-upgrade upgrade-progress software partition "Partition #1" current version "ROX 2.1.0 (2010-12-03 17:38) ... statistics in sessions 0 in xml parse errs 0 in bad hellos 0 in rpcs 0 in bad rpcs 0 in not... supported rpcs 0 out rpc replies 0 out rpc errors 0 out notifications 0 ```
include	Schließt Zeilen ein, die den angegebenen Text enthalten. Daten, die der eingeschlossenen Zeile *untergeordnet* sind, werden üblicherweise eingeschlossen, was jedoch in manchen Fällen nicht geschieht. Mit dieser Umleitung können reguläre Ausdrücke verwendet werden. Weitere Informationen über reguläre Ausdrücke finden Sie unter Abschnitt 2.5.7, „Verwenden von regulären Ausdrücken“. Beispiel: show admin | include time zeigt die `time`– Zeilen aus den *admin*-Daten an. ``` ruggedcom# show admin | include time time gmtime "Tue Feb 15 08:34:55 2011\n" localtime "Tue Feb 15 03:34:55 2011\n" ruggedcom# ```
linnum	Nummeriert die Zeilen in der Ausgabe. Beispiel: ``` ruggedcom# show admin | linnum 1: admin 2: time 3: gmtime "Tue Feb 15 08:37:42 2011\n" localtime "Tue Feb 15 03:37:42 2011\n" 4: software-upgrade . . . ```
more	Paginiert die Ausgabe. Wenn die Ausgabe die Einstellung für die Bildschirmlänge erreicht, werden Sie von der CLI aufgefordert, eine Taste zu drücken, um mehr anzuzeigen. Mit der **Eingabetaste** können Sie zeilenweise vorangehen, mit der **Leertaste** können Sie seitenweise blättern.
nomore	Unterdrückt die Paginierung.
notab	Unterdrückt die Tabellenausgabe. Beispiel: show chassis | begin line-modules zeigt die folgende Tabelle an: ``` ruggedcom# show chassis | begin line-modules line-modules line-module BYPASS OVERCURRENT SLOT DETECTED MODULE STATUS STATUS --- swport SM M88E6097F, 4FT 2GP - - eth none - - serport 2xRS232/422/485 - - celport 1x Cell LTE EU - - ```

For example, show chassis | begin line-modules | notab suppresses the table formatting:

Parameter	Beschreibung

	`ruggedcom# show chassis | begin line-modules | notab`
	` line-modules`
	`  line-module swport`
	`   detected module "SM M88E6097F, 4FT 2GP"`
	`  line-module eth`
	`   detected module none`
	`  line-module serport`
	`   detected module 2xRS232/422/485`
	`  line-module celport`
	`   detected module "1x Cell LTE EU"`

repeat	Wiederholt den Ausdruck im angegebenen Zeitraum. Geben Sie ein Intervall in Sekunden ein. Der Ausdruck wird solange wiederholt, bis Sie ihn mit **Strg-C** abbrechen. Beispiel: show admin | repeat 10s wiederholt den Ausdruck show admin alle 10 Sekunden.
save	Speichert die Ausgabe in der angegebenen ASCII-Textdatei. Beispiel: show chassis | save foo.txt speichert die *chassis*-Daten in der Datei `foo.txt`
select	*Diese Umleitung ist noch nicht implementiert.*
tab	Erzwingt das Tabellenlayout für spaltenförmige Daten.

until	Schließt sämtliche Ausgabe ein, bis eine Zeile mit dem angegebenen Text erscheint. Mit dieser Umleitung können reguläre Ausdrücke verwendet werden. Weitere Informationen über reguläre Ausdrücke finden Sie unter Abschnitt 2.5.7, „Verwenden von regulären Ausdrücken“.
	Beispiel: show chassis | begin line-modules | until status gibt die **chassis**-Daten zurück, mit Beginn an `line-modules` und Ende an `status`:
	`ruggedcom# show chassis | begin line-modules | until status`
	` line-modules`
	`  line-module`
	`                                BYPASS  OVERCURRENT`
	`SLOT     DETECTED MODULE       STATUS  STATUS`
	`-----------------------------------------------------`
	`swport   SM M88E6097F, 4FT 2GP  -       -`
	`eth      none                  -       -`
	`serport  2xRS232/422/485       -       -`
	`celport  1x Cell LTE EU        -       -`

Abschnitt 2.5.7

Verwenden von regulären Ausdrücken

Die regulären Ausdrücke der Befehlszeile des RUGGEDCOM ROX II sind eine Teilmenge der regulären Ausdrücke von egrep und der Programmiersprache AWK. Reguläre Ausdrücke können zusammen mit einigen Ausgabeumleitungen verwendet werden. Weitere Informationen über das Verwenden von Ausgabeumleitungen finden Sie in Abschnitt 2.5.6, „Ausgabeumleitung verwenden“.

Zeichen	Beschreibung	Beispiel
.	Stimmt mit einem beliebigen einzelnen Zeichen überein (z. B. .100, 100., .100.)	.100 100. .100.
*	Stimmt mit null (0) oder mehreren Vorkommen eines Musters überein	100*
+	Stimmt mit 1 oder mehreren Vorkommen eines Musters überein	100+

Zeichen	Beschreibung	Beispiel
?	Stimmt mit 0 oder 1 Vorkommen eines Musters überein	100?
^	Stimmt mit dem Anfang der Zeile überein	^100
$	Stimmt mit dem Ende der Zeile überein	100$
()	Stimmt nur mit den angegebenen Zeichen überein	(38a)
[]	Stimmt mit beliebigen Zeichen außer den angegebenen Zeichen überein	[^abc]
_ (Unterstrich)	Das Unterstrich-Zeichen hat in einem autonomen Systempfad spezielle Bedeutungen. Es stimmt überein mit: • Jedem Leerzeichen ( ) und Komma (,) • Jedem AS Set Delimiter (z. B. *{* und *}*) • Jedem AS Confederation Delimiter (z. B. *(* und *)*) • Dem Anfang und Ende der Zeile Daher kann der Unterstrich zur Übereinstimmung mit AS-Werten verwendet werden.	_100,100_, _100_

Um beispielsweise alle IP-Schnittstellen anzuzeigen, die sich im Zustand *up* befinden:

```
ruggedcom# show interfaces ip | include up
 admin state up
 state       up
 admin state up
 state       up
 admin state up
 state       up
 admin state up
 admin state up
 admin state up
 admin state up
 admin state up
```

Abschnitt 2.5.8

CLI-Dienstprogramme verwenden

Der Betriebsmodus bietet eine Reihe von Standard-Utility-Anwendungen, ähnlich denen auf einem typischen Linux-basierten Betriebssystem.

Parameter	Beschreibung
ssh [host | *address/name*] { bind-address | *address* } { cipher-spec | *cipher* } { login | *name* } { port | *number* } { sub-system }	Öffnet eine sichere Shell auf einem anderen Host. Parameter sind u.a.: • `host` ist die IP-Adresse des Hosts. Er ist obligatorisch. • `bind-address` ist die Quelladresse der Verbindung. Nur in Systemen mit mehr als einer Adresse sinnvoll. • `cipher-spec` ist die Verschlüsselungsspezifikation zum Verschlüsseln der Sitzung. Es werden die folgenden Verschlüsselungsoptionen unterstützt: 128-cbc, 3des-cbc, blowfish-cbc, cast128-cbc, arcfour128, arcfour256, arcfour, aes192-cbc, aes256-cbc, aes128-ctr, aes192-ctr und aes256-ctr. • `login` ist der Login-Name des Benutzers auf dem Host. • `port` ist die TCP-Portnummer zum Öffnen einer SSH-Sitzung. • `sub-system` ruft ein Subsystem auf dem entfernten System auf, wie NETCONF.
telnet { host | *address/name* }	Öffnet eine Telnet-Sitzung zu einem anderen Host. Parameter sind u.a.: • *`host`* ist die Bezeichnung oder die IP-Adresse des Hosts.

Weitere Informationen über diese bekannten Anwendungen erhalten Sie im Internet.

Abschnitt 2.5.9
Einen Bereich festlegen

Einige CLI-Befehle lassen einen Wertebereich wie 3-6 zu, um mehrere Ziele anzugeben. Im folgenden Beispiel wird ein Befehl auf die Ports 1, 2 und 3 am Steckplatz swport angewendet:

```
ruggedcom(config)# interface switch swport 1-3
```

In diesem Beispiel wird ein Befehl an die Ports 1, 2 und 4 am Steckplatz swport abgesetzt:

```
ruggedcom(config)# interface switch swport 1-2,4
```

Sofern verfügbar, kann der Parameter `range` vor dem Wertebereich eingefügt werden:

```
ruggedcom(config)# interface switch range swport 1-2,4
```

Abschnitt 2.5.10
Gängige Befehle

Dieser Abschnitt beschreibt einige der gängigen Befehle für Betrieb und Konfiguration.

INHALT

- Abschnitt 2.5.10.1, „Grundlegende CLI-Befehle“
- Abschnitt 2.5.10.2, „Dateibefehle“
- Abschnitt 2.5.10.3, „Schnittstellen- und Dienstbefehle“
- Abschnitt 2.5.10.4, „Administrationsbefehle“
- Abschnitt 2.5.10.5, „Allgemeine Befehle für den Konfigurationsmodus“

Abschnitt 2.5.10.1
Grundlegende CLI-Befehle

Verwenden Sie die folgenden Befehle, um grundlegende CLI-Funktionen auszuführen.

Parameter	Beschreibung
exit [level | configuration-mode | no-confirm]	**Standard:** level Beendet den aktuellen Modus. • `level` beendet den aktuellen Modus. Sofern dieser Befehl in der obersten Ebene ausgeführt wird, wird der Konfigurationsmodus beendet. • `configuration-mode` beendet den Konfigurationsmodus ungeachtet des Modus. • `no-confirm` beendet den Konfigurationsmodus, ohne den Benutzer aufzufordern, ausstehende Änderungen zu übernehmen.
help *command*	Zeigt den Hilfetext zum spezifizierten Befehl an.
id	Zeigt die aktuellen Benutzerinformationen an. Beispiel:

Parameter	Beschreibung
	`ruggedcom# id` ` user = admin(0), gid=0, groups=admin, gids=`
logout [logout | sessionid]	Beendet die spezifizierte Sitzung. Eine Sitzung kann basierend auf ihrer Benutzer-ID oder Sitzungs-ID spezifiziert werden.
quit	Meldet den Benutzer aus der CLI-Sitzung ab und beendet die Sitzung.

send [all | admin] *message*	Sendet eine Meldung an alle Benutzer des spezifizierten Typs.Diese Meldung erscheint sowohl in der CLI als auch in der Web-Schnittstelle. Beispiel:
	`ruggedcom# send all "Rebooting at midnight!"Message from`
	` admin@ruggedcom at 2011-02-15 08:42:49...`
	` Rebooting at midnight!`
	` EOF`

show [admin | chassis | interface | interfaces | netconf | routing | services]	Zeigt ausgewählte Konfigurationsinformationen an. Verwenden Sie die Auto-Vervollständigen-Funktion, um eine Liste der auf jeder Konfigurationsebene verfügbaren Optionen anzuzeigen. Beispiel:
	`ruggedcom# show chassis hardware slot-hardware`
	`         ORDER                                SERIAL`
	`SLOT     FIELD     DETECTED MODULE        NUMBER`
	`-----------------------------------------------------`
	`swport   SM0001    SM M88E6097F, 4FT 2GP`
	`serport  SER0001   2xRS232/422/485`
	`celport  CELL0001  Cellular Modem`

show [cli | history | jobs | log | *logfile*]	Zeigt ausgewählte Systeminformationen an.
	• `cli` zeigt die CLI-Umgebungseinstellungen an. Beispiel:
	`ruggedcom# show cli`
	` autowizard  true`
	` complete-on-space  true`
	` display-level  99999999`
	` history  100`
	` ignore-leading-space  true`
	` output-file  terminal`
	` paginate  true`
	` screen-length  65`
	` screen-width  237`
	` service prompt config  true`
	` show-defaults  false`
	` terminal  xterm`
	• `history` zeigt den CLI-Befehlsverlauf an.
	• `jobs` zeigt aktuell im Hintergrund laufende Aufträge an. Beispiel:
	`ruggedcom# show jobs JOB COMMAND 2 monitor start /tmp/saved`
	• `log` und `logfile` zeigen die ausgewählte Protokolldatei an. Mit der Autovervollständigung können Sie eine Liste der verfügbaren Protokolldateien anzeigen.

show parser dump *command*	Zeigt alle möglichen Befehle an, die mit dem spezifizierten Befehl beginnen.
show running-config *option*	Zeigt die aktuelle Konfiguration an. Wenn ein *option*-Parameter nicht spezifiziert ist, dann wird standardmäßig die komplette Konfiguration angezeigt. Mit der Autovervollständigung können Sie eine Liste der Konfigurationsoptionen anzeigen. Verwenden Sie | und eine oder mehrere Ausgabeumleitungen, um die anzuzeigenden Informationen einzuschränken.

Abschnitt 2.5.10.2
Dateibefehle

Der Betriebszustand bietet Befehle zum Verwalten von Protokoll- und Konfigurationsdateien auf dem Gerät.

Parameter	Beschreibung
file	Führt Dateioperationen durch, dazu gehören: • **compare-config** • **copy-config** • **delete-config** • **delete-featurekey** • **list-config** • **list-featurekey** • **rename-config** • **rename-featurekey** • **scp-config-from-url** • **scp-config-to-url** • **scp-featurekey-from-url** • **scp-featurekey-to-url** • **scp-log-to-url** • **show-config** • **show-featurekey**

file compare-config *filename1 filename2*	Vergleicht die Inhalte der beiden Dateien. Das Zeichen **<** zeigt an, dass in der ersten ausgewählten Datei Text vorhanden ist, der in der zweiten Datei nicht vorhanden ist. Das Zeichen **>** zeigt an, dass in der zweiten ausgewählten Datei Text vorhanden ist, der in der ersten Datei nicht vorhanden ist. Im folgenden Beispiel ist die Benutzerinformation in der zweiten Datei vorhanden, jedoch nicht in der ersten:
	`ruggedcom# file compare deleted_users all_users`
	`125,127d124`
	`<  userid jsmith`
	`<   password $1$N1YT8Azl$KcG1E6/r91EXc4mgEEsAW. role administrator`
	`<  !`

file copy-config *current-filename new-filename*	Kopiert eine Konfigurationsdatei. Drücken Sie nach Eingabe des Befehls die **Tab**-Taste, um eine Liste verfügbarer Dateien anzuzeigen. Beispiel: Der folgende Befehl kopiert die `deleted_users` Datei in die `archive001` Datei: `ruggedcom# file copy-config deleted_users archive001`
file delete-config *filename*	Löscht eine Konfigurationsdatei. Drücken Sie nach Eingabe des Befehls die **Tab**-Taste, um eine Liste verfügbarer Dateien anzuzeigen. Beispiel: Der folgende Befehl löscht die `deleted_users` Datei: `ruggedcom# file delete-config deleted_users`

file list-config	Listet die Konfigurationsdateien auf. Beispiel:
	`ruggedcom# file list-config`
	`--help 10.200.20.39  _tmp_confd_cmd.0 archive001 archive002`
	`default_rx1000_config`

file rename-config *current-filename new-filename*	Benennt eine Konfigurationsdatei um. Beispiel: Der folgende Befehl führt eine Umbenennung durch der `test002` Datei in `production_config`: `ruggedcom# file rename-config test002 production_config`

Parameter	Beschreibung

file scp-config-from-url *user@host:/path/current-filename new-filename*	Kopiert eine Konfigurationsdatei sicher von einem entfernten Computer auf das Gerät. Auf dem entfernten Computer muss ein SCP- oder SSH-(Secure Shell)-Dienst oder -Client installiert und in Betrieb sein.
	Um diesen Befehl zu verwenden, müssen die Zugangsdaten des Benutzers für den entfernten Computer, die IP-Adresse bzw. der Hostname des entfernten Computers, der Verzeichnispfad der Konfigurationsdatei auf dem entfernten Computer und der Dateiname der Konfigurationsdatei bekannt sein.
	Geben Sie den Befehl in folgendem Format ein:
	file scp-config-from-url *user@host:/path/current-filename new-filename*
	Erläuterung:
	• *user* ist ein Benutzername mit Zugriffsrechten auf den entfernten Computer.
	• *host* ist der Hostname bzw. die IP-Adresse des entfernten Computers.
	• *path* ist der Pfad der Konfigurationsdatei auf dem entfernten Computer.
	• *current-filename* ist der aktuelle Dateiname der Konfigurationsdatei.
	• *new-filename* ist der neue Dateiname für die Konfigurationsdatei. Um den aktuellen Dateinamen zu verwenden, geben Sie den aktuellen Dateinamen an oder schließen diesen Parameter aus dem Befehl aus.
	Geben Sie bei Aufforderung das Passwort ein, um eine Verbindung zum entfernten Computer herzustellen. Beispiel:
	`ruggedcom# file scp-config-from-url jsmith@10.200.20.39:/c:/ruggedcom/standard_config standard_config`
	`jsmith@10.200.20.39's password:`
	`standard_config.txt 100% 7673 7.5KB/s 00:00`

file scp-config-to-url *current-filename user@host:/path/new-filename*	Kopiert eine Konfigurationsdatei sicher vom Gerät zu einem entfernten Computer. Auf dem entfernten Computer muss ein SCP- oder SSH-(Secure Shell)-Dienst oder -Client installiert und in Betrieb sein.
	Um diesen Befehl zu verwenden, müssen die Zugangsdaten des Benutzers für den entfernten Computer, die IP-Adresse bzw. der Hostname des entfernten Computers, der Verzeichnispfad der Konfigurationsdatei auf dem entfernten Computer und der Dateiname der Konfigurationsdatei bekannt sein.
	Geben Sie den Befehl in folgendem Format ein:
	file scp-config-to-url *current-filename user@host:/path/new-filename*
	Erläuterung:
	• *current-filename* ist der aktuelle Dateiname der Konfigurationsdatei.
	• *user* ist ein Benutzername mit Zugriffsrechten auf den entfernten Computer.
	• *host* ist der Hostname bzw. die IP-Adresse des entfernten Computers.
	• *path* gibt an, wo die Konfigurationsdatei auf dem entfernten Computer gespeichert werden soll.
	• *new-filename* ist der neue Dateiname für die Konfigurationsdatei. Um den aktuellen Dateinamen zu verwenden, geben Sie den aktuellen Dateinamen an oder schließen diesen Parameter aus dem Befehl aus.
	Geben Sie bei Aufforderung das Passwort ein, um eine Verbindung zum entfernten Computer herzustellen. Beispiel:
	`ruggedcom# file scp-config-to-url default_config jsmith@10.200.20.39:/c:/ruggedcom/default_config`
	`jsmith@10.200.20.39's password:`
	`standard_config.txt 100% 7673 7.5KB/s 00:00`

Parameter	Beschreibung

file scp-log-to-url *current-filename user@host:/path/new-filename*
 	
scp-log-to-url
	Kopiert eine Protokolldatei sicher vom Gerät auf einen entfernten Computer. Auf dem entfernten Computer muss ein SCP- oder SSH-(Secure Shell)-Dienst oder -Client installiert und in Betrieb sein.
	
	Um diesen Befehl zu verwenden, müssen die Zugangsdaten des Benutzers für den entfernten Computer, die IP-Adresse bzw. der Hostname des entfernten Computers, der Verzeichnispfad der Protokolldatei auf dem entfernten Computer und der Dateiname der Protokolldatei bekannt sein.
	
	Erläuterung:
	
	• *current-filename* ist der aktuelle Dateiname der Protokolldatei.
	• *user* ist ein Benutzername mit Zugriffsrechten auf den entfernten Computer.
	• *host* ist der Hostname bzw. die IP-Adresse des entfernten Computers.
	• *path* gibt an, wo die Protokolldatei auf dem entfernten Computer gespeichert werden soll.
	• *new-filename* ist der neue Dateiname für die Protokolldatei. Um den aktuellen Dateinamen zu verwenden, geben Sie den aktuellen Dateinamen an oder schließen diesen Parameter aus dem Befehl aus.
	
	Geben Sie bei Aufforderung das Passwort ein, um eine Verbindung zum entfernten Computer herzustellen. Beispiel:
	
	`ruggedcom# file scp-log-to-url syslog.1 jsmith@10.200.20.39:/c:/ruggedcom/syslog.1`
	`jsmith@10.200.20.39's password:`
	`syslog.1 100% 12KB 12.4KB/s 00:00`

file show-config *filename*	Zeigt den Inhalt einer angegebenen Datei an. Verwenden Sie die Autovervollständigung, um eine Liste verfügbarer Dateien anzuzeigen. Beispiel:
	
	`ruggedcom# file show-config added_users.txt`
	`admin system-name "System Name" location Location contact Contact`
	`admin hostname name ruggedcom domain localdomain`
	`admin session-limits max-sessions 50`
	`.`
	`.`
	`.`

Abschnitt 2.5.10.3

Schnittstellen- und Dienstbefehle

Im Betriebsmodus werden Befehle für den Neustart und die Anzeige von Informationen für verschiedene Schnittstellen und Dienste zur Verfügung gestellt.

Parameter	Beschreibung
interfaces cellmodem cel-1 lte [at | reset]	Sendet einen AT- oder Rücksetzbefehl an das angegebene Modem. Verwenden Sie die Autovervollständigung, um eine Liste verfügbarer Modems anzuzeigen. • at: Sendet einen AT-Befehl an das ausgewählte Modem. Zum Senden mehrerer AT-Befehle sind diese mit einem : Doppelpunkt zu trennen. • reset: Setzt das Modem zurück.
interfaces serial restart-serserver	Startet den seriellen Kommunikationsdienst neu.
interfaces switch swport *port* clearportstats	Löscht die Statistiken für den ausgewählten Port.

Parameter	Beschreibung
services dhcpserver show-active-leases	Zeigt aktive DHCP-Leases an.

Abschnitt 2.5.10.4

Administrationsbefehle

Der Betriebszustand bietet Befehle zum Durchführen von Administrationsaufgaben für das Gerät.

Parameter	Beschreibung
admin acknowledge-all-alarms	Quittiert alle Systemalarme.
admin clear-all-alarms	Löscht alle Systemalarme.
admin delete-all-ssh-known-hosts	Löscht die Liste der bekannten Hosts.
admin delete-ssh-known-hosts	Löscht den Hosteintrag aus der Liste der bekannten Hosts.
admin restore-factory-defaults	Stellt die werkseitig voreingestellte Konfiguration und die werkseitigen Einstellungen wieder her, löscht jedoch keine Dateien, die Sie auf dem Gerät gespeichert haben.
admin reboot	Startet das Gerät neu.
admin restore-factory-defaults	Stellt die werkseitig voreingestellte Konfiguration und die werkseitigen Einstellungen wieder her, löscht jedoch keine Dateien, die Sie auf dem Gerät gespeichert haben.
admin set-system-clock time *YYYY-MM-DD HH:MM:SS*	Stellt das Datum und die Uhrzeit auf dem Gerät ein. Um nur das Datum anzugeben, verwenden Sie das Format *YYYY-MM-DD*. Um nur die Uhrzeit anzugeben, verwenden Sie das Format *HH:MM:SS*. Um Datum und Uhrzeit anzugeben, setzen Sie die Zeichenkette in Anführungszeichen und verwenden das Format *"YYYY-MM-DD HH:MM:SS"*. **HINWEIS** *Beim Einstellen der Uhrzeit ist die Angabe der Sekunden (SS) optional.*
admin shutdown	Fährt das Gerät herunter. Weitere Informationen zum Herunterfahren des Geräts finden Sie unter Abschnitt 4.5, „Das Gerät herunterfahren“
admin software-upgrade decline-upgrade	Bricht ein gerade durchgeführtes Software-Upgrade ab (oder lehnt es ab), das auf einen Neustart der aktualisierten Partition wartet.
admin software-upgrade launch-upgrade	Startet ein Upgrade auf der alternativen Partition.
admin software-upgrade rollback-reboot	Startet eine Vorgängerversion der Software auf der alternativen Partition.
maint-login	**ACHTUNG!** *Konfigurationsgefahr – Gefahr von Datenverlust/Beschädigung. Der Wartungsmodus dient zur Fehlersuche und sollte nur von Siemens Canada Ltd-Technikern verwendet werden. Der Wartungsmodus dient zur Fehlersuche und es sind nicht sämtliche möglichen Befehle dokumentiert. Eine falsche*

Parameter	Beschreibung
	Anwendung der im Wartungsmodus verfügbaren Befehle kann den Betriebszustand des Geräts beschädigen und das Gerät unzugänglich machen. Meldet sich beim zugrunde liegenden Betriebssystem als Stammbenutzer an. Der Benutzer muss ein Administrator sein und das Passwort für die Wartungsanmeldung eingeben können.
monitor start *filename*	Startet die Anzeige des angegebenen Systemprotokolls und das Tracing der angegebenen Datei. Bei Bedarf kann die Ausgabe in eine Datei umgeleitet werden. Informationen zum Umleiten der Ausgabe finden Sie unter Abschnitt 2.5.6, „Ausgabeumleitung verwenden“. Mit der Autovervollständigung können Sie eine Liste der verfügbaren Protokolle und Dateien anzeigen.
monitor stop *filename*	Stoppt die Anzeige des angegebenen Systemprotokolls und das Tracing der angegebenen Datei. Mit der Autovervollständigung können Sie eine Liste der verfügbaren Protokolle und Dateien anzeigen.
reportstats	Zeigt eine umfangreiche Zusammenstellung gerätespezifischer Statistiken an. Bei Bedarf kann die Ausgabe in eine Datei umgeleitet werden. Informationen zum Umleiten der Ausgabe finden Sie unter Abschnitt 2.5.6, „Ausgabeumleitung verwenden“.
config private	Geht in den Konfigurationsmodus, in dem der Benutzer Änderungen am System vornehmen kann. Dies ist der primäre Modus für die meisten Benutzer, die Änderungen an der Geräte-/Netzwerkkonfiguration vornehmen möchten. Der Zugriff ist für mehrere Bediener- und Admin-Benutzer möglich. Alle in einer privaten Konfigurationssitzung vorgenommenen Änderungen werden vor den anderen Benutzern solange verborgen, bis sie festgeschrieben werden. Jede Änderung muss festgeschrieben werden, damit sie ins aktive System übernommen wird. Wenn ein Benutzer während der privaten Konfigurationssitzung eines anderen Benutzers eine exklusive Konfigurationssitzung eröffnet, kann der Benutzer in der privaten Konfigurationssitzung seine Änderungen erst festschreiben, wenn der andere Benutzer seine Sitzung beendet.
config exclusive	Geht in den Konfigurationsmodus, in dem der Benutzer Änderungen am System vornehmen kann. Dieser Modus ähnelt dem privaten Konfigurationsmodus, mit der Ausnahme, dass alle anderen Benutzer ihre Änderungen erst festschreiben können, wenn der Benutzer den exklusiven Konfigurationsmodus beendet. Es kann pro Gerät jeweils nur ein Bediener- oder Admin-Benutzer den exklusiven Konfigurationsmodus nutzen. Verwenden Sie beim Festschreiben der Änderungen im exklusiven Konfigurationsmodus die bestätigte Option zum Festlegen eines Timeout-Zeitraums. Die Änderungen werden für den festgelegten Zeitraum angewendet, nach dem die Konfiguration wieder auf ihre vorherigen Einstellungen zurückgesetzt wird. Dadurch kann der Benutzer seine Konfigurationsänderungen testen, bevor diese vollständig ins aktive System übernommen werden. Weitere Informationen zur bestätigten Option finden Sie unter Abschnitt 2.5.10.5, „Allgemeine Befehle für den Konfigurationsmodus“. **WICHTIG!** *Melden Sie sich stets vom exklusiven Konfigurationsmodus ab oder beenden Sie die Transaktion. Wenn die Sitzung beendet wird, bevor ein Benutzer sie ordnungsgemäß beendet, können andere am Gerät angemeldete Benutzer weiterhin keine Änderungen vornehmen, solange der Timeout-Zeitraum der Sitzung noch nicht abgelaufen ist.*

Abschnitt 2.5.10.5

Allgemeine Befehle für den Konfigurationsmodus

Der Konfigurationsmodus bietet eine Reihe von allgemeinen Befehlen, die der Benutzer für die Arbeit mit Konfigurationsdaten verwenden kann.

Parameter	Beschreibung
abort	Beendet die Konfigurationssitzung, ohne die Änderungen zu speichern. **HINWEIS** *In einer exklusiven Bearbeitungssitzung werden anstehende unbestätigte Festschreibungen erst abgebrochen, wenn deren Timeout-Zeitraum abläuft. Eine neue exklusive Bearbeitungssitzung kann erst eröffnet werden, wenn der Timeout-Zeitraum abgelaufen ist.*
clear	Löscht alle Konfigurationsänderungen.
commit no-confirm	Schreibt die aktuellen Konfigurationsänderungen sofort fest. Dieser Befehl fordert den Benutzer auf, den Vorgang zu bestätigen. Verwenden Sie den Parameter `no-confirm`, um die Konfiguration wiederherzustellen, ohne dass eine Bestätigung erforderlich ist.
commit abort	In einer exklusiven Bearbeitungssitzung bricht dieser Befehl sämtliche bestätigte Festschreibungen ab.
commit and-quit	Schreibt alle bestätigen und unbestätigten Änderungen fest und beendet den Konfigurationsmodus.
commit check	Validiert die aktuelle Konfiguration.
commit confirmed *timeout*	Schreibt Änderungen vorübergehend für einen bestimmten Zeitraum fest, so dass der Benutzer die Konfiguration testen kann, bevor die Änderungen vollständig festgeschrieben werden. Die Änderungen müssen mit einem Standardbefehl **commit** festgeschrieben werden, bevor der Timeout-Zeitraum endet. Wenn die Änderungen vor dem Ende des Timeout-Zeitraums nicht festgeschrieben werden, werden sie automatisch verworfen und die vorherigen Einstellungen wiederhergestellt. Ein Timeout-Zeitraum kann am Ende des Befehls angegeben werden. Der Standardwert für den Timeout-Zeitraum beträgt 10 Minuten. Der Mindestwert für den Timeout-Zeitraum beträgt 1 Minute. Beispiel: `ruggedcom(config-admin)# commit confirmed 2` Um eine Festschreibung abzubrechen, bevor der Zeitraum abläuft, und die Änderungen zu verwerfen, geben Sie Folgendes ein: **commit** abort Um die Änderungen dauerhaft festzuschreiben, bevor der Zeitraum abläuft, geben Sie Folgendes ein: **commit**
commit comment *text*	Schreibt die aktuellen Konfigurationsänderungen zusammen mit einem benutzerspezifischen Kommentar sofort fest. Der Kommentar wird neben der Festschreibung in einer Liste anstehender Festschreibungen angezeigt.
commit label *text*	Schreibt die aktuellen Konfigurationsänderungen zusammen mit einer benutzerspezifischen Kennzeichnung sofort fest. In einer Liste anstehender Festschreibungen wird statt der automatisch generierten Festschreibe-ID die Kennzeichnung angezeigt.
commit persist-id *text*	Schreibt die aktuellen Konfigurationsänderungen sofort fest und weist eine benutzerspezifische ID oder einen Merker zu.
commit save-running *file*	Schreibt die aktuellen Konfigurationsänderungen sofort fest und speichert sie in der angegebenen Datei. Es wird nicht die vollständige laufende Konfiguration gespeichert.
copy	Kopiert ein konfiguriertes Element in ein neues Element. Beispiel: Der folgende Befehl kopiert die Benutzer-ID *admin* in die neue Benutzer-ID *wsmith*: `ruggedcom(config)# copy admin users userid admin smith`

Parameter	Beschreibung
	Das neue Element hat alle Attribute des Elements, aus dem es kopiert wurde. In diesem Beispiel hat die Benutzer-ID *wsmith* die gleichen Attribute für Passwort und Rolle wie die Benutzer-ID *admin*.

details	Bei Verwendung in Kombination mit dem Befehl **save**, schließt der Befehl **details** Standardwerte in die gespeicherte Konfigurationsdatei ein. Beispiel:
	`ruggedcom(config)# save {Dateiname} | details`
	Der Befehl details kann auch zum Anzeigen von Standard-Konfigurationswerten verwendet werden. Beispiel:
	`ruggedcom(config)# show running-config admin session-limits | details`

do	Führt einen Betriebszustandsbefehl aus. Beispiel: Der folgende Befehl führt den Betriebszustandsbefehl **ping** in der Sitzung im Konfigurationsmodus aus: `ruggedcom(config)# do ping 172.30.134.12`
end	Beendet die Konfigurationssitzung. Das System fordert den Benutzer auf, noch nicht festgeschriebene Änderungen festzuschreiben.
exit	Beendet den aktuellen Modus. Im Gegensatz zum Befehl **end** fordert das System den Benutzer nicht auf, noch nicht festgeschriebene Änderungen festzuschreiben.
help command	Zeigt Hilfeinformationen zum angegebenen Befehl an.
load [merge | override] *filename*	Lädt eine Konfiguration aus einer ASCII-CLI-Konfigurationsdatei. Für den CLI-Befehl stehen zwei Parameter zur Verfügung: override und merge. • **Override:** Dieser Parameter ist für Benutzer geeignet, die eine vollständige Konfigurationsdatei gespeichert haben und diese wieder zurück auf das Gerät laden möchten. Die vollständige Konfigurationsdatei kann zuvor mit dem auf oberster Ebene im Konfigurationsbaum ausgeführten CLI-Befehl **save** oder mit dem Befehl **admin** full-configuration-save erstellt worden sein. Mit dem Parameter override wird die gesamte laufende Konfiguration mit dem Inhalt der Konfigurationsdatei überschrieben. Die Override-Option hat die folgenden Einschränkungen: ▫ Die Konfigurationsdatei muss eine *vollständige* Konfiguration für das Gerät enthalten. Eine *vollständige* Konfiguration umfasst den gesamten Konfigurationsbaum. ▫ Der Befehl **load** muss an der Basis des Konfigurationsbaums aufgerufen werden. • **Merge:** Dieser Parameter ist für Benutzer geeignet, die eine Vorlagenkonfiguration generieren und diese auf viele Geräte laden möchten. Die Vorlagen-Konfigurationsdatei kann über den CLI-Befehl **save** erstellt werden. Mit dem Parameter merge wird der Inhalt der Konfigurationsdatei mit der laufenden Konfiguration zusammengeführt. Die verbleibenden Konfigurationen, die nicht in der Konfigurationsdatei enthalten sind, werden nicht geändert. Nach dem Laden der Konfiguration verwenden Sie den Befehl **commit**, um die Änderungen festzuschreiben.
move ip *interface* ipv4 address *address* [after | before | first | last] *address*	Verschiebt eine vorhandene IPv4-Adresse an eine neue Position in der Liste der Adressen. Die Adresse kann an die erste oder letzte (Standard) Position in der Liste oder vor oder nach eine andere Adresse verschoben werden. Beispiel: Der folgende Befehl verschiebt 172.30.137.37/9 vor 172.30.137.31/19: `ruggedcom(config)# move ip fe-3-1 ipv4 address 172.30.137.37/19 before 172.30.137.31/19`
no	Negiert einen Befehl oder setzt ihn auf seine Standardeinstellung zurück. Beispiel: Der folgende Befehl löscht die IP-Adresse 172.30.137.37/19:

Parameter	Beschreibung

	`ruggedcom(config)# no ip fe-3-1 ipv4 address 172.30.137.37/19`
	
	HINWEIS
	Der Befehl **no** *wirkt sich nur auf den explizit im Befehl angegebenen Parameter oder die Einstellung des Knotens aus. Wenn Sie mit dem Befehl* **no** *einen Parameter oder eine Einstellung mit Abhängigkeiten negieren, werden durch Löschen des angegebenen Parameters nicht die zugehörigen Abhängigkeiten gelöscht.*
	Beispiel: Der folgende Befehl fügt eine IPv4-Route mit einem Gateway hinzu:
	`ruggedcom(config)# routing ipv4 route 192.168.33.0/24 via 192.168.11.2`
	Der folgende Befehl löscht das Gateway, jedoch nicht die Route:
	`ruggedcom(config)# no routing ipv4 route 192.168.33.0/24 via 192.168.11.2`
	Der Befehl **no** *löscht nur den explizit angegebenen Parameter bzw. das explizit angegebene Objekt.*

pwd	Zeigt den Pfad zum aktuellen Knoten an. Beispiel: Nach der Navigation zu einer IPv4-Adresse zeigt der folgende Befehl den Pfad durch die Befehlshierarchie zum aktuellen Knoten an: `ruggedcom(config-address-172.30.137.31/19)# pwd Current submode path: ip fe-3-1 \ ipv4 \ address 172.30.137.31/19`
rename	Ändert den Wert eines Parameters. Beispiel: Der folgende Befehl ändert die IPv4-Adresse 172.30.137.36/19 in 172.30.137.40/19: `ruggedcom(config)# rename ip fe-3-1 ipv4 address 172.30.137.36/19 172.30.137.40/19`
resolved	Setzen Sie diesen Befehl ab, wenn Konflikte aufgelöst wurden. Konflikte werden normalerweise beim Festschreiben erkannt. Konflikte entstehen typischerweise, wenn mehrere Benutzer die gleichen Teile einer Konfiguration bearbeiten.
revert `no-confirm`	Kopiert die laufende Konfiguration in die aktuelle Konfiguration. Dabei werden alle Änderungen an der aktuellen Konfiguration verworfen. Dieser Befehl fordert den Benutzer auf, den Vorgang zu bestätigen. Verwenden Sie den Parameter `no-confirm`, um die Konfiguration wiederherzustellen, ohne dass eine Bestätigung erforderlich ist.

rollback `configuration` *number*	Setzt die Konfiguration auf eine zuvor festgeschriebene Konfiguration zurück. Das System speichert eine begrenzte Anzahl alter Konfigurationen. Nachdem die maximale Anzahl alter Konfigurationen erreich ist, wird durch Speichern einer neuen Konfiguration die älteste Konfiguration in der Liste gelöscht. Die zuletzt festgeschriebene Konfiguration (die laufende Konfiguration) erscheint als Element 0 in der Liste. Wählen Sie in der Liste eine Nummer aus und drücken Sie **Enter**.
	`ruggedcom(config)# rollback configuration`
	`Possible completions:`
	`0 2012-01-08 13:51:46 by admin via cli`
	`1 2012-01-08 13:50:58 by admin via cli`
	`2 2012-01-08 12:05:46 by admin via cli`
	`3 2012-01-08 10:47:42 by admin via cli`
	`4 2012-01-08 07:49:38 by admin via cli`
	`5 2012-01-08 07:46:14 by admin via cli`
	`ruggedcom(config)# rollback configuration`

Parameter	Beschreibung
	Nach dem Rollback der Konfiguration verwenden Sie den Befehl **commit**, um die Änderungen festzuschreiben.

save *filename*	Speichert die aktuelle Konfiguration ohne Standardwerte in eine ASCII-Datei. Geben Sie einen Dateinamen für die Datei an.
	Unter *aktuelle Konfiguration* ist die Konfiguration auf der aktuellen Ebene des Benutzers in der Hierarchie der Konfigurationsdaten zu verstehen. Beispiel: Wenn sich der Benutzer auf oberster Ebene befindet, speichert der Befehl **save** die vollständige Konfiguration des Geräts.
	`ruggedcom(config)# save {Dateiname-vollständige-Konfiguration}`
	Wenn sich der Benutzer auf einer anderen Ebene als der obersten befindet, z. B. auf der Ebene *firewall*, speichert der Befehl **save** eine Teilkonfiguration der aktuellen Ebene.
	`ruggedcom(config)#security firewall`
	`ruggedcom(config-firewall)# save {Dateiname-Firewall-Konfiguration}`
	Verwenden Sie diesen Befehl zusammen mit dem Befehl **details**, um Standardwerte in die gespeicherte Konfigurationsdatei einzuschließen. Beispiel:
	`ruggedcom(config)# save {Dateiname} | details`

show	Zeigt Parser-Informationen zu Konfiguration, Verlauf oder Befehlszeilenschnittstelle an. Geben Sie **show** ein und drücken Sie die **Tab**-Taste, um durch die zum Anzeigen verfügbaren Elemente zu navigieren. Dieser Befehl kann auch mit dem Befehl **details** verbunden werden, um die Standard-Konfigurationswerte anzuzeigen. Beispiel: `ruggedcom# show running-config admin session-limits | details`
top command	Geht zur obersten Ebene der Befehlshierarchie und führt optional einen Befehl aus.
validate	Validiert die aktuelle Konfiguration.
wizard [rox_flash | rox_upgrade]	Führt den Assistenten rox_flash oder rox_upgrade aus. Weitere Informationen finden Sie unter Abschnitt 4.15.5.2, „Downgrade mittels ROXflash“ und Abschnitt 4.15.3, „Upgrade der Software RUGGEDCOM ROX II“.

Abschnitt 2.6

Konfigurieren der CLI-Schnittstelle

Folgende Befehle können zum Konfigurieren bestimmter Eigenschaften und Anpassen der CLI-Schnittstelle verwendet werden.

Parameter	Beschreibung
autowizard { true | false }	Im aktivierten Zustand zeigt die CLI eine Aufforderung für erforderliche Einstellungen an, wenn eine neue Kennung erstellt wurde.
clear history	Löscht den CLI-Verlauf.
display-level	Legt die Tiefe der in den Befehlsergebnissen anzuzeigenden hierarchischen Informationen fest.
history *integer*	Legt die Anzahl der im CLI-Verlauf aufzuzeichnenden Elemente fest.

Parameter	Beschreibung
output-file { *filename* | terminal }	Leitet die CLI-Ausgabe an die angegebene ASCII-Textdatei oder an das Terminal weiter. Die Ausgabe wird solange an das angegebene Ziel geleitet, bis ein anderes Ziel mit einem nachfolgenden Befehl **output-file** festgelegt wird.
paginate { true | false }	Die Längenausgabe wird standardmäßig paginiert. Wenn die Ausgabe die Einstellung "screen-length" erreicht, fordert die CLI den Benutzer zum Drücken einer Taste für weitere Ausgabe auf. Drücken Sie auf **Enter**, um zeilenweise fortzufahren, oder auf **Space**, um seitenweise fortzufahren. Im deaktivierten Zustand wird die Ausgabe nicht paginiert.
screen-length *integer*	Legt die Anzahl an Zeilen auf einer Terminal-Seite fest.
screen-width *integer*	Legt die Länge der Terminal-Zeilen fest.
show-defaults { true | false }	Legt fest, ob Standardwerte beim Anzeigen der Konfiguration angezeigt werden. Im aktivierten Zustand werden die Standardwerte als Kommentare hinter dem konfigurierten Wert angezeigt. Im folgenden Beispiel wird der Standardwert für den Kontaktwert als Kommentar gefolgt von der konfigurierten Kontaktzeichenfolge von *wsmith@example.com* angezeigt: `ruggedcom# show running-config admin contact admin contact "wsmith@example.com" ! Contact !` Standardwerte werden nur für Parameter mit Standardwerten angezeigt. Hat ein Parameter keinen Standardwert, wird kein Standardwert angezeigt, wenn **show-defaults** auf "true" gesetzt ist.
terminal { dumb | vt100 | xterm | linux | ansi }	Legt den Terminal-Typ fest und steuert die Zeilenbearbeitung. Unterstützte Terminals sind: "dumb", "vt100", "xterm", "linux" und "ansi". Andere Terminals funktionieren möglicherweise auch, werden jedoch nicht explizit unterstützt.

Abschnitt 2.7

Auf die verschiedenen Modi zugreifen

Neben dem normalen Betriebsmodus gibt es drei weitere Modi in RUGGEDCOM ROX II, die verschiedene Arten der Steuerung des Betriebssystems erlauben.

INHALT

- Abschnitt 2.7.1, „Zugreifen auf den BIST-Modus“
- Abschnitt 2.7.2, „Zugreifen auf den Servicemodus“
- Abschnitt 2.7.3, „Auf den Wartungsmodus zugreifen“

Abschnitt 2.7.1

Zugreifen auf den BIST-Modus

Der BIST-Modus (Built-In-Self-Test) wird vom RUGGEDCOM ROX II zum Testen und Konfigurieren interner Funktionen auf dem Gerät verwendet. Das Verfahren für den Zugriff auf den BIST-Modus weicht ab, falls ein neues Software-Image auf die Flash-Karte gespielt wurde.

ACHTUNG!
Sicherheitsgefahr – Risiko des unbefugten Zugriffs und/oder Missbrauchs. Der Zugriff auf den BIST-Modus sollte ausschließlich auf Admin-Benutzer beschränkt werden.

ACHTUNG!
Konfigurationsrisiko - Gefahr der Datenbeschädigung. Der BIST-Modus dient zur Fehlersuche und der erweiterten Konfiguration und sollte nur von Siemens Canada Ltd-Technikern verwendet werden. Daher ist dieser Modus nicht vollständig dokumentiert. Eine falsche Anwendung der in diesem Modus verfügbaren Befehle kann den Betriebszustand des Geräts beschädigen und unzugänglich machen.

HINWEIS
Der BIST-Modus öffnet Port 222.

Um auf den BIST-Modus normal zuzugreifen, gehen Sie wie folgt vor:

WICHTIG!
Verbinden Sie das Gerät nicht mit dem Netzwerk, wenn es sich im BIST-Modus befindet. In diesem Modus erzeugt das Gerät einen übermäßigen Multicast-Datenverkehr.

1. Trennen Sie das Gerät vom Netzwerk.
2. Stellen Sie eine Verbindung zum RUGGEDCOMRX1400 über die RS-232-Konsolenverbindung und eine Terminal-Anwendung her. Weitere Informationen finden Sie unter Abschnitt 3.1.2, „Herstellen einer Direktverbindung“.
3. Starten Sie das Gerät neu. Weitere Informationen finden Sie unter Abschnitt 4.6, „Gerät neu booten“.
4. Bei Aufforderung geben Sie das Boot-Passwort bzw. die Boot-Passphrase für das Gerät ein.
5. Sobald das Gerät mit dem Neustart beginnt, drücken Sie auf **ESC**. Eine Liste der möglichen Boot-Modi wird für jede Partition angezeigt.

```
****Boot Partition 4****
 [4-0]: Debian GNU/Linux, kernel 3.0.0-2-8360e
 [4-1]: Debian GNU/Linux, kernel 3.0.0-2-8360e (BIST mode)
 [4-2]: Debian GNU/Linux, kernel 3.0.0-2-8360e (single-user mode)
 [4-3]: Debian GNU/Linux, kernel 3.0.0-2-8360e (service mode)

 ****Boot Partition 6****
 [6-0]: Debian GNU/Linux, kernel 3.0.0-2-8360e
 [6-1]: Debian GNU/Linux, kernel 3.0.0-2-8360e (BIST mode)
 [6-2]: Debian GNU/Linux, kernel 3.0.0-2-8360e (single-user mode)
 [6-3]: Debian GNU/Linux, kernel 3.0.0-2-8360e (service mode)

 Auto booting [4-0], Hit [ESC] key to stop:  0
 Welcome to the boot menu. Please select from the following options:

 Enter [BootPartition-BootTarget] (e.g. '4.0') to boot.
 'h' Show this help menu
 'l' List the available boot targets
 'c' Exit to the boot loader command line

 Will reboot after 60 seconds of inactivity
 :
```

HINWEIS
Im vorstehenden Beispiel gibt der Text `Auto booting [4-0]` *an, dass Boot Partition 4 die aktive Partition ist.*

6. Rufen Sie den Boot-Modus auf der aktiven Partition auf, indem Sie die zugehörige Zielnummer eingeben. Wenn beispielsweise Boot Partition 6 die aktive Partition ist, dann geben Sie **6-1** ein und bestätigen Sie mit **Enter**. Daraufhin beginnt der Selbsttestzyklus.
7. Drücken Sie **Strg+C**, um den Selbsttestzyklus zu stoppen und den übermäßigen Multicast-Datenverkehr anzuhalten. Eine BIST-Aufforderung wird angezeigt.

```
BIST:~#
```

Um nach dem Aufspielen eines neuen Software-Image auf die Flash-Karte auf den BIST-Modus zuzugreifen, gehen Sie wie folgt vor:

1. Stellen Sie eine Verbindung zum RUGGEDCOMRX1400 über die RS-232-Konsolenverbindung und eine Terminal-Anwendung her. Weitere Informationen finden Sie unter Abschnitt 3.1.2, „Herstellen einer Direktverbindung“.
2. Schalten Sie die Stromversorgung am Gerät aus und wieder ein.
3. Bei Aufforderung geben Sie das Boot-Passwort bzw. die Boot-Passphrase für das Gerät ein.
4. Drücken Sie **Strg+C**, um den Selbsttestzyklus zu stoppen und den übermäßigen Multicast-Datenverkehr anzuhalten. Eine BIST-Aufforderung wird angezeigt.

```
BIST:~#
```

Nachdem alle Konfigurationsänderungen bzw. Tests abgeschlossen sind, ist eine Änderung des Boot-Modus erforderlich. Gehen Sie dazu wie folgt vor:

1. Setzen Sie den nächsten Neustart auf "normal", indem Sie Folgendes eingeben:

```
nextboot normal
```

2. Starten Sie das Gerät neu, indem Sie Folgendes eingeben:

```
reboot
```



ACHTUNG!
Sicherheitsgefahr – Risiko des unbefugten Zugriffs und/oder Missbrauchs. Stellen Sie nach dem Zugriff auf den BIST-Modus auf einem mit einem Netzwerk verbundenen Gerät sicher, dass SSH deaktiviert ist. Wenn SSH nach dem Zugriff auf den BIST-Modus nicht deaktiviert wird, dann könnte jede Person mit Fernzugriff auf das Gerät und das Root-Passwort auf die Linux-Shell zugreifen.



HINWEIS
SSH wird automatisch aktiviert, sobald das Gerät im Normalmodus neu gestartet ist. Eine manuelle Aktivierung ist möglich, indem Sie Folgendes eingeben:

```
/etc/init.d/ssh start
```

3. Sobald das Gerät neu gestartet ist, deaktivieren Sie sofort SSH, indem Sie Folgendes eingeben:

```
/etc/init.d/ssh stop
```

4. Verbinden Sie das Gerät mit dem Netzwerk.

Abschnitt 2.7.2

Zugreifen auf den Servicemodus

Der Servicemodus gewährt Zugriff auf die Linux-Shell.

Um auf den Servicemodus zuzugreifen, gehen Sie wie folgt vor:

ACHTUNG!
Konfigurationsrisiko - Gefahr der Datenbeschädigung. Der Servicemodus dient zur Fehlersuche und der erweiterten Konfiguration und sollte nur von Siemens-Technikern verwendet werden. Daher ist dieser Modus nicht vollständig dokumentiert. Eine falsche Anwendung der in diesem Modus verfügbaren Befehle kann den Betriebszustand des Geräts beschädigen und unzugänglich machen.

ACHTUNG!
Sicherheitsgefahr – Risiko des unbefugten Zugriffs und/oder Missbrauchs. SSH wird an Port 222 automatisch aktiviert, wenn das Gerät in den Servicemodus versetzt wird. Wenn das Gerät mit dem Netzwerk verbunden ist, könnte ein Benutzer mit Fernzugriff auf das Gerät und das Root-Passwort auf die Linux-Shell zugreifen. Bei Bedarf schützen Sie das Gerät wie folgt:

- *Trennen Sie das Gerät vom Netzwerk*
- *Deaktivieren Sie SSH über den Wartungsmodus, bevor Sie auf den Servicemodus zugreifen*

WICHTIG!
Änderungen an der Konfiguration in diesem Modus überschreiben die aktuellen Konfigurationseinstellungen (z. B. IP-Adressen, VLAN-Einstellungen, usw.), werden aber nach einem Neustart des Systems verworfen.

1. Stellen Sie eine Verbindung zum RUGGEDCOM ROX II über die RS-232-Konsolenverbindung und eine Terminal-Anwendung her. Weitere Informationen finden Sie unter Abschnitt 3.1.2, „Herstellen einer Direktverbindung“.
2. Starten Sie das Gerät neu. Weitere Informationen finden Sie unter Abschnitt 4.6, „Gerät neu booten“.
3. Sobald das Gerät mit dem Neustart beginnt, drücken Sie auf **ESC**. Eine Liste der möglichen Boot-Modi wird für jede Partition angezeigt.

```
****Boot Partition 4****
 [4-0]: Debian GNU/Linux, kernel 3.0.0-2-8360e
 [4-1]: Debian GNU/Linux, kernel 3.0.0-2-8360e (BIST mode)
 [4-2]: Debian GNU/Linux, kernel 3.0.0-2-8360e (single-user mode)
 [4-3]: Debian GNU/Linux, kernel 3.0.0-2-8360e (service mode)

 ****Boot Partition 6****
 [6-0]: Debian GNU/Linux, kernel 3.0.0-2-8360e
 [6-1]: Debian GNU/Linux, kernel 3.0.0-2-8360e (BIST mode)
 [6-2]: Debian GNU/Linux, kernel 3.0.0-2-8360e (single-user mode)
 [6-3]: Debian GNU/Linux, kernel 3.0.0-2-8360e (service mode)

 Auto booting [4-0], Hit [ESC] key to stop:  0
 Welcome to the boot menu. Please select from the following options:

 Enter [BootPartition-BootTarget] (e.g. '4.0') to boot.
 'h' Show this help menu
 'l' List the available boot targets
 'c' Exit to the boot loader command line

 Will reboot after 60 seconds of inactivity
 :
```

HINWEIS
Im vorstehenden Beispiel gibt der Text `Auto booting [4-0]` *an, dass Boot Partition 4 die aktive Partition ist.*

4. Rufen Sie den Servicemodus auf der aktiven Partition auf, indem Sie die zugehörige Zielnummer eingeben. Wenn beispielsweise Boot Partition 6 die aktive Partition ist, dann geben Sie **6–3** ein. Eine Anmeldeaufforderung für den Servicemodus wird angezeigt.
5. Geben Sie `root` ein und drücken Sie **Enter**. Sie werden aufgefordert, ein Passwort einzugeben.

HINWEIS
Falls kein eindeutiges Passwort bzw. keine eindeutige Passphrase konfiguriert wurde, verwenden Sie das werkseitig eingestellte Passwort. Weitere Informationen finden Sie unter *Abschnitt 2.1, „Voreingestellte Benutzernamen und Passwörter“*.

HINWEIS
Das aktuelle Passwort bzw. die aktuelle Passphrase für den Servicemodus ist mit dem Passwort bzw. der Passphrase für den Zugriff auf den Wartungsmodus identisch.

6. Geben Sie das aktuelle Passwort bzw. die aktuelle Passphrase für den Servicemodus ein und bestätigen Sie mit **Enter**.

```
ruggedcom login: root
 Password:
 Last login: Tue Oct 13 13:37:38 EDT 2020 on ttyS0
 Linux ruggedcom 3.0.0-2-8360e #1 Thu Jan 24 21:20:30 UTC 2013 ppc

 The programs included with the Debian GNU/Linux system are free software;
 the exact distribution terms for each program are described in the
 individual files in /usr/share/doc/*/copyright.

 Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
 permitted by applicable law.
                                                                    8t-eterminal size
 now 80x20

 Welcome to ruggedcom Partition1 (Rev ROX 2.4.0 (2013-01-24 18:20)) RX1510 SN
 12110102-0012-0030060017   13:42:07 up 7 min
 Temperature +38.5 C (+101.3 F)  Disk 24%  Memory 41%

 root@ruggedcom:~#
```

ACHTUNG!
Sicherheitsgefahr – Risiko des unbefugten Zugriffs und/oder Missbrauchs. Stellen Sie nach dem Zugriff auf den Servicemodus auf einem mit einem Netzwerk verbundenen Gerät sicher, dass SSH deaktiviert ist. Wenn SSH nach dem Zugriff auf den Servicemodus nicht deaktiviert wird, dann könnte jede Person mit Fernzugriff auf das Gerät und das Root-Passwort auf die Linux-Shell zugreifen.

Abschnitt 2.7.3
Auf den Wartungsmodus zugreifen

Der Wartungsmodus gewährt Zugriff auf die Linux-Shell.

Gehen Sie wie folgt vor, um auf den Wartungsmodus zuzugreifen:

ACHTUNG!
Konfigurationsrisiko - Gefahr der Datenbeschädigung. Der Wartungsmodus dient zur Fehlersuche und sollte nur von Siemens Canada Ltd-Technikern verwendet werden. Daher ist dieser Modus nicht vollständig dokumentiert. Eine falsche Anwendung der in diesem Modus verfügbaren Befehle kann den Betriebszustand des Geräts beschädigen und unzugänglich machen.

WICHTIG!
Änderungen an der Konfiguration in diesem Modus überschreiben die aktuellen Konfigurationseinstellungen (z. B. IP-Adressen, VLAN-Einstellungen usw.), werden aber nach einem Neustart des Systems verworfen.

1. Geben Sie im normalen Betriebszustand **`maint-login`** ein und drücken Sie **Enter**. Sie werden aufgefordert, ein Passwort einzugeben.

   HINWEIS
   Das aktuelle Passwort/die Passphrase des Wartungsmodus entspricht dem Passwort/der Passphrase für den Zugriff auf den Servicemodus.

2. Geben Sie das aktuelle Passwort/die Passphrase ein und bestätigen Sie mit **Enter**.

   Beispiel:

```
ruggedcom# maint-login
 Password:

 Welcome to ruggedcom Partition2 (Rev ROX 2.4.0 (2013-01-24 18:20)) RX1511 SN R15R-3410-PR061
 22:29:20 up 1 day,  8:42
 Temperature +41.0 C (+105.8 F)  Disk 25%  Memory 43%

 root@ruggedcom:~#
```

3 Erste Schritte

In diesem Abschnitt wird beschrieben, welche Aufgaben bei der erstmaligen Inbetriebnahme des Geräts auszuführen sind. Solche Aufgaben sind die Herstellung der Verbindung mit dem Gerät und der Zugang zur RUGGEDCOM ROX II CLI sowie das Konfigurieren eines Basis-Netzwerks.

INHALT

- Abschnitt 3.1, „Verbindung mit RUGGEDCOM ROX II herstellen “
- Abschnitt 3.2, „Ein Basis-Netzwerk konfigurieren“

Abschnitt 3.1

Verbindung mit RUGGEDCOM ROX II herstellen

Der Zugang zur Web-Benutzeroberfläche und zur Befehlszeilenschnittstelle (Command Line Interface, CLI) ist über eine direkte Verbindung zwischen einer Workstation und einem Gerät oder über eine entfernte Verbindung über das Netzwerk möglich.

INHALT

- Abschnitt 3.1.1, „Standard-IP-Adresse“
- Abschnitt 3.1.2, „Herstellen einer Direktverbindung“
- Abschnitt 3.1.3, „Herstellen einer entfernten Verbindung“

Abschnitt 3.1.1

Standard-IP-Adresse

Die Standard-IP-Adresse für das Gerät ist 192.168.0.2/24.

Abschnitt 3.1.2

Herstellen einer Direktverbindung

Auf die Befehlszeilenschnittstelle (CLI) kann über eine geeignete Kabelverbindung zwischen dem Gerät und einer Workstation direkt zugegriffen werden.

Um auf die Befehlszeilenschnittstelle (CLI) über eine Direktverbindung zum Gerät zuzugreifen, gehen Sie wie folgt vor:

1. Verbinden Sie eine Workstation, auf der eine Terminal-Emulationssoftware läuft, mit dem RS-232-Konsolen-Port am Gerät.

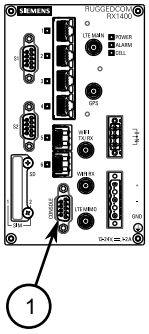


Abbildung 3: RS-232-Konsolen-Port

2. Konfigurieren Sie das Terminal folgendermaßen:
   - 57600 bps
   - Keine Parität
   - 8 Bits
   - Stellen Sie als Terminaltyp VT100 ein.
   - Deaktivieren Sie die Hardware- und Software-Flusskontrolle.
3. Stellen Sie eine Verbindung zum Gerät her und drücken Sie eine beliebige Taste. Die Anmeldeaufforderung wird angezeigt.

   ```
   {host name} login:
   ```
4. Loggen Sie sich bei RUGGEDCOM ROX II ein. Weitere Informationen finden Sie unter Abschnitt 2.2, „Anmelden“.

Abschnitt 3.1.3

Herstellen einer entfernten Verbindung

Auf die Befehlszeilenschnittstelle (CLI) kann sicher und dezentral mithilfe eines SSH-Clients zugegriffen werden.

Um auf die CLI zuzugreifen, gehen Sie wie folgt vor:

1. Starten Sie einen SSH-Client und legen Sie folgende Verbindungseinstellungen fest:
   - **Host Name:** Die IP-Adresse des Geräts oder die IP-Adresse, der das gewünschte Benutzerprofil als Präfix vorangestellt ist (z. B. admin@192.168.0.2)
   - **Port:** 22
2. Stellen Sie eine Verbindung zum Gerät her.
3. Falls der SSH-Schlüssel des Geräts nicht in der Registry der Workstation zwischengespeichert wurde, wird eine Meldung zur Bestätigung angezeigt, ob der Host vertrauenswürdig ist. Klicken Sie auf **Yes**, um fortzufahren. Die Anmeldeaufforderung wird angezeigt.

   ```
   login as:
   ```
4. Loggen Sie sich bei RUGGEDCOM ROX II ein. Weitere Informationen finden Sie unter Abschnitt 2.2, „Anmelden“.

Abschnitt 3.2

Ein Basis-Netzwerk konfigurieren

RUGGEDCOM ROX II verfügt über die folgenden standardmäßig konfigurierten Internet-Schnittstellen: *dummy0* und *switch.0001*. Die voreingestellten IP-Adressen für *switch.0001* werden unter ***ip » switch.0001 » ipv4*** konfiguriert. Die standardmäßige Schnittstelle *switch.0001* ist die VLAN-Schnittstelle. Sie ist nur dann sichtbar, wenn ein oder mehrere Ethernet-Line-Module installiert sind. Sie wird implizit erstellt, da alle geschalteten Ports eine voreingestellte PVID von 1 haben.

In der folgenden Tabelle sind die voreingestellten IP-Adressen aufgelistet.

Schnittstelle	IP Address
switch.0001	192.168.0.2/24

INHALT

- Abschnitt 3.2.1, „Konfigurieren eines IPv4-Basis-Netzwerks“
- Abschnitt 3.2.2, „Konfigurieren eines IPv6-Basis-Netzwerks“

Abschnitt 3.2.1

Konfigurieren eines IPv4-Basis-Netzwerks

Um ein IPv4-Basis-Netzwerk zu konfigurieren, gehen Sie wie folgt vor:

1. Wählen Sie zwei Switched-Ethernet-Ports und weisen Sie ihnen jeweils ein eindeutiges VLAN zu. Weitere Informationen über das Zuweisen von VLANs zu Switched-Ethernet-Ports finden Sie in Abschnitt 8.1.2, „Einen Switched-Ethernet-Port konfigurieren“.

   Für den Zweck dieses Verfahrens werden die Ports als VLAN 1 bzw. VLAN 2 bezeichnet.
2. Konfigurieren Sie eine IPv4-Adresse für die VLAN-Schnittstelle, die jeden Port repräsentiert, und stellen Sie sicher, dass die VLAN-2-Schnittstelle sich in einem anderen Subnetz befindet. Weitere Informationen finden Sie unter Abschnitt 7.1.3.2, „Eine IPv4-Adresse hinzufügen“.
3. Verbinden Sie einen Computer mit dem VLAN-1-Port.
4. Konfigurieren Sie den Computer, sodass er sich im selben Subnetz wie die VLAN-1-Schnittstelle befindet.
5. Konfigurieren Sie den Standard-Gateway für den Computer, sodass er dieselbe IPv4-Adresse wie die VLAN-1-Schnittstelle hat.
6. Verbinden Sie einen Switch eines IPv4-fähigen Netzwerks mit dem VLAN-2-Port.
7. Konfigurieren Sie alle Computer im IPv4-Netzwerk, sodass sie sich im selben Subnetz wie die VLAN-2-Schnittstelle befinden.
8. Konfigurieren Sie den Standard-Gateway für alle Computer im IPv4-Netzwerk, sodass er dieselbe IPv4-Adresse wie die VLAN-2-Schnittstelle hat.
9. Aktivieren Sie das System zum Schutz vor Brute-Force-Angriffen (BFA) auf dem Gerät. Weitere Informationen finden Sie unter Abschnitt 6.3, „Schutz vor Brute-Force-Angriffen aktivieren/deaktivieren“.
10. Stellen Sie sicher, dass alle mit dem Gerät verbundenen Computer sich gegenseitig Ping-Anfragen senden können.

Abschnitt 3.2.2

Konfigurieren eines IPv6-Basis-Netzwerks

Um ein IPv6-Basis-Netzwerk zu konfigurieren, gehen Sie wie folgt vor:

1. Wählen Sie zwei Switched-Ethernet-Ports und weisen Sie ihnen jeweils ein eindeutiges VLAN zu. Weitere Informationen über das Zuweisen von VLANs zu Switched-Ethernet-Ports finden Sie in Abschnitt 8.1.2, „Einen Switched-Ethernet-Port konfigurieren“.

   Für den Zweck dieses Verfahrens werden die Ports als VLAN 1 bzw. VLAN 2 bezeichnet.
2. Konfigurieren Sie eine IPv6-Adresse für die VLAN-Schnittstelle, die jeden Port repräsentiert, und stellen Sie sicher, dass die VLAN-2-Schnittstelle sich in einem anderen Subnetz befindet. Weitere Informationen finden Sie unter Abschnitt 7.1.4.2, „Eine IPv6-Adresse hinzufügen“.
3. Verbinden Sie einen Computer mit dem VLAN-1-Port.
4. Konfigurieren Sie den Computer, sodass er sich im selben Subnetz wie die VLAN-1-Schnittstelle befindet.
5. Konfigurieren Sie das Standard-Gateway für den Computer, sodass es dieselbe IPv6-Adresse wie die VLAN-1-Schnittstelle hat.
6. Verbinden Sie einen Switch eines IPv6-fähigen Netzwerks mit dem VLAN-2-Port.
7. Konfigurieren Sie alle Computer im IPv6-Netzwerk, sodass sie sich im selben Subnetz wie die VLAN-2-Schnittstelle befinden.
8. Konfigurieren Sie das Standard-Gateway für alle Computer im IPv6-Netzwerk, sodass es dieselbe IPv6-Adresse wie die VLAN-2-Schnittstelle hat.
9. Aktivieren Sie das System zum Schutz vor Brute-Force-Angriffen (BFA) auf dem Gerät. Weitere Informationen finden Sie unter Abschnitt 6.3, „Schutz vor Brute-Force-Angriffen aktivieren/deaktivieren“.
10. Aktivieren Sie IPv6 Neighbor Discovery. Weitere Informationen finden Sie unter Abschnitt 7.1.5, „Konfigurieren der IPv6 Neighbor Discovery“.
11. Stellen Sie sicher, dass alle mit dem Gerät verbundenen Computer sich gegenseitig Ping-Anfragen senden können.

4 Gerätemanagement

Dieses Kapitel beschreibt das Management der Geräte-Hardware einschließlich Ports, Dateien, Protokollen, Firmware usw.

INHALT

- Abschnitt 4.1, „Geräte- und Softwareinformationen anzeigen“
- Abschnitt 4.2, „Die GPS-Position des Geräts bestimmen“
- Abschnitt 4.3, „Chassis-Informationen und -Status anzeigen“
- Abschnitt 4.4, „Anzeigen der Teileliste“
- Abschnitt 4.5, „Das Gerät herunterfahren“
- Abschnitt 4.6, „Gerät neu booten“
- Abschnitt 4.7, „Auf Werkseinstellungen zurücksetzen“
- Abschnitt 4.8, „Außerbetriebnahme des Geräts“
- Abschnitt 4.9, „Anzeigen einer Liste der Line-Modul-Konfigurationen“
- Abschnitt 4.10, „Anzeigen von SFP-Informationen“
- Abschnitt 4.11, „Verwalten von Feature Keys“
- Abschnitt 4.12, „Dateien verwalten“
- Abschnitt 4.13, „Verwalten von Protokollen“
- Abschnitt 4.14, „Die Softwarekonfiguration verwalten“
- Abschnitt 4.15, „Ein Upgrade/Downgrade derRUGGEDCOM ROX II-Software ausführen“

Abschnitt 4.1

Geräte- und Softwareinformationen anzeigen

Bei der Fehlersuche oder bei der Bestellung neuer Geräte/Funktionen kann Siemens spezifische Informationen über das Gerät anfordern, wie z. B. Modell, Bestellcode (MLFB) oder System-Seriennummer.

Um allgemeine Angaben zum Gerät und seiner Software anzuzeigen, geben Sie Folgendes ein:

```
show chassis chassis-status
```

Eine Tabelle oder Liste ähnlich dem folgenden Beispiel wird angezeigt:

```
ruggedcom# show chassis chassis-status
chassis-status
 model                RX1400
 software license     "Layer 3 Security Edition"
 mlfb                 6GK60140AM2
 rox release          "ROX 2.7.0 (2014-12-17 11:49)"
```

```
system serial number RUMEN07068796
BootLoader           2014.04RR12
```

Diese Tabelle oder Liste liefert die folgenden Informationen:

Parameter	Beschreibung
model	**Zusammenfassung:** Eine Zeichenkette Der Modellname des RuggedCom-Geräts.
software-license	**Zusammenfassung:** Eine Zeichenkette Die aktuelle Funktionalität der Software.
mlfb	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 256 Zeichen MLFB (maschinenlesbare Produktbezeichnung) oder Bestellcode
rox-release	**Zusammenfassung:** Eine Zeichenkette Das ROX-Release für das Chassis. Dieser Parameter ist obligatorisch.
system-serial-number	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 32 Zeichen Die Seriennummer des Systems auf dem Chassisschild. Dieser Parameter ist obligatorisch.
BootLoader	**Zusammenfassung:** Eine Zeichenkette Die Version ROX-Bootloader-Software auf dem installierten Modul. Dieser Parameter ist obligatorisch.

Abschnitt 4.2

Die GPS-Position des Geräts bestimmen

Wenn GPS eingeschaltet ist, kann über RUGGEDCOM ROX II der Standort des Geräts bestimmt werden.

Um die GPS-Position des Geräts zu bestimmen, gehen Sie wie folgt vor:

```
interfaces cellmodem port lte gps-location
```

Erläuterung:

- *port* ist die Portnummer für das Modul

Die GPS-Position des Geräts wird dargestellt. Beispiel:

```
ruggedcom# interfaces cellmodem cel-1 lte gps-location
gps_location_reply

UTC time:  2015-03-18 19:25:20 UTC
Localtime: 2015-03-18 15:25:20 EDT
Latitude: 43 deg. 48.4717 min. N
Longitude: 079 deg. 32.4272 min. W
Number of satellites in view: 8
```

Abschnitt 4.3
Chassis-Informationen und -Status anzeigen

Dieser Abschnitt beschreibt, wie Sie Informationen über das Chassis des Geräts ansehen können, zum Beispiel seine Konfiguration und seinen Betriebsstatus.

INHALT

- Abschnitt 4.3.1, „Anzeigen der Steckplatz-Hardware“
- Abschnitt 4.3.2, „Flash-Card-Speicherbelegung anzeigen“
- Abschnitt 4.3.3, „Anzeigen des Steckplatz-Status“
- Abschnitt 4.3.4, „Status des Steckplatzsensors anzeigen“

Abschnitt 4.3.1
Anzeigen der Steckplatz-Hardware

Um eine Liste der in jedem Steckplatz installierten Hardware anzuzeigen, geben Sie Folgendes ein:

```
show chassis hardware slot-hardware
```

Eine Tabelle oder Liste ähnlich dem folgenden Beispiel wird angezeigt:

```
ruggedcom# show chassis hardware slot-hardware | tab ORDER SERIAL SLOT FIELD DETECTED MODULE NUMBER
 ------------------------------------------------- swport SM0001 SM M88E6097F, 4FT 2GP serport SER0001
 2xRS232/422/485 celport CELL0001 1x Cell LTE EU
```

Abschnitt 4.3.2
Flash-Card-Speicherbelegung anzeigen

Um die Speicherbelegungsstatistik für die im Gerät installierte Flash-Card anzusehen, geben Sie Folgendes ein:

```
show chassis storage
```

Eine Tabelle oder Liste ähnlich dem folgenden Beispiel wird angezeigt:

```
ruggedcom# show chassis storage | tab
storage
 flash
  storage name                "Flash"
  total capacity              994896
  current partition           "Partition #1"
  current partition capacity  490496
  secondary partition capacity 490496
  current partition usage     67
```

Diese Tabelle oder Liste liefert die folgenden Informationen:

Parameter	Beschreibung
storage-name	**Zusammenfassung:** Eine Zeichenkette mit 0 bis 32 Zeichen Die Art der Speicherung.
total-capacity	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 0 und 4294967295

Parameter	Beschreibung
	Die Gesamtkapazität des Flash-Speichers in kB. Dieser Parameter ist obligatorisch.
current-partition	**Zusammenfassung:** Eine Zeichenkette mit 0 bis 32 Zeichen Die Partition, auf der ROX derzeit ausgeführt wird und wovon ROX gestartet wird. Dieser Parameter ist obligatorisch.
current-partition-capacity	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 0 und 4294967295 Die Kapazität der aktuellen Partition in kB. Dieser Parameter ist obligatorisch.
secondary-partition-capacity	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 0 und 4294967295 Die Kapazität der sekundären Partition in kB. Dieser Parameter ist obligatorisch.
current-partition-usage	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 0 und 100 Die Auslastung in % der aktuellen Partition. Dieser Parameter ist obligatorisch.

Abschnitt 4.3.3
Anzeigen des Steckplatz-Status

Um den Gesamtstatus jedes Steckplatzes anzuzeigen, geben Sie Folgendes ein:

```
show chassis status slot-status
```

Eine Tabelle oder Liste ähnlich dem folgenden Beispiel wird angezeigt:

```
ruggedcom# show chassis status slot-status | tab STATUS START SLOT DETECTED MODULE STATE STRING UPTIME
 START DATE TIME
 ------------------------------------------------------------------------------------------------ cm CM
 TI-AM5726 variant 0001 operating Normal 0D 0hr 0min 0sec 2015-01-06Z 16:36:20Z
```

Diese Tabelleoder Liste liefert die folgenden Informationen:

Parameter	Beschreibung
slot	**Zusammenfassung:** { { --- }{ pm1, pm2, main }{ sm, lm1, lm2, lm3, lm4, lm5, lm6, swport, eth, serport, celport, wlanport }{ cm, em }{ trnk } } Der Name des Steckplatzes gemäß Siebdruckmarkierung auf der Chassisoberseite.
detected-module	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 60 Zeichen Die Typenspezifizierung des installierten Moduls. Dieser Parameter ist obligatorisch.
state	**Zusammenfassung:** { unknown, empty, disabled, resetting, operating, failed, disconnected } Der aktuelle Zustand des installierten Moduls. Dieser Parameter ist obligatorisch.
status-string	**Zusammenfassung:** Eine Zeichenkette Der Laufzeitzustand des installierten Moduls. Dieser Parameter ist obligatorisch.
uptime	**Zusammenfassung:** Eine Zeichenkette

Parameter	Beschreibung
	Die Gesamtzeit, die seit Beginn der Inbetriebnahme des installierten Moduls abgelaufen ist. Dieser Parameter ist obligatorisch.
start-date	**Zusammenfassung:** Eine Zeichenkette Das Datum, an dem das installierte Modul in Betrieb genommen wurde. Dieser Parameter ist obligatorisch.
start-time	**Zusammenfassung:** Eine Zeichenkette Die Uhrzeit, zu der das installierte Modul in Betrieb genommen wurde. Dieser Parameter ist obligatorisch.

Abschnitt 4.3.4
Status des Steckplatzsensors anzeigen

Um Informationen zum Steckplatzsensor anzuzeigen, geben Sie Folgendes ein:.

```
show chassis sensors
```

Eine Tabelle oder Liste ähnlich dem folgenden Beispiel wird angezeigt:

```
show chassis sensors sensors SLOT DETECTED MODULE TEMPERATURE CURRENT VOLTAGE
 ------------------------------------------------------------------------------------------ cm CM TI-AM5726
 variant 0001 38 wlanport 1x WLAN 802.11 US
```

Diese Tabelle oder Liste liefert die folgenden Informationen:

Parameter	Beschreibung
slot	**Zusammenfassung:** { { --- }{ pm1, pm2, main }{ sm, lm1, lm2, lm3, lm4, lm5, lm6, swport, eth, serport, celport, wlanport }{ cm, em }{ trnk } } Der Name des Steckplatzes gemäß Siebdruckmarkierung auf der Chassisoberseite.
detected-module	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 60 Zeichen Die Typenspezifizierung des installierten Moduls. Dieser Parameter ist obligatorisch.
temperature	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen -55 und 125 Die Temperatur des installierten Moduls, in Grad Celsius. Befinden sich mehrere Temperaturaufnehmer auf der Baugruppe, wird der höchste aufgezeichnete Wert gemeldet. Dieser Parameter ist obligatorisch.

Abschnitt 4.4
Anzeigen der Teileliste

Um eine Liste aller im Gerät installierten Teile anzuzeigen, geben Sie Folgendes ein:

```
show running-config chassis part-list
```

Falls Aufträge konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config chassis part-list | tab
MODEL   ORDERFIELD  PARTNUMBER                    PARTNAME
```

```
--------------------------------------------------------------------------------
RX1400  CELL0001    CELL-LTE-0.001  1x Cell LTE EU

                    DB-CELL-LTE-1.
                    001
RX1400  CELL0002    CELL-LTE-0.001  1x Cell LTE NAM A/R/B/T

                    DB-CELL-LTE-1.
                    002
RX1400  CELL0003    CELL-LTE-0.001  1x Cell LTE NAM V/S

                    DB-CELL-LTE-1.
                    003
RX1400  CELL0004    CELL-LTE-0.001  1x Cell LTE APAC

                    DB-CELL-LTE-1.
                    004
RX1400  CELL0005    CELL-LTE-0.001  1x Cell LTE Japan

                    DB-CELL-LTE-1.
                    005
RX1400  CM0001      BACKPLANE.001   CM TI-AM5726 variant 0001
RX1400  CM0001      CM-AM5726-0.00  CM TI-AM5726 variant 0001
                    1
RX1400  PM0001      PM-24VDC.001    12-24VDC Unmonitored PM
RX1400  PM0002      PM-48VDC.001    48VDC Unmonitored PM
RX1400  PM0003      PM-HI.001       HI AC-DC Unmonitored PM
RX1400  SER0001     SER-TP-0.001    2xRS232/422/485
                    DB-SER-TP-2.00
                    1
RX1400  SM0001      SM-L2-0.001     SM M88E6097F, 4FT 2GP
                    DB-ETH-FT-4.00
                    1
                    DB-ETH-GP-2.00
                    1
.
.
.
```

Abschnitt 4.5

Das Gerät herunterfahren

Um das Gerät herunterzufahren, geben Sie Folgendes ein:

ACHTUNG!
Sicherheitsgefahr – Risiko eines unberechtigten Zugriffs und/oder einer unberechtigten Nutzung
Fahren Sie das Gerät immer herunter, bevor Sie es von der Spannungsversorgung trennen. Andernfalls kann es zu einer Datenbeschädigung kommen.

HINWEIS
Das Gerät ist nie dauerhaft abgeschaltet. Wenn die Geräte zum Herunterfahren aufgefordert werden, schalten sie sich mit einer Timeout-Dauer aus, während der die Stromversorgung vom Gerät getrennt werden kann. Die voreingestellte Dauer des Timeouts beträgt 300 Sekunden (fünf Minuten). Nach Ablauf der Timeout-Dauer fährt das Gerät wieder hoch und startet neu.

HINWEIS
Wenn aufgrund der Verdrahtung die Stromversorgung nicht unterbrochen werden kann, kann/können stattdessen das/die Leistungsmodul(e) entfernt werden.

```
admin shutdown
```

Abschnitt 4.6
Gerät neu booten

Um das Gerät neu zu booten, geben Sie Folgendes ein:

```
admin reboot
```

Abschnitt 4.7
Auf Werkseinstellungen zurücksetzen

Um das Gerät auf die Werkseinstellungen zurückzusetzen, geben Sie den folgenden Befehl ein:

```
admin restore-factory-defaults
```

Fügen Sie bei Bedarf die folgenden Optionen ein:

Parameter	Beschreibung
delete-logs	**Zusammenfassung:** { true, false } **Standard:** false Löschen Sie die Systemprotokolle und stellen Sie die Grundeinstellungen wieder her.
default-both-partitions	**Zusammenfassung:** { true, false } **Standard:** false Führen Sie den Vorgang an beiden Partitionen durch.
delete-saved-configurations	**Zusammenfassung:** { true, false } **Standard:** false Löschen Sie die gespeicherten Konfigurationsdateien (möglich mit Option "default-both-partitions").
shutdown	**Zusammenfassung:** { true, false } **Standard:** false Nach dem Wiederherstellen der Werkseinstellungen schalten sie ab, anstatt neuzustarten.

Abschnitt 4.8
Außerbetriebnahme des Geräts

Bevor Sie das Gerät außer Betrieb setzen, entweder dauerhaft oder für Wartungsarbeiten durch Dritte, stellen Sie sicher, dass es vollständig außer Betrieb genommen wurde. Dazu gehört auch das Entfernen vertraulicher, geschützter Informationen.

Um das Gerät außer Betrieb zu nehmen, gehen Sie wie folgt vor:

1. Machen Sie eine Kopie der derzeitig auf dem Gerät installierten RUGGEDCOM ROX II-Firmware. Weiterführende Informationen erhalten Sie beim Siemens-Kundensupport
2. Melden Sie sich im Wartungsmodus an. Weitere Informationen finden Sie im Abschnitt 2.7.3, „Auf den Wartungsmodus zugreifen“ .
3. Löschen Sie das aktuelle Passwort/die Passphrase zum Systemstart, indem Sie Folgendes eingeben:

   ```
   rox-delete-bootpwd --force
   ```
4. Geben Sie **`exit`** ein und drücken Sie **Enter**.
5. Loggen Sie sich bei RUGGEDCOM ROX II ein. Weitere Informationen finden Sie unter Abschnitt 2.2, „Anmelden“.
6. Flashen Sie die RUGGEDCOM ROX II-Firmware, die Sie in Schritt 1 erhalten haben, in die inaktive Partition und starten Sie das Gerät neu. Weitere Informationen finden Sie unter Abschnitt 4.15.5.2, „Downgrade mittels ROXflash“.
7. Wiederholen Sie Schritt 5 und Schritt 6. um die RUGGEDCOM ROX II-Firmware, die Sie in Schritt 1 erhalten haben, in die andere Partition zu flashen, und starten Sie das Gerät neu.
8. Fahren Sie das Gerät herunter. Weitere Informationen finden Sie unter Abschnitt 4.5, „Das Gerät herunterfahren“.

Abschnitt 4.9

Anzeigen einer Liste der Line-Modul-Konfigurationen

Um eine Liste der Line-Modul-Konfigurationen anzuzeigen, geben Sie Folgendes ein:

HINWEIS
Line-Modul-Konfigurationen sind nicht konfigurierbar.

```
show running-config chassis line-modules
```

Falls Line-Module konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
show running-config chassis line-modules | tab
chassis
 line-modules
  line-module
                                  ADMIN    ADMIN
SLOT      MODULE TYPE             ENABLED  BYPASS
-------------------------------------------------
swport    SM M88E6097F, 4FT 2GP   X        -
serport   2xRS232/422/485         X        -
celport   1x Cell LTE NAM A/R/B/T X        -
wlanport  1x WLAN 802.11 US       X        -

 !
!
```

Abschnitt 4.10

Anzeigen von SFP-Informationen

Um Informationen über einen bestimmten Transceiver vom Typ Small Form-Factor Pluggable (SFP) in einem Line-Modul anzuzeigen, geben Sie Folgendes ein:

HINWEIS
Einige SFPs stellen möglicherweise keine Informationen über sich zur Verfügung. In diesen Fällen wird eine Meldung ähnlich der Folgenden angezeigt:

```
ID: Unknown FF
```

```
interfaces switch slot port sfp
```

Erläuterung:

- *slot* ist die Bezeichnung des Modul-Einbauorts
- *port* ist die Nummer des Ports (oder eine Liste von Ports, wenn sie in einem Port-Trunk gebündelt sind) für das Modul.

Wenn ein SFP-Transceiver im ausgewählten Port vorhanden ist, werden Einzelheiten zum Transceiver angezeigt. Beispiel:

```
ruggedcom# interfaces switch lm1 1 sfp
sfp-info-string
ID: SFP or SFP "Plus"
Extended ID: GBIC/SFP function is defined by serial ID only
Connector: LC
Transceiver:
      Ethernet Compliance: 100Base-FX
      10G Ethernet Compliance: Not specified
      Fibre Channel link length: Not specified
      Fibre Channel transmitter technology: Not specified
      SFP+ cable technology: Not specified
      Fibre Channel transmission media: Not specified
      Fibre Channel speed: Not specified
Baud Rate, nominal: 100 Mbps
Encoding type: 4B5B
Length(SMF): Not specified
Length(SMF): Not specified
Length(50um): 2000 m
Length(62.5um): 2000 m
Length(Copper): Not specified
Length(OM3): Not specified
Vendor: AVAGO
IEEE company ID: 8193
Part number:
Revision: O
Laser wavelength: 8224 nm
Options: Power Level (see SFF-8431) - level 2
         Linear Receiver Output implemented (see SFF-8431)
         Loss of Signal implemented, inverted (often called Signal Detect)
BRmax: 700 Mbps
BRmin: Not specified
Serial number:
Manufacturing date code: Y:AV M:AG D:O
Monitoring type: Digital diag monitoring - MUST be '1' but is '0'
                 Internally calibrated
                 Received power measurement type - OMA
Enhanced options: Soft TX_FAULT monitoring
SFF-8472 revision compliance: Unknown 20
```

Abschnitt 4.11

Verwalten von Feature Keys

Der RUGGEDCOM ROX II kann jederzeit durch Hinzufügen von Feature Levels um weitere Funktionen erweitert werden. Feature Levels sind in Feature Keys verschlüsselt, die auf ein Gerät geladen werden können. Bei der Bestellung wird ein Geräte-Feature-Key in der elektronischen Unterschrift des Geräts verschlüsselt. Weitere dateibasierte Feature Keys können je nach Bedarf hinzugefügt werden.

HINWEIS
Bestimmte RUGGEDCOM ROX II-Funktionen stehen nur durch Erwerb von Feature Levels zur Verfügung. Weitere Informationen über erhältliche Feature Levels finden Sie im Produktdatenblatt des Geräts unter https://www.siemens.com/ruggedcom, oder Sie wenden sich an einen Siemens-Vertriebsmitarbeiter.

Geben Sie bei der Bestellung von Feature Levels die *Haupt*-Seriennummer des Geräts an. Es wird eine aktualisierte Feature-Key-Datei bereitgestellt, die für das Gerät lizenziert wird. Informationen über die Bestimmung der *Haupt*-Seriennummer finden Sie in Abschnitt 4.1, „Geräte- und Softwareinformationen anzeigen“.

INHALT

- Abschnitt 4.11.1, „Inhalt eines Feature Key anzeigen“
- Abschnitt 4.11.2, „Installieren von Feature Keys“

Abschnitt 4.11.1

Inhalt eines Feature Key anzeigen

Um den Inhalt eines im Gerät gespeicherten Feature Key anzusehen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Betriebsmodus befindet.
2. Wenn die Eingabeaufforderung erscheint, geben Sie Folgendes ein:

   ```
   file show-featurekey filename
   ```

   Erläuterung:

   - *filename* ist der Name der im Gerät gespeicherten Feature-Key-Datei

   Beispiel:

   ```
   ruggedcom# file show-featurekey 1_cmRX1K-12-11-0015.key
   ```

3. Drücken Sie auf **Enter**. Das System zeigt den Inhalt der Feature-Key-Datei an. Beispiel:

   ```
   ruggedcom# file show-featurekey L3SE_cmRUMHD06096338.key
   GPG_FEATUREKEY_LEVEL=L3SE
   GPG_FEATUREKEY_CM_SERIALNUMBER=RUMHD06096338
   GPG_FEATUREKEY_SIGNATURE=iEYEABECAAYFAliGF4EACgkQP2pya+G5kdYj1ACfecKysp3DK3QBsP87I/
   gXgi92cwAAnjqrsgdqwaCczY4ghWrR0ELkr2TK
   ```

Abschnitt 4.11.2

Installieren von Feature Keys

Bei der Installation eines neuen Feature Keys evaluiert der RUGGEDCOM ROX II den neuen dateibasierten Feature Key und den Geräte-Feature-Key und aktiviert das durch die Feature Keys beschriebene geeignetste Feature Level.

Feature Keys können von einem Host-Computer oder einem microSD/microSDHC-Speicher installiert werden.

» Installation von einem Host-Computer

HINWEIS
Vor der Installation eines Feature Keys von einem Host-Computer werden folgende Informationen benötigt:

- *Der Dateiname des Feature Keys*
- *Der Benutzername und das Passwort, die zum Anmelden auf dem Host-Computer erforderlich sind, auf dem der Feature Key gespeichert ist*
- *Der Hostname oder die IP-Adresse des Computers, auf dem der Feature Key gespeichert ist*

1. Stellen Sie sicher, dass sich die CLI im Betriebsmodus befindet.
2. Installieren Sie den Feature Key, indem Sie Folgendes eingeben:

   ```
   file scp-featurekey-from-url username@host:/path/current-filename new-filename
   ```

   Erläuterung:

   - *username* ist die Bezeichnung eines Benutzers, der sich auf dem Computer anmelden kann, auf dem der Feature Key gespeichert ist.
   - *host* ist der Hostname oder die IP-Adresse des Computers, auf dem der Feature Key gespeichert ist.
   - *path* ist der Verzeichnispfad zur Feature-Key-Datei auf dem Host-Computer.
   - *current-filename* ist die aktuelle Bezeichnung der Feature-Key-Datei.
   - *new-filename* ist die neue Bezeichnung der Feature-Key-Datei auf dem Gerät. Dieser Parameter ist optional. Der aktuelle Dateiname wird verwendet, falls kein neuer Dateiname verfügbar ist.

   Beispiel:

   ```
   file scp-featurekey-from-url wsmith@10.200.10.39:/files/keys/L3SE_cmRUMHD06096338.key
    L3SE_cmRUMHD06096338.key
   ```

3. Bei Aufforderung geben Sie das Benutzerpasswort ein und drücken anschließend auf **Enter**. Das System führt einen Upload der Feature-Key-Datei aus:

   ```
    ruggedcom# file scp-featurekey-from-url wsmith@10.200.20.39:/files/keys/
   L3SE_cmRUMHD06096338.key L3SE_cmRUMHD06096338.key
   wsmith@10.200.20.39's password:
   L3SE_cmRUMHD06096338.key               100%  192     0.2KB/s   00:00
   ```

» Installation von einer MicroSD-Karte

1. Stellen Sie sicher, dass sich die CLI im Betriebsmodus befindet.
2. Stecken Sie den microSD/microSDHC-Speicher in den microSD/microSDHC-Steckplatz des Geräts. Ausführliche Informationen hierzu finden Sie im *RUGGEDCOM RX1400 Installationsleitfaden*.

3. Installieren Sie den Feature Key, indem Sie Folgendes eingeben:

```
file scp-featurekey-from-url usb:///path/current-filename new-filename
```

Erläuterung:

- *path* ist der Verzeichnispfad zur Feature-Key-Datei auf dem USB-Massenspeicher.
- *current-filename* ist die aktuelle Bezeichnung der Feature-Key-Datei.
- *new-filename* ist die neue Bezeichnung der Feature-Key-Datei auf dem Gerät. Dieser Parameter ist optional. Der aktuelle Dateiname wird verwendet, falls kein neuer Dateiname verfügbar ist.

Beispiel:

```
file scp-featurekey-from-url usb://repository/keys/L3SE_cmRUMHD06096338.key
 L3SE_cmRUMHD06096338.key
```

Das System führt einen Upload der Feature-Key-Datei aus:

```
 ruggedcom# file scp-featurekey-from-url usb://repository/keys/
L3SE_cmRUMHD06096338.key L3SE_cmRUMHD06096338.key
L3SE_cmRUMHD06096338.key                100%  192     0.2KB/s   00:00
```

Abschnitt 4.12

Dateien verwalten

RUGGEDCOM ROX II ermöglicht die Übertragung ausgewählter Dateien zu und vom Gerät mit den folgenden Verfahren:

- **Install**
  Damit können Benutzer mit einem Dateiübertragungsprotokoll wie FTP Dateien von einem einer MicroSD/SDHC-Karte oder von einem entfernten Server in das Gerät laden.
- **Backup**
  Damit können Benutzer mit einem Dateiübertragungsprotokoll wie FTP Dateien in ein eine MicroSD/SDHC-Karte oder in einen entfernten Server hochladen.

INHALT

- Abschnitt 4.12.1, „Installieren von Dateien“
- Abschnitt 4.12.2, „Sichern von Dateien“

Abschnitt 4.12.1

Installieren von Dateien

Um eine Datei (z. B. Konfigurationsdatei, Feature Key oder Image einer virtuellen Maschine) auf dem Gerät zu installieren, gehen Sie wie folgt vor:

WICHTIG!
Wenn es sich bei dem Dateityp um das Image einer virtuellen Maschine handelt, dann muss ein microSD/microSDHC-Speicher installiert sein. Images virtueller Maschinen werden nach der Installation auf dem microSD/microSDHC-Speicher gespeichert.

1. Falls die Quelle der Datei ein microSD/microSDHC-Speicher ist, stecken Sie den Speicher in den microSD/microSDHC-Port des Geräts. Ausführliche Informationen hierzu finden Sie im *RUGGEDCOM RX1400 Installationsleitfaden*.
2. Navigieren Sie zu ***admin » install-files*** und konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

HINWEIS
Der RUGGEDCOM ROX II unterstützt Implicit FTP over TLS (FTPS) URLs. Explicit FTP over TLS wird nicht unterstützt.

Parameter	Beschreibung
file-type { file-type }	**Zusammenfassung:** { config, featurekey, vmfile } Die Dateitypen, die kopiert werden sollen. Dieser Parameter ist obligatorisch.
url { url }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 1024 Zeichen Die URL der zu kopierenden ROX II-Datei. Die URL HTTP, SCP, SFTP, FTPS und FTP werden unterstützt. Zum Installieren von einem USB-Flash-Laufwerk oder einer microSD-Karte (sofern zutreffend) ist das URL-Format "usb://{usb-device-name}/path-to-file-on-system" oder "sd://sd-1//path-to-file-on-system". Führen Sie "show chassis" aus, um den Namen des USB-Geräts zu bestimmen. Beachten Sie, dass für jeden Datenträger nur eine Partition unterstützt wird. Bei allen anderen Protokollen ist das Format: "protocol://user:password@host:port/path-to-file". Ist "port" nicht festgelegt, wird der für das Protokoll voreingestellte Port verwendet. Dieser Parameter ist obligatorisch.

Abschnitt 4.12.2
Sichern von Dateien

Um auf dem Gerät gespeicherte Dateien zu sichern, gehen Sie wie folgt vor:

1. Falls sich der Zielpfad der Datei auf einem microSD/microSDHC-Speicher befindet, stecken Sie den Speicher in den microSD/microSDHC-Port des Geräts. Ausführliche Informationen hierzu finden Sie im *RUGGEDCOM RX1400 Installationsleitfaden*.
2. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
3. Navigieren Sie zu ***admin » backup-files*** und konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

HINWEIS
Der RUGGEDCOM ROX II unterstützt Implicit FTP over TLS (FTPS) URLs. Explicit FTP over TLS wird nicht unterstützt.

Parameter	Beschreibung
file-type { file-type }	**Zusammenfassung:** { config, featurekey, logfiles, rollbacks, licenses, logarchive } Die Dateitypen, die kopiert werden sollen. Dieser Parameter ist obligatorisch.
file { file }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 255 Zeichen Der Name des Protokollarchivs (logarchive) oder eine Liste von Dateinamen, die zu kopieren sind. Bei logarchive ist nur ein Dateiname zulässig, um das "tar-

Parameter	Beschreibung
	archive" (Zielarchiv) zu benennen, das als Sicherung des Gesamten Verzeichnisses "/var/log" dient. Das Archiv wird im Verzeichnis "/tmp" erstellt und automatisch gelöscht, Dieser Parameter ist obligatorisch.
timestamp	**Zusammenfassung:** { true, false } **Standard:** false Sofern aktiviert, wird ein Zeitstempel an den Dateinamen angehängt. Diese Option ist nicht für Dateinamen verfügbar, die ein '*' enthalten.
url { url }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 1024 Zeichen Die URL der zu kopierenden ROX II-Datei. Die URL HTTP, SCP, SFTP, FTPS und FTP werden unterstützt. Zum Speichern auf ein USB-Flash-Laufwerk oder eine microSD-Karte (sofern zutreffend) ist das URL-Format "usb://{usb-device-name}/path-to-file" oder "sd://sd-1//path-to-file". Führen Sie "show chassis" aus, um den Namen des USB-Geräts zu bestimmen. Beachten Sie, dass für jeden Datenträger nur eine Partition unterstützt wird. Bei allen anderen Protokollen ist das Format: "protocol://user:password@host:port/path-to-file". Wenn Sie nur einen Pfad verwenden, beenden Sie ihn mit '/'. Ist "port" nicht festgelegt, wird der für das Protokoll voreingestellte Port verwendet. Dieser Parameter ist obligatorisch.

Abschnitt 4.13

Verwalten von Protokollen

Der RUGGEDCOM ROX II unterstützt verschiedene Protokolle zur Aufzeichnung von Informationen über wichtige Ereignisse. Jedes Protokoll gehört einem der folgenden Protokolltypen an:

Sicherheitsereignis-Protokolle

Informationen im Zusammenhang mit den folgenden Sicherheitsereignissen werden vom RUGGEDCOM ROX II protokolliert:

HINWEIS
Die Eingabe von Passwörtern kann bis zu dreimal erfolgen, bevor der Anmeldeversuch als Sicherheitsereignis eingestuft wird.

- Erfolgreiche und nicht erfolgreiche Anmeldeversuche
- Lokale und dezentrale (RADIUS-)Authentifizierung
- Sicherheitsrelevante Befehle (erfolgreich und nicht erfolgreich)
- Ein optional konfigurierbares SNMP Authentication Failure Trap (standardmäßig deaktiviert) gemäß SNMPv2-MIB

Alle Sicherheitsereignis-Protokolle werden erfasst unter `var/log/auth.log` und können im Authlog Viewer angezeigt werden. Weitere Informationen über das Anzeigen von Protokollen finden Sie in Abschnitt 4.13.1, „Anzeigen von Protokollen“.

Syslogs

Syslog gestattet Benutzern, lokale und dezentrale Syslog-Verbindungen zum Aufzeichnen wichtiger, nicht-sicherheitsrelevanter Ereignisinformationen zu konfigurieren. Das Protokoll Remote Syslog ist nach RFC 3164 [http://tools.ietf.org/html/rfc3164] ein UDP/IP-basiertes Transportprotokoll, mit dem ein Gerät Ereignisbenachrichtigungen über IP-Netzwerke an Event Message Collector (d.h. Syslog-Server) sendet. Mithilfe des Protokolls sollen diese Ereignisnachrichten vom generierenden Gerät auf einfache Weise an den Collector transportiert werden.

Alle Protokolldateien werden im Protokollverzeichnis (`/var/log`) gemäß der Facility und Priorität organisiert, entsprechend der sie protokolliert wurden. Remote Syslog sendet die angeforderten Protokolle an den/die dezentralen Server mit der Facility und Priorität, entsprechend der sie ursprünglich protokolliert wurden, im Anschluss an eine Filterung der Protokolle basierend auf den für den Server konfigurierten Selektoren.

Die folgenden Protokolldateien werden mit den folgenden Standardselektoren eingerichtet:

- `syslog` erfasst alle Protokolle mit Ausnahme der Protokolle "daemon.debug", "auth" oder "authpriv"

	• `daemon.log` erfasst alle Protokolle auf *err*-Ebene (und höher), die in die Daemon-Facility geschrieben wurden • `messages` erfasst alle Protokolle auf *info*-, *notice*- und *warn*-Ebene mit Ausnahme von "auth", "authpriv", "cron", "daemon", "mail" und "news" Ein Selektor-Setup, das die folgenden Facilities auf der *info*-Ebene (und höher) verwendet, wird empfohlen: • daemon • user • kern • syslog
Diagnoseprotokolle	Diagnoseprotokolle zeichnen Systeminformationen zur Fehlerbehebung auf.

INHALT

- Abschnitt 4.13.1, „Anzeigen von Protokollen“
- Abschnitt 4.13.2, „Protokolle löschen“
- Abschnitt 4.13.3, „Das sichere Remote Syslog konfigurieren“
- Abschnitt 4.13.4, „Diagnoseprotokolle verwalten“
- Abschnitt 4.13.5, „Entfernte Syslog-Server verwalten“
- Abschnitt 4.13.6, „Selektoren für entfernte Server verwalten“

Abschnitt 4.13.1

Anzeigen von Protokollen

Ausgewählte Protokolle können direkt in der CLI angezeigt werden. Andernfalls können diese und andere Protokolle vom Gerät geladen und in einem Texteditor/-Viewer angezeigt werden.

HINWEIS
Weitere Informationen über das Herunterladen von Protokolldateien vom Gerät finden Sie in Abschnitt 4.12.2, „Sichern von Dateien“.

Um ein Protokoll in der CLI anzuzeigen, gehen Sie wie folgt vor:

```
show log file
```

Erläuterung:

- `file` ist die anzuzeigende Protokolldatei

Um beispielsweise das Protokoll auth.log anzuzeigen, geben Sie Folgendes ein:

```
show log auth.log
```

Ein Ergebnis ähnlich dem Folgenden wird angezeigt:

```
ruggedcom# show log auth.log
Jan 29 09:25:00 ruggedcom confd[2068]: audit user: admin/0 failed to login using externalauth:  Local
 authentication
Jan 29 09:25:00 ruggedcom confd[2068]: audit user: admin/0 logged in through Web UI from 192.168.0.200
Jan 29 09:25:00 ruggedcom confd[2068]: audit user: admin/32 assigned to groups: admin
Jan 29 09:25:01 ruggedcom CRON[4599]: pam_unix(cron:session): session opened for user root by (uid=0)
.
.
.
```

Abschnitt 4.13.2
Protokolle löschen

Um alle im Gerät gespeicherten Protokolle zu löschen, geben Sie Folgendes ein:

```
admin delete-logs
```

Abschnitt 4.13.3
Das sichere Remote Syslog konfigurieren

Das sichere Remote Syslog verschlüsselt alle an Syslog-Server gesendeten Systemprotokolle mit einem von einer Zertifizierungsstelle signierten SSL-(Secure Sockets Layer)-Zertifikat.

WICHTIG!
Die Zertifikate für Client (RUGGEDCOM ROX II) und Server müssen von der gleichen Zertifizierungsstelle signiert sein.

INHALT

- Abschnitt 4.13.3.1, „Aktivieren/Deaktivieren des sicheren Remote Syslog“
- Abschnitt 4.13.3.2, „Eine Liste der zulässigen Peers anzeigen“
- Abschnitt 4.13.3.3, „Einen erlaubten Peer hinzufügen“
- Abschnitt 4.13.3.4, „Einen erlaubten Peer löschen“
- Abschnitt 4.13.3.5, „Konfigurieren einer IP-Quelladresse für dezentrale Syslog-Meldungen“

Abschnitt 4.13.3.1
Aktivieren/Deaktivieren des sicheren Remote Syslog

Um eine bestimmte IP-Quelladresse für alle dezentralen Syslog-Meldungen zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.

   HINWEIS
   Sobald die sichere Remote-Systemprotokollierung aktiviert und ein Remote-Syslog-Server konfiguriert ist, wird der TCP-Port 6514 automatisch geöffnet.

2. Aktivieren oder deaktivieren Sie das sichere Remote Syslog, indem Sie Folgendes eingeben:

   Aktivieren

   ```
   admin logging secure-remote-syslog enable
   ```

   Deaktivieren

   ```
   no admin logging secure-remote-syslog enable
   ```

   WICHTIG!
   Alle Zertifikate müssen folgende Anforderungen erfüllen:
   - *Digitales Zertifikatformat X.509 v3*

- *PEM-Format*
- *RSA-Schlüsselpaar, Bitlänge 512 bis 2048*

3. Wenn das sichere Remote Syslog aktiviert ist, geben Sie ein Zertifikat zur Authentifizierung mit dem Remote-Syslog-Server an, indem Sie Folgendes eingeben:

```
certificate certificate
```

Erläuterung:

- *certificate* ist die Bezeichnung des Zertifikats.

Falls das gewünschte Zertifikat nicht aufgeführt ist, fügen Sie es hinzu. Weitere Informationen finden Sie unter Abschnitt 6.6.7.3, „Hinzufügen eines Zertifikats“.

4. [Optional] Legen Sie einen oder mehrere Abstimmungsmuster oder *erlaubte Peers* fest. Erlaubte Peers vergleichen den Hostnamen des Servers mit dem gemeinsamen im SSL-Zertifikat definierten Namen. Weitere Informationen finden Sie unter Abschnitt 4.13.3.3, „Einen erlaubten Peer hinzufügen“.
5. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 4.13.3.2
Eine Liste der zulässigen Peers anzeigen

Um eine Liste der zulässigen Peers anzusehen, geben Sie Folgendes ein:

```
show running-config admin logging secure-remote-syslog permitted-peer
```

Falls Peers konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config admin logging secure-remote-syslog permitted-peer

admin
 logging
  secure-remote-syslog permitted-peer *.example.com
  !
 !
!
```

Falls keine Peers konfiguriert wurden, fügen Sie je nach Bedarf Peers hinzu. Weitere Informationen finden Sie unter Abschnitt 4.13.3.3, „Einen erlaubten Peer hinzufügen“.

Abschnitt 4.13.3.3
Einen erlaubten Peer hinzufügen

Um einen erlaubten Peer für ein Remote Syslog hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den erlaubten Peer hinzu, indem Sie Folgendes eingeben:

```
admin logging secure-remote-syslog permitted-peer pattern
```

Erläuterung:

- *pattern* ist das verwendete Muster, um den im SSL-Zertifikat definierten und vom Server erhaltenen gemeinsamen Namen miteinander abzustimmen

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 4.13.3.4
Einen erlaubten Peer löschen

Um einen erlaubten Peer für das sichere Remote Syslog zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die Firewall, indem Sie Folgendes eingeben:

   ```
   no admin logging secure-remote-syslog permitted-peer pattern
   ```

   Erläuterung:

   - *`pattern`* ist das verwendete Muster, um den Hostnamen des Servers mit dem gemeinsamen im SSL-Zertifikat definierten Namen abzustimmen
3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 4.13.3.5
Konfigurieren einer IP-Quelladresse für dezentrale Syslog-Meldungen

IP-Pakete für dezentrale Syslog-Meldungen beinhalten eine IP-Zieladresse und eine IP-Quelladresse. Die IP-Quelladresse ist die Schnittstelle, von der aus die Meldung gesendet wird (z. B. switch.0001). Jedoch ist diese Adresse im Systemprotokoll möglicherweise nicht aussagekräftig bzw. die Adresse kann im Gegensatz zu einer Firewall-Regel oder -Grundregel stehen. In solchen Fällen kann eine alternative IP-Quelladresse für alle dezentralen Syslog-Meldungen konfiguriert werden.

Um eine bestimmte IP-Quelladresse für alle dezentralen Syslog-Meldungen zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Stellen Sie sicher, dass zuerst eine IP-Adresse für die gewünschte Schnittstelle definiert wird. Für weitere Informationen siehe Abschnitt 7.1.3.2, „Eine IPv4-Adresse hinzufügen“ oder Abschnitt 7.1.4.2, „Eine IPv6-Adresse hinzufügen“.
3. Konfigurieren Sie die IP-Quelladresse, indem Sie Folgendes eingeben:

   ```
   admin logging source-ip address
   ```

   Erläuterung:

   - *`address`* ist die alternative IP-Quelladresse
4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 4.13.4
Diagnoseprotokolle verwalten

Für die Fehlerbehebung im Gerät stehen Diagnoseprotokolle zur Verfügung. In den folgenden Protokollen sind verschiedene Verhaltensarten des Geräts aufgezeichnet:

Protokoll	Dateiname
Entwicklerprotokoll	`/var/log/confd-dev.log`
SNMP-Protokoll	`/var/log/snmp-trace.log`
NETCONF-Übersichtsprotokoll	`/var/log/netconf.log`
NETCONF-Trace-Protokoll	`/var/log/netconf-trace.log`
XPATH-Trace-Protokoll	`/var/log/xpath-trace.log`
WebUI-Trace-Protokoll	`/var/log/webui-trace.log`

ACHTUNG!
Konfigurationsrisiko - Gefahr der Leistungsminderung. Das Aktivieren der Diagnoseprotokollierung hat deutliche Auswirkungen auf die Leistung von RUGGEDCOM ROX II. Aktivieren Sie die Diagnoseprotokollierung nur auf Anweisung von Siemens.

INHALT

- Abschnitt 4.13.4.1, „Das Entwicklerprotokoll aktivieren/deaktivieren“
- Abschnitt 4.13.4.2, „Das SNMP-Protokoll aktivieren/deaktivieren“
- Abschnitt 4.13.4.3, „Aktivieren/Deaktivieren des NETCONF-Summary-Protokolls“
- Abschnitt 4.13.4.4, „Aktivieren/Deaktivieren des NETCONF-Trace-Protokolls“
- Abschnitt 4.13.4.5, „Das XPATH-Trace-Protokoll aktivieren/deaktivieren“
- Abschnitt 4.13.4.6, „Das WebUI-Trace-Protokoll aktivieren/deaktivieren“

Abschnitt 4.13.4.1

Das Entwicklerprotokoll aktivieren/deaktivieren

Das Entwicklerprotokoll zeichnet interne Systemtransaktionen aus der operativen Sicht auf.

ACHTUNG!
Gefährdung durch Konfiguration - Gefahr der Leistungsminderung. Das Aktivieren der Diagnoseprotokollierung hat deutliche Auswirkungen auf die Leistung von RUGGEDCOM ROX II. Aktivieren Sie die Diagnoseprotokollierung nur auf Anweisung von Siemens.

Um das Entwicklerprotokoll zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Aktivieren oder deaktivieren Sie das Entwicklerprotokoll, indem Sie Folgendes eingeben:

   Aktivieren

   ```
   admin logging diagnostics developer-log enabled
   ```

   Deaktivieren

   ```
   no admin logging diagnostics developer-log enabled
   ```

3. Konfigurieren Sie den Stand der Informationen, den das Entwicklerprotokoll liefert, indem Sie Folgendes eingeben:

Parameter	Beschreibung
log-level { log-level }	**Zusammenfassung:** { error, info, trace } **Standard:** info Stellt das Maß an Ausführlichkeit auf Entwickler-Logging ein.

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 4.13.4.2
Das SNMP-Protokoll aktivieren/deaktivieren

Das SNMP-Protokoll zeichnet alle SNMP-bezogenen Ereignisse auf.

ACHTUNG!
Gefährdung durch Konfiguration - Gefahr der Leistungsminderung. Das Aktivieren der Diagnoseprotokollierung hat deutliche Auswirkungen auf die Leistung von RUGGEDCOM ROX II. Aktivieren Sie die Diagnoseprotokollierung nur auf Anweisung von Siemens.

Um das SNMP-Protokoll zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Aktivieren oder deaktivieren Sie das SNMP-Protokoll, indem Sie Folgendes eingeben:

   Aktivieren

   ```
   admin logging diagnostics snmp-log enabled
   ```

   Deaktivieren

   ```
   no admin logging diagnostics snmp-log enabled
   ```

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 4.13.4.3
Aktivieren/Deaktivieren des NETCONF-Summary-Protokolls

Das NETCONF-Summary-Protokoll zeichnet zusammenfassend NETCONF-Protokolltransaktionen und insbesondere erfolgreich abgeschlossene Transaktionen auf. Beispiel:

```
.
.
.
<INFO> 5-Apr-2012::04:26:33.877 ruggedcom confd[2098]: netconf id=9450 new ssh session for user "admin"
 from 192.168.0.10
<INFO> 5-Apr-2012::04:27:03.574 ruggedcom confd[2098]: netconf id=9450 got rpc:
 {urn:ietf:params:xml:ns:netconf:base:1.0}validate attrs: message-id="103"
<INFO> 5-Apr-2012::04:27:04.167 ruggedcom confd[2098]: netconf id=9450 validate source=candidate attrs:
 message-id="103"
<INFO> 5-Apr-2012::04:27:06.691 ruggedcom confd[2098]: netconf id=9450 sending rpc-reply, attrs:
 message-id="103"
.
.
.
```

ACHTUNG!
Konfigurationsrisiko – Gefahr von verminderter Leistung. Das Aktivieren der diagnostischen Protokollierung hat deutliche Auswirkungen auf die Leistung von RUGGEDCOM ROX II. Aktivieren Sie die Diagnoseprotokollierung nur auf Anweisung von Siemens.

Um das NETCONF-Summary-Protokoll zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Aktivieren oder deaktivieren Sie das NETCONF-Summary-Protokoll, indem Sie Folgendes eingeben:

   Aktivieren

   ```
   admin logging diagnostics netconf-summary-log enabled
   ```

   Deaktivieren

   ```
   no admin logging diagnostics netconf-summary-log enabled
   ```

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 4.13.4.4

Aktivieren/Deaktivieren des NETCONF-Trace-Protokolls

Das NETCONF-Trace-Protokoll zeichnet den Text jeder vom Gerät empfangenen und gesendeten NETCONF-XML-Nachricht auf. Jeder Eintrag beinhaltet die Kennung der NETCONF-Sitzung und den vollständigen Text der XML-Nachricht. Steht hinter der Sitzungskennung das Wort *read*, dann wurde die XML-Nachricht vom Gerät empfangen. Das Wort *write* gibt an, dass die XML-Nachricht vom Gerät gesendet wurde. Beispiel:

```
.
.
.
**> sess:9450 read:
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="103">
  <validate>
    <source>
      <running/>
    </source>
  </validate>
</rpc>

**< sess:9450 write:
<rpc-reply message-id="103" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <ok/>
</rpc-reply>
.
.
.
```

ACHTUNG!
Konfigurationsrisiko – Gefahr von verminderter Leistung. Das Aktivieren der diagnostischen Protokollierung hat deutliche Auswirkungen auf die Leistung von RUGGEDCOM ROX II. Aktivieren Sie die Diagnoseprotokollierung nur auf Anweisung von Siemens.

Um das NETCONF-Trace-Protokoll zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Aktivieren oder deaktivieren Sie das NETCONF-Trace-Protokoll, indem Sie Folgendes eingeben:

Aktivieren

```
admin logging diagnostics netconf-trace-log enabled
```

Deaktivieren

```
no admin logging diagnostics netconf-trace-log enabled
```

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 4.13.4.5

Das XPATH-Trace-Protokoll aktivieren/deaktivieren

Das XPATH-Trace-Protokoll zeichnet interne Ereignisse im Zusammenhang mit XPATH-Routinen auf, die eine Interaktion mit einer XPATH-Komponente erfordern.

ACHTUNG!
Gefährdung durch Konfiguration - Gefahr der Leistungsminderung. Das Aktivieren der Diagnoseprotokollierung hat deutliche Auswirkungen auf die Leistung von RUGGEDCOM ROX II. Aktivieren Sie die Diagnoseprotokollierung nur auf Anweisung von Siemens.

Um das XPATH-Trace-Protokoll zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Aktivieren oder deaktivieren Sie das XPATH-Trace-Protokoll, indem Sie die folgenden Befehle eingeben:

   Aktivieren

   ```
   admin logging diagnostics xpath-trace-log enabled
   ```

   Deaktivieren

   ```
   no admin logging diagnostics xpath-trace-log enabled
   ```

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 4.13.4.6

Das WebUI-Trace-Protokoll aktivieren/deaktivieren

Das WebUI-Trace-Protokoll zeichnet alle Transaktionen auf, die mit der Webschnittstelle zusammenhängen, wie z. B. Konfigurationsänderungen, Fehlermeldungen usw.

ACHTUNG!
Gefährdung durch Konfiguration - Gefahr der Leistungsminderung. Das Aktivieren der Diagnoseprotokollierung hat deutliche Auswirkungen auf die Leistung von RUGGEDCOM ROX II. Aktivieren Sie die Diagnoseprotokollierung nur auf Anweisung von Siemens.

Um das WebUI-Trace-Protokolll zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Aktivieren oder deaktivieren Sie das WebUI-Trace-Protokoll, indem Sie die folgenden Befehle eingeben:

Aktivieren

```
admin logging diagnostics webui-trace-log enabled
```

Deaktivieren

```
no admin logging diagnostics webui-trace-log enabled
```

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 4.13.5

Entfernte Syslog-Server verwalten

RUGGEDCOM ROX II kann bis zu 6 Ereignismeldungssammler oder entfernte Syslog-Server unterstützen. Das entfernte Syslog ermöglicht die Konfiguration:

- von IP-Adressen der Sammler
- der Ereignisfilterung für jeden Sammler auf der Grundlage des Schweregrads des Ereignisses

INHALT

- Abschnitt 4.13.5.1, „Eine Liste der entfernten Server anzeigen“
- Abschnitt 4.13.5.2, „Einen entfernten Server hinzufügen“
- Abschnitt 4.13.5.3, „Einen entfernten Server löschen“

Abschnitt 4.13.5.1

Eine Liste der entfernten Server anzeigen

Um eine Liste entfernter Server anzusehen, geben Sie Folgendes ein:

```
show running-config admin logging server
```

Falls entfernte Server konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config admin logging server
admin
 logging
  server 172.30.144.254
   enabled
   selector 1
    no negate
    facility-list [ all ]
   !
  !
 !
!
```

Falls keine entfernten Server konfiguriert wurden, fügen Sie je nach Bedarf Server hinzu. Weitere Informationen finden Sie unter Abschnitt 4.13.5.2, „Einen entfernten Server hinzufügen“.

Abschnitt 4.13.5.2
Einen entfernten Server hinzufügen

Um einen entfernten Server hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie einen entfernten Server hinzu, indem Sie Folgendes eingeben:

```
admin logging server address
```

   Erläuterung: *address* ist die IP-Adresse des entfernten Servers
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
enabled	Aktiviert/Deaktiviert den Feed zum dezentralen Logging-Server.
transport { transport }	**Zusammenfassung:** { udp, tcp } **Standard:** udp TCP oder UDP.
monitor-interface { monitor-interface }	**Zusammenfassung:** Eine Zeichenkette Die zu überwachende Schnittstelle. Wird die IP-Adresse an der Schnittstelle geändert, startet der Logging-Daemon neu.
port { port }	**Zusammenfassung:** Eine vorzeichenlose 16-Bit-Ganzzahl zwischen 1 und 65535 **Standard:** 514 Portnummer.

4. Konfigurieren Sie einen oder mehrere Selektoren für den Server. Für weitere Informationen siehe Abschnitt 4.13.6.2, „Einen Selektor zum Auswählen eines entfernten Servers hinzufügen“.
5. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 4.13.5.3
Einen entfernten Server löschen

Um einen entfernten Server zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den entfernten Server durch Eingabe von:

```
no admin logging server address
```

   Erläuterung:

   - *address* ist die IP-Adresse des entfernten Servers.
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 4.13.6

Selektoren für entfernte Server verwalten

Selektoren für entfernte Server filtern die an bestimmte Server gesendeten Informationen.

INHALT

- Abschnitt 4.13.6.1, „Eine Liste der Selektoren für entfernte Server anzeigen“
- Abschnitt 4.13.6.2, „Einen Selektor zum Auswählen eines entfernten Servers hinzufügen“
- Abschnitt 4.13.6.3, „Einen Selektor zum Auswählen eines entfernten Servers löschen“

Abschnitt 4.13.6.1

Eine Liste der Selektoren für entfernte Server anzeigen

Um eine Liste der Selektoren für entfernte Server anzusehen, geben Sie Folgendes ein:

```
show running-config admin logging server address selector
```

Erläuterung:

- *address* ist die IP-Adresse des entfernten Servers.

Falls Selektoren für entfernte Server konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config admin logging server 172.30.144.254 selector
admin
 logging
  server 172.30.144.254
   selector 1
    no negate
    facility-list [ all ]
   !
  !
 !
!
```

Falls keine Selektoren für entfernte Server konfiguriert wurden, fügen Sie je nach Bedarf Selektoren hinzu. Weitere Informationen finden Sie unter Abschnitt 4.13.6.2, „Einen Selektor zum Auswählen eines entfernten Servers hinzufügen“.

Abschnitt 4.13.6.2

Einen Selektor zum Auswählen eines entfernten Servers hinzufügen

Um einen Selektor zum Auswählen eines entfernten Servers hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie einen Selektor zum Auswählen eines entfernten Servers hinzu, indem Sie Folgendes eingeben:

   ```
   admin logging server address selector name
   ```

   Erläuterung:

   - *address* ist die IP-Adresse des entfernten Servers
   - *name* ist die Bezeichnung des Identifikators für den Protokoll-Selektor

3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
negate	Schließt Nachrichten vom Protokoll aus, die in den Feldern *Remote Server Selector* festgelegt sind. Durch Auswahl dieser Option gilt ein logisches NOT für die Selektordefinition. Beispiel: Durch Auswahl von **same**, **debug** und **mail** in den Feldern *Comparison*, *Level* und *Facility-list* werden Debug-Nachrichten aus dem Mail-Teilsystem ins Protokoll aufgenommen. Ist **Negate** ausgewählt, werden die Debug-Nachrichten aus dem Mail-Teilsystem ins Protokoll *nicht aufgenommen*.
comparison { comparison }	**Zusammenfassung:** { same_or_higher, same } **Standard:** same_or_higher Die Schweregrade der Nachrichten, die ins Protokoll aufgenommen werden sollen: • **same:** Es werden ausschließlich Nachrichten des Schweregrads aufgenommen, der im Feld *Level* ausgewählt ist. • **same_or_higher:** Es werden ausschließlich Nachrichten des Schweregrads aufgenommen, der im Feld *Level* ausgewählt ist, sowie sämtliche Nachrichten mit höherem Schweregrad. Beispiel: • Durch Auswahl von **debug** im Feld *Level* und von **same** im Feld *Comparison* werden nur Debug-Nachrichten ins Protokoll aufgenommen. • Durch Auswahl von **debug** im Feld *Level* und von **same_or_higher** im Feld *Comparison* werden Debug-Nachrichten und alle Nachrichten mit höherem Schweregrad ins Protokoll aufgenommen.
level { level }	**Zusammenfassung:** { emerg, alert, crit, err, warning, notice, info, debug, none, all } **Standard:** all Der allgemeine Schweregrad, der ins Protokoll aufgenommen werden soll. Bei **all** werden alle Nachrichten aufgenommen. Bei **none** werden alle Nachrichten ausgeschlossen. Weitere Grade sind nach steigendem Schweregrad aufgelistet.
facility-list { facility-list }	**Zusammenfassung:** { auth, authpriv, cron, daemon, ftp, kern, lpr, mail, news, security, syslog, user, uucp, local0, local1, local2, local3, local4, local5, local6, local7, all } Die Teilsysteme, die Protokollnachrichten generieren. Nachrichten vom ausgewählten Teilsystem werden ins Protokoll aufgenommen. Es muss mindestens ein Teilsystem ausgewählt sein; es können bis zu 8 Teilsysteme ausgewählt werden.

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 4.13.6.3

Einen Selektor zum Auswählen eines entfernten Servers löschen

Um einen Selektor zum Auswählen eines entfernten Servers zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den Selektor zum Auswählen eines entfernten Servers, indem Sie Folgendes eingeben:

```
no admin logging server address selector name
```

Erläuterung:

- *`address`* ist die IP-Adresse des entfernten Servers
- *`name`* ist die Bezeichnung des Identifikators für den Protokoll-Selektor

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 4.14

Die Softwarekonfiguration verwalten

Die Konfigurationsparameter für RUGGEDCOM ROX II können im Gerät gespeichert und später wieder geladen werden.

INHALT

- Abschnitt 4.14.1, „Die Konfiguration speichern“
- Abschnitt 4.14.2, „Eine Konfiguration laden“

Abschnitt 4.14.1

Die Konfiguration speichern

Um die Einstellungen der Konfiguration für RUGGEDCOM ROX II als separate Datei zu speichern, geben Sie Folgendes ein:

```
admin full-configuration-save format cli file-name filename
```

Erläuterung:

- *filename* ist die Bezeichnung der Konfigurationsdatei

Um alternativ nur die Standardwerte der Konfigurationsparameter in die gespeicherte Konfigurationsdatei aufzunehmen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Speichern Sie die Standardwerte, indem Sie Folgendes eingeben:

   ```
   save filename | details
   ```

   Erläuterung:

   - *filename* ist die Bezeichnung der Konfigurationsdatei

Sichern Sie bei Bedarf die Konfigurationsdatei nach dem Speichern auf einer FlashmicroSD/microSDHC-Flash-Karte. Weitere Informationen finden Sie unter Abschnitt 4.12.2, „Sichern von Dateien“.

Abschnitt 4.14.2

Eine Konfiguration laden

Um eine Konfigurationsdatei für RUGGEDCOM ROX II zu laden, gehen Sie wie folgt vor:

WICHTIG!
RUGGEDCOM ROX II akzeptiert nur Konfigurationsdateien von Geräten mit demselben Hardwareprofil und derselben Software-Version. Es wird empfohlen, nur Konfigurationsdateien von demselben Gerät zu laden.

1. [Optional] Installieren Sie die Konfigurationsdatei auf dem Gerät. Für weitere Informationen siehe Abschnitt 4.12.1, „Installieren von Dateien“.
2. Laden Sie die Konfigurationsdatei, indem Sie Folgendes eingeben:

   ```
   admin full-configuration-load format cli file-name filename
   ```

Erläuterung:

- *filename* ist die Bezeichnung der Konfigurationsdatei

3. Eine Bestätigungsaufforderung wird angezeigt. Geben Sie **yes** ein, um die Datei zu laden, bzw. **no** um abzubrechen.

Abschnitt 4.15

Ein Upgrade/Downgrade derRUGGEDCOM ROX II-Software ausführen

Dieser Abschnitt beschreibt, wie Sie die Version von RUGGEDCOM ROX II, die im Gerät läuft, ändern können.

INHALT

- Abschnitt 4.15.1, „Die Quelle für Upgrades konfigurieren“
- Abschnitt 4.15.2, „Einrichten eines Upgrade-Servers“
- Abschnitt 4.15.3, „Upgrade der Software RUGGEDCOM ROX II“
- Abschnitt 4.15.4, „Ein Software-Upgrade anhalten/ablehnen“
- Abschnitt 4.15.5, „Downgrade der RUGGEDCOM ROX II-Software durchführen“

Abschnitt 4.15.1

Die Quelle für Upgrades konfigurieren

Firmware zum Auf- und Abrüsten von RUGGEDCOM ROX II kann entweder von einem Upgrade-Server oder einem tragbarem microSD/microSDHC-Laufwerk hochgeladen werden. Information zum Einrichten eines Upgrade-Servers erhalten Sie unter Abschnitt 4.15.2, „Einrichten eines Upgrade-Servers“.

WICHTIG!
*Ein Trusted Root CA (Certified Authority)-Zertifikat ist erforderlich, wenn HTTPS zum Hochladen von Paketen von einem Upgrade-Server verwendet wird. Das Zertifikat wird über den Parameter **Server CA** ausgewählt. Ist ein Zertifikat nicht verfügbar, muss es auf das Gerät geladen werden. Für weitere Informationen siehe Abschnitt 6.6.4.3, „Hinzufügen eines CA-Zertifikats und der CRL“.*

Um die Quelle der RUGGEDCOM ROX II Software und eine spezifische Version festzulegen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***admin » software-upgrade » upgrade-settings*** und konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
repository-url { repository-url }	**Zusammenfassung:** Eine Zeichenkette Die URL für den Upgrade-Server oder das Dateisystem. Die URL HTTP, HTTPS, FTP, USB und SD werden unterstützt. Zum Upgrade von einem USB-Flash-Laufwerk oder einer microSD-Karte (sofern zutreffend) ist das URL-Format "usb://device-name/path-to-repository" bzw. "sd://device-name/path-to-repository". Um den Gerätenamen zu bestimmen, legen Sie Ihr Gerät ein und gehen Sie in der Web-Benutzeroberfläche zu "chassis", "storage", "removable" ODER

Parameter	Beschreibung
	geben Sie in der CLI "show chassis" ein. Beachten Sie, dass für jeden Datenträger nur eine Partition unterstützt wird. Bei allen anderen Protokollen ist das Format: "protocol://user:password@host:port/path-to-file". Wenn der Server keine Authentifizierung benötigt, lassen Sie "user:password" weg. Bei Verwendung des für das Protokoll voreingestellten Ports, lassen Sie ":port" weg.
target-version { target-version }	**Zusammenfassung:** Eine Zeichenkette Die Ziel-Softwareversion. Spezifizieren Sie einen bestimmten Software-Release im Format 'rrX.Y.Z' oder geben Sie 'current' ein, um auf das neueste auf dem Upgrade-Server verfügbare Software-Release zu aktualisieren.

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 4.15.2

Einrichten eines Upgrade-Servers

Ein Upgrade-Server mit Software-Repository kann für ein Upgrade oder Downgrade der RUGGEDCOM ROX II-Software über das Netzwerk verwendet werden.

Der Upgrade-Server muss folgende Anforderungen erfüllen:

- Jedes Gerät, auf dem ein Upgrade bzw. Downgrade durchgeführt wird, muss Zugriff auf einen Host haben, der als Web-Server bzw. FTP-Server agiert.
- Der Server muss über einen ausreichenden Speicherplatz für mindestens zwei vollständige Software-Releases verfügen. Jedes vollständige Software-Release ist circa 75 MB groß, obwohl die meisten Upgrades üblicherweise wesentlich kleiner sind.
- Der Server muss über eine ausreichende Bandbreite verfügen. Die Anforderungen an die Bandbreite hängen von der Anzahl an Geräten, der Größe des Upgrades und von der Zeit ab, wann die Geräte mit dem Upgrade beginnen. Die Bandbreite ist pro Gerät standardmäßig auf 500 kBit/s begrenzt. Ein kleiner Webserver (z. B. der Klasse 486) sollte in der Lage sein, Dateien bis zur Obergrenze der Bandbreite der Netzwerkschnittstelle zu dienen.
- Der Server muss mindestens so viele HTTP-, HTTPS- oder FTP-Verbindungen akzeptieren, wie Geräte im Netzwerk vorhanden sind.
- Der Server muss ein Verzeichnis speziell für die Software-Releases des RUGGEDCOM ROX II enthalten und veröffentlichen. Der Name dieses Verzeichnisses wird in den Upgrade-Einstellungen für jedes Gerät festgelegt.
- Die Kommunikation zwischen Server und Gerät muss über einen sicheren Kanal (z. B. IPSec) erfolgen.
- Für Upgrades via HTTPS muss der öffentliche Schlüssel des Servers von einer vertrauenswürdigen Zertifizierungsstelle (CA) signiert sein. Eine Liste anerkannter CAs ist verfügbar unter `/etc/ssl/certs/`

HINWEIS
Jedes Gerät sollte so konfiguriert werden, dass das Upgrade zu verschiedenen Zeiten ausgeführt wird, um die Auswirkungen auf das Netzwerk zu minimieren. Ein großes Upgrade (bzw. ein niedriger Bandbreite-begrenzender Wert auf jedem Gerät) kann dazu führen, dass alle Geräte das Upgrade zur selben Zeit durchführen.

INHALT

- Abschnitt 4.15.2.1, „Konfigurieren des Upgrade-Servers“

- Abschnitt 4.15.2.2, „Ein Software-Release zum Upgrade-Server hinzufügen“
- Abschnitt 4.15.2.3, „Firmware-Releases im Upgrade-Server hinzufügen“

Abschnitt 4.15.2.1
Konfigurieren des Upgrade-Servers

Damit der RUGGEDCOM ROX II Dateien von einem Upgrade-Server ordnungsgemäß abrufen kann, muss auf dem Server Folgendes konfiguriert werden:

- **MIME-Typen**
  Folgende MIME-Typen müssen für den ausgewählten Upgrade-Server (z. B. Microsoft IIS Manager, Apache HTTP Server, Lighttpd usw.) definiert werden, damit der RUGGEDCOM ROX II Dateien vom Upgrade-Server ordnungsgemäß abrufen kann:

  HINWEIS
  __2.x.y__ steht für die RUGGEDCOM ROX II-Version, wobei __x__ die Hauptversionsnummer und __y__ die Zwischenversionsnummer ist. Beispiel: __2.11.1__.

Dateityp	Dateiname	MIME-Typ
RUGGEDCOM ROX II-Image-Archiv	imagerr2.x.y-armhf.tar.bz2	application/x-bzip2
RUGGEDCOM ROX II-Upgrade-Archiv	rr2/dists/rr2.x.y/Release (extrahiert von rr2.x.y.zip)	text/plain
GNU Privacy Guard (GPG)	imagerr2.x.y-armhf.tar.bz2.gpg	text/plain

  Upgrades/Installationen der RUGGEDCOM ROX II-Software und -Anwendungen schlagen möglicherweise fehl, wenn diese MIME-Typen nicht konfiguriert sind.

- **Aktivieren von Double-Escaping**
  Double-Escaping erlaubt bestimmte doppelt codierte Zeichen (z. B. +, % und &) in einer URI. Da bestimmte Dateien in den Upgrade/Downgrade-Paketen des RUGGEDCOM ROX II ein *+*-Zeichen im Dateinamen enthalten, muss das Double-Escaping für den Upgrade-Server aktiviert werden. Wenn das Double-Escaping nicht aktiviert ist, sind bestimmte Dateien nicht abrufbar und das Upgrade schlägt fehl.

  Beim Internet Information Services (IIS)-Manager von Microsoft aktivieren Sie Double-Escaping durch Setzen des Attributs **allowDoubleEscaping** in `web.config` auf `true`.

```
<system.webServer>
 <security>
  <requestFiltering allowDoubleEscaping="true" />
 </security>
</system.webServer>
```

Weitere Informationen über das Konfigurieren von MIME-Typen und das Double-Escaping für den Upgrade-Server finden Sie im Benutzerhandbuch zum Produkt.

Abschnitt 4.15.2.2
Ein Software-Release zum Upgrade-Server hinzufügen

Software-Releases, einschließlich Updates, sind mithilfe einer Supportanfrage über die Website Siemens Industry Online Support [https://support.industry.siemens.com] erhältlich. Für weitere Informationen siehe https://support.industry.siemens.com/My/ww/en/requests.

Um Software-Releases zum Upgrade-Server hinzuzufügen, gehen Sie wie folgt vor:

1. Reichen Sie über Siemens Industry Online Support [https://support.industry.siemens.com] eine Supportanfrage ein. Der Siemens Kundensupport gibt Ihnen eine Anleitung, wie Sie das entsprechende Softwarepaket herunterladen können.
2. Laden Sie das Softwarepaket ins Upgrade-Verzeichnis auf dem Upgrade-Server herunter.

   HINWEIS
   *Die Dateinamen von Software-Releases haben die Form **rrX.Y.Z.zip**, wobei **X** für die Hauptversionsnummer, **Y** für die Zwischenversionsnummer und **Z** für die Patch-Nummer steht.*
3. Extrahieren Sie die komprimierte ZIP-Datei im Verzeichnis. Die Datei wird in einen Ordner extrahiert, der die gleiche Bezeichnung wie die Hauptversion hat (d. h. /rr2/dists/rr2.11.0). Nachfolgende Releases werden ebenfalls in diesen Ordner extrahiert (d. h. /rr2/dists/rr2.11.1).

Abschnitt 4.15.2.3
Firmware-Releases im Upgrade-Server hinzufügen

Bei entsprechender Konfigurierung kann RUGGEDCOM ROX II auf den Upgrade-Server zugreifen und die Firmware für das LTE-Modem mittels Fernzugriff hochrüsten. Weitere Informationen finden Sie unter Abschnitt 10.6.7, „Firmware-Updates verwalten“.

Siemens stellt eine komprimierte ZIP-Datei bereit, die das für das Firmware-Upgrade benötigte Package enthält.

Um eine Firmware-Release zum Upgrade-Server hinzuzufügen, gehen Sie wie folgt vor:

HINWEIS
Um zu erfahren, wie Sie die ZIP-Datei mit den benötigten Dateien für das Firmware-Upgrade erhalten, wenden Sie sich an den Siemens Kunden-Support.

1. Besorgen Sie sich die komprimierte ZIP-Datei mit der jeweiligen Firmware-Release bei Siemens.
2. Fügen Sie die ZIP-Datei im Upgrade-Verzeichnis auf dem Update-Server hinzu.
3. Extrahieren Sie die ZIP-Datei im Verzeichnis.

Abschnitt 4.15.3
Upgrade der Software RUGGEDCOM ROX II

RUGGEDCOM ROX II Software-Upgrades erfolgen zwischen zwei Partitionen. Eine Partition ist stets aktiv, während die andere stets inaktiv ist. Software-Upgrades werden immer auf der inaktiven Partition durchgeführt. Dadurch kann die aktive Partition während eines Software-Upgrades weiterhin normal funktionieren und der Benutzer kann ein Software-Upgrade auf die Vorgängerversion zurückstufen.

Nach erfolgreichem Software-Upgrade und Neustart wird die hochgerüstete Partition aktiviert.

WICHTIG!
Wenn ein microSD/microSDHC-Laufwerk verwendet wird, entfernen Sie das Laufwerk während der Dateiübertragung nicht.

HINWEIS
Während eines Software-Upgrades sind alle Parameter gesperrt, bis das Gerät neu gestartet und die hochgerüstete Partition in den aktiven Zustand versetzt wird. Dadurch werden im Anschluss an

das Upgrade vorgenommene Konfigurationsänderungen verhindert, die nicht auf die hochgerüstete Partition übernommen werden.

Sofern erforderlich, kann das Software-Upgrade jederzeit vor dem Neustart des Geräts gestoppt bzw. abgelehnt werden. Weitere Informationen zum Stoppen bzw. Ablehnen eines Software-Upgrades finden Sie unter Abschnitt 4.15.4, „Ein Software-Upgrade anhalten/ablehnen“.

HINWEIS
Sämtliche Systemkonfigurationen und Benutzerdateien (d.h. Konfigurationsdateien usw.) werden auf die hochgerüstete Partition übernommen.

HINWEIS
Wird beim Neustart der neu aufgerüsteten Partition ein schwerer Systemfehler erkannt, kehrt das Gerät automatisch zur vorherigen aktiven Partition zurück.

Zum Upgrade der Software RUGGEDCOM ROX II gehen Sie wie folgt vor:

1. Wenn es sich bei der Quelle der Software um ein microSD/microSDHC-Laufwerk handelt, stecken Sie das Laufwerk in den microSD/microSDHC-Anschluss am Gerät. Ausführliche Informationen hierzu finden Sie im *RUGGEDCOM RX1400 Installationshandbuch*.
2. Vergewissern Sie sich, dass die Quelle des Software-Upgrades konfiguriert wurde. Weitere Informationen finden Sie unter Abschnitt 4.15.1, „Die Quelle für Upgrades konfigurieren“.
3. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
4. Starten Sie den Assistent für Software-Upgrades durch Eingabe von:

   ```
   wizard rox_upgrade
   ```

   Der Assistent benötigt Benutzereingaben, um das Upgrade fertigzustellen. Befolgen Sie die Online-Anweisungen.

   Wenn der Upgrade-Vorgang beginnt, zeigt der Assistent den Status des Upgrades an. Beispiel:

   ```
   ruggedcom(config)# wizard rox_upgrade
   The upgrade repository url is set to: http://rceng03/debianppc/rr2
   Press <ENTER> to accept this or type a new address to change it:

   The software release you are upgrading to is: rr2
   Press <ENTER> to accept this or type a different version:

   Checking for a more recent version of the upgrade system
   Already running the most recent version of the upgrade system
   ****************************************************************
   Launching ROXII Upgrade.......

   Upgrading system to Partition 2
   Estimating size of upgrade. This may take a few minutes....
   31 packages to install, 20799050 bytes to download
   15768 files, 635375611 bytes will be copied to Partition 2
   Starting upgrade...

   Preparing to transfer files to alternate partition. You may not see activity for a few minutes....

   ---- File Transfer Phase: 635375611 bytes, 15768 files ----
   progress: 100%
   File transfer phase complete.

   Starting download of packages...

   ---- Package Download Phase ----
   progress: 100%
   ```

```
Download phase complete.

Installing packages...

---- Package Install phase ----
progress: 100%
Package installation complete.

Upgrade to partition 2 completed successfully.
A reboot is required to run the upgraded partition.
```

5. Wenn das Software-Upgrade erfolgreich war, starten Sie das Gerät neu oder lehnen das Software-Upgrade ab. Weitere Informationen finden Sie unter Abschnitt 4.6, „Gerät neu booten“ oder Abschnitt 4.15.4, „Ein Software-Upgrade anhalten/ablehnen“.

Abschnitt 4.15.4

Ein Software-Upgrade anhalten/ablehnen

Um ein Software-Upgrade anzuhalten/abzulehnen und zu der zuvor installierten Version zurückzukehren, gehen Sie wie folgt vor:

WICHTIG!
Ein Software-Upgrade kann nur abgelehnt werden, solange das Gerät noch nicht neu gebootet wurde. Wurde das Software-Upgrade bereits im Anschluss an ein erneutes Booten aktiviert, kann die frühere Software-Version, die auf der anderen Partition installiert ist, wieder aktiviert werden. Weitere Informationen finden Sie unter Abschnitt 4.15.5.1, „Ein Software-Upgrade rückgängig machen“.

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Um eine frühere Software-Version wieder zu aktivieren, geben Sie Folgendes ein:

```
admin software-upgrade decline-upgrade
```

Abschnitt 4.15.5

Downgrade der RUGGEDCOM ROX II-Software durchführen

Die RUGGEDCOM ROX II-Software kann jederzeit auf eine frühere Release herabgestuft werden.

INHALT

- Abschnitt 4.15.5.1, „Ein Software-Upgrade rückgängig machen“
- Abschnitt 4.15.5.2, „Downgrade mittels ROXflash“

Abschnitt 4.15.5.1

Ein Software-Upgrade rückgängig machen

Um eine frühere Version der RUGGEDCOM ROX II-Software wieder zu aktivieren, die in der inaktiven Partition gespeichert ist, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Um eine frühere Software-Version wieder zu aktivieren, geben Sie Folgendes ein:

```
admin software-upgrade rollback-reboot
```

Das Gerät wird automatisch neu gebootet. Sobald das Booten beendet ist, ist die zuvor inaktive Partition mit der älteren Software-Version aktiv.

Abschnitt 4.15.5.2

Downgrade mittels ROXflash

Mit ROXflash kann jede Vorgängerversion eines RUGGEDCOM ROX II Software-Images auf die inaktive Partition geflasht werden. Um ein RUGGEDCOM ROX II Software-Image zu erhalten, wenden Sie sich an den Siemens-Kundensupport.

Nach erfolgreichem Software-Downgrade und Neustart wird die herabgestufte Partition aktiviert.

WICHTIG!
Verwenden Sie ROXflash nur, um frühere Versionen der Software RUGGEDCOM ROX II zu installieren. Neuere Software-Versionen müssen mit den Software-Upgrade-Funktionen installiert werden. Weitere Informationen zum Upgrade der Software RUGGEDCOM ROX II finden Sie unter Abschnitt 4.15.3, „Upgrade der Software RUGGEDCOM ROX II“.

WICHTIG!
Wenn ein microSD/microSDHC-Laufwerk verwendet wird, entfernen Sie das Laufwerk während der Dateiübertragung nicht.

HINWEIS
Wird beim Neustart der neu herabgestuften Partition ein schwerer Systemfehler erkannt, kehrt das Gerät automatisch zur vorherigen aktiven Partition zurück.

Um die inaktive Partition mit einer Vorgängerversion der Software RUGGEDCOM ROX II zu flashen, gehen Sie wie folgt vor:

1. Wenden Sie sich an den Siemens-Kundensupport und fordern Sie die erforderliche Firmware-Version an. Es werden zwei Tarball-Dateien (*.tar.bz2) bereitgestellt: das Firmware-Image und eine GPG (GNU Private Guard)-Signaturdatei.
2. Fügen Sie beide Dateien dem Upgrade-Repository hinzu oder speichern Sie sie auf einem microSD/microSDHC-Laufwerk.
3. Wenn es sich bei der Quelle der Software um ein microSD/microSDHC-Laufwerk handelt, stecken Sie das Laufwerk in den microSD/microSDHC-Anschluss am Gerät. Ausführliche Informationen hierzu finden Sie im *RUGGEDCOM RX1400 Installationshandbuch*.
4. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.

   WICHTIG!
   Bei Downgrades über HTTPS (SSL) muss der öffentliche Schlüssel des Servers von einer vertrauenswürdigen Zertifizierungsstelle (CA) signiert sein.

5. Starten Sie den ROXflash-Assistenten durch Eingabe von:

   ```
   wizard rox_flash
   ```

   Der Assistent benötigt Benutzereingaben, um das Downgrade fertigzustellen. Befolgen Sie die Online-Anweisungen.

   Wenn der Downgrade-Vorgang beginnt, zeigt der Assistent den Status des Downgrades an. Beispiel:

```
ruggedcom(config)# wizard rox_flash
This wizard will flash a ROXII image to the inactive partition. On your next boot, that partition
will become active and you will boot into the flashed ROXII version. Your configurations will not
 be transferred.
Do you wish to continue?(y/n): y


Enter the url of the ROXII image. The following protocols are supported: http, https, ftp, ftps,
 usb and sd.
The url should take the form of protocol://user:password@host/path-to-file.
If the server does not require authentication, you may leave out 'user:password@'.

Enter url: ftp://root:admin@rceng03/debianppc/rr2/image/imagerr2.tar.bz2
Starting download of ROXII image...

######################################################################## 100.0%
Download complete.
Preparing partition #2 to be flashed...
Flashing image to partition#2...
progress: 100%
Flashed image detected to be version ROX 2 (2011-03-29 03:04)

The other partition was imaged successfully.
A reboot is required to boot the other partition.
```

6. Wenn das Software-Downgrade erfolgreich war, starten Sie das Gerät neu. Weitere Informationen finden Sie unter Abschnitt 4.6, „Gerät neu booten“.

5 Systemverwaltung

Dieses Kapitel beschreibt, wie Sie administrative Aufgaben in Bezug auf die Geräte-Identifikation, Benutzerberechtigungen, Alarmkonfiguration, Zertifikate und Schlüssel und vieles mehr ausführen können.

INHALT

- Abschnitt 5.1, „Systemname und Standort konfigurieren“
- Abschnitt 5.2, „Den Hostnamen konfigurieren“
- Abschnitt 5.3, „Benutzerspezifische Anpassung des Begrüßungsbildschirms“
- Abschnitt 5.4, „Die maximale Anzahl Sitzungen festlegen“
- Abschnitt 5.5, „Webschnittstellen-Sitzungen aktivieren und konfigurieren“
- Abschnitt 5.6, „Verwalten von Alarmen“
- Abschnitt 5.7, „Benutzer verwalten“
- Abschnitt 5.8, „Verwalten von Passwörtern und Passphrasen“
- Abschnitt 5.9, „Aufträge planen“

Abschnitt 5.1

Systemname und Standort konfigurieren

Um den Systemnamen und den Standort des Geräts zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***admin*** und konfigurieren Sie den/die folgenden Parameter nach Bedarf:

Parameter	Beschreibung
system-name { system-name }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 255 Zeichen **Standard:** System Name Ein verwaltungstechnisch zugewiesener Name für diesen verwalteten Knoten. Gemeinhin ist dies der vollqualifizierte Domain-Name des Knotens. Ist der Name unbekannt, ist der Wert eine leere Zeichenkette.
location { location }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 255 Zeichen **Standard:** Location Der physische Ort dieses Knotens (z. B. 'Verteilerschrank, 3. Etage'). Ist der Ort unbekannt, ist der Wert eine leere Zeichenkette.
contact { contact }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 255 Zeichen **Standard:** Contact Die Identifizierung der Kontaktperson für diesen verwalteten Knoten in Textform, zusammen mit Kontaktdaten dieser Person. Sind die Kontaktdaten unbekannt, ist der Wert eine leere Zeichenkette.

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 5.2
Den Hostnamen konfigurieren

Um den Hostnamen für das Gerät zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***admin » hostname*** und konfigurieren Sie den/die folgenden Parameter nach Bedarf:

WICHTIG!
Sonderzeichen (!@#$%^&()_+-={}[];:',<.>/?\|`~) sind in Hostnamen nicht zulässig.*

Parameter	Beschreibung
name { name }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 63 Zeichen **Standard:** ruggedcom Der Hostname ist der Name des Geräts.
domain { domain }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 253 Zeichen **Standard:** localdomain Die Domäne für diesen Hostnamen.

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 5.3
Benutzerspezifische Anpassung des Begrüßungsbildschirms

Bei der Anmeldung kann eine individuelle Begrüßung für die Web- und die CLI-Oberfläche angezeigt werden.

Um einen Begrüßungstext hinzuzufügen, geben Sie Folgendes ein:

```
admin authentication banner message
```

Erläuterung:

- *`message`* ist der benutzerdefinierte Begrüßungstext

Abschnitt 5.4
Die maximale Anzahl Sitzungen festlegen

Um die maximale Anzahl an Sitzungen festzulegen, die gleichzeitig offen sein können, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***admin » session-limits*** und konfigurieren Sie den/die folgenden Parameter nach Bedarf:

Parameter	Beschreibung
max-sessions-total { max-sessions-total }	**Zusammenfassung:** eine vorzeichenlose 32-Bit-Ganzzahl **Standard:** 70 Begrenzt die Gesamtzahl der gleichzeitigen Sitzungen mit ROX.

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 5.5

Webschnittstellen-Sitzungen aktivieren und konfigurieren

Um Webschnittstellen-Sitzungen zu aktivieren und zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***admin » webui*** und konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
enabled	**Zusammenfassung:** { true, false } **Standard:** true Ermöglicht es, WebUI-Funktionen am Gerät zu konfigurieren.
listen-ip { listen-ip }	**Zusammenfassung:** Eine Zeichenkette **Standard:** 0.0.0.0 Die IP-Adresse, an der die CLI WebUI-Anfragen empfängt.
port { port }	**Zusammenfassung:** Eine vorzeichenlose 16-Bit-Ganzzahl zwischen 0 und 65535 **Standard:** 443 Der Port, an dem die WebUI CLI-Anfragen empfängt.
extra-ip-ports { extra-ip-ports }	**Zusammenfassung:** Eine Zeichenkette Das WebUI empfängt auch an diesen IP-Adressen. Fügen Sie bei Port-Werten ':#' hinzu, um die nicht voreingestellten Port-Werte einzustellen (d. h. xxx.xxx.xxx.xxx:19343 [::]:16000). Bei Verwendung der Standardadresse legen Sie keine empfangende Adresse mit dem gleichen Port fest.
max-sessions { max-sessions }	**Zusammenfassung:** eine vorzeichenlose 32-Bit-Ganzzahl **Standard:** 20 Die maximale Anzahl gleichzeitiger WebUI-Sitzungen.
idle-timeout { idle-timeout }	**Zusammenfassung:** Eine Zeichenkette **Standard:** PT30M Das maximale Zeitintervall des betriebsfreien Zustands, bevor eine WebUI-Sitzung beendet wird. Wartet die Sitzung auf Meldungen oder steht ein bestätigtes Commit aus, wird kein Timeout für das Zeitintervall des betriebsfreien Zustands verwendet. Ein Wert von 0 bedeutet, dass kein Timeout erfolgt. PT30M steht für 30 Minuten.
ssl-redirect-enabled	**Zusammenfassung:** { true, false } **Standard:** true Leitet Verkehr von Port 80 an Port 443 weiter. In deaktiviertem Zustand wird Port 80 geschlossen.
client-certificate-verification { client-certificate-verification }	**Zusammenfassung:** { none, peer, fail-if-no-peer-cert } **Standard:** none

Parameter	Beschreibung
	Umfang der Verifizierung, den der Server an Zertifikaten des Clients vornimmt • none - Es wird keine Verifizierung vorgenommen. • peer - Der Server fragt den Client nach einem Client-Zertifikat, aber fällt nicht aus, falls der Client kein Client-Zertifikat vorweist. • fail-if-no-peer-cert - Der Server fordert vom Client ein Client-Zertifikat.

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 5.6

Verwalten von Alarmen

Das Alarmsystem im RUGGEDCOM ROX II informiert Benutzer bei Auftreten wichtiger Ereignisse. Das System ist in hohem Maße konfigurierbar und gestattet Benutzern Folgendes:

- Aktivieren/Deaktivieren der meisten Alarme mit Ausnahme von obligatorischen Alarmen
- Konfigurieren, ob ein Alarm das fehlersichere Relais auslöst und eine LED-Alarmanzeige am Gerät aufleuchtet
- Konfigurieren des Schweregrads der meisten Alarme (d.h. Notfall, Hinweis, kritisch, Fehler usw.) mit Ausnahme bestimmter Alarme mit festgelegtem Schweregrad

Jeder Alarm wird anhand seines Typs (oder Subsystems) kategorisiert:

Alarmtyp	Beschreibung
Admin	Admin-Alarme informieren über administrative Aspekte des Geräts wie Probleme mit Feature Keys.
Chassis	Chassis-Alarme informieren über physische oder elektrische Probleme oder über ähnlich wichtige Ereignisse. Hierzu zählen u.a. unregelmäßige Spannungen der Spannungsversorgung oder das Stecken oder Ziehen eines Moduls.
Switch	Switch-Alarme informieren über Link-up-/Link-down-Ereignisse an Switch-Schnittstellen.
Eth	Eth-Alarme informieren über Ereignisse im Zusammenhang mit dem fe-cm-Port wie Link-up-/Link-down-Ereignisse.
WAN	WAN-Alarme informieren über Ereignisse im Zusammenhang mit der T1/E1- und DDS-Schnittstelle wie Link-up-/Link-down-Ereignisse.
Cellmodem	Mobilfunk-Alarme informieren über Ereignisse im Zusammenhang mit der Mobilfunkschnittstelle wie Link-up-/Link-down-Ereignisse.
Security	Sicherheitsalarme informieren über Ereignisse im Zusammenhang mit abgelaufenen Zertifikaten. Dies erstreckt sich auf Warnmeldungen 30 Tage vor dem Ablaufen eines Zertifikats und bei Installation eines abgelaufenen Zertifikats.
Services	Service-Alarme informieren über Ereignisse im Zusammenhang mit RUGGEDCOM ROX II-Services wie Zeitdiensten, Verbindungs-Failover, Dynamic Domain Name Server (DNS) usw.

INHALT

- Abschnitt 5.6.1, „Vorkonfigurierte Alarme“
- Abschnitt 5.6.2, „Eine Liste der aktiven Alarme anzeigen“
- Abschnitt 5.6.3, „Alarme löschen und quittieren“
- Abschnitt 5.6.4, „Konfigurieren eines Alarms“

Abschnitt 5.6.1
Vorkonfigurierte Alarme

Der RUGGEDCOM ROX II ist mit einer Reihe vorkonfigurierter Alarme zum Überwachen und Schützen des Geräts ausgestattet.

Alarmtyp	Alarm	Beschreibung	Empfohlene Lösung
Admin	Featurekey mismatch	Der Feature Key stimmt nicht mit den Seriennummern des Steuermoduls und der Rückwand-Hardware überein.	Verschieben Sie den Feature Key auf das korrekte Gerät mit der passenden Hardware oder fordern Sie einen aktualisierten Key beim Siemens-Kundensupport an.
Chassis	PM1 bad supply	Die Eingangsleistung zum Power-Modul liegt außerhalb des Nennbetriebsbereichs.	Stellen Sie sicher, dass der Betriebsbereich der Eingangsleistung den Geräteanforderungen entspricht.
	PM1 MOV protection bad	Die Schutzkomponente des Metalloxidvaristors (MOV) im PM1-Power-Modul ist beschädigt.	Wenden Sie sich an den Siemens-Kundensupport, um das Power-Modul zurückzugeben.
	Real-time clock battery low	Die Batterie der Echtzeituhr (RTC) im Steuermodul ist erschöpft.	Wenden Sie sich an den Siemens-Kundensupport, um das Gerät zur Reparatur einzusenden.

Abschnitt 5.6.2
Eine Liste der aktiven Alarme anzeigen

Um eine Liste der aktiven Alarme für einen spezifischen Alarmtyp anzuzeigen, geben Sie Folgendes ein:

```
show admin alarms
```

Eine Tabelle oder Liste ähnlich dem folgenden Beispiel wird angezeigt:

```
ruggedcom# show admin alarms | tab
           ALARM  EVENT
SUBSYSTEM  ID     ID     SEVERITY  DESCRIPTION                DATE TIME                USER ACTIONS
  ACTUATORS
-------------------------------------------------------------------------------------------------------
switch     1      1      notice    Link-up on port swport/1   Thu Oct  2 09:28:25 2014  clear-or-ack
  none
switch     2      1      warning   Link-down on port swport/4 Thu Oct  2 09:28:23 2014  resolve-or-ack
  resolved
```

Informationen zum Löschen oder Quittieren von aktiven Alarmen finden Sie unter Abschnitt 5.6.3, „Alarme löschen und quittieren“.

Abschnitt 5.6.3
Alarme löschen und quittieren

Es gibt zwei Alarmarten: bedingungsabhängige und bedingungsunabhängige Alarme. Bedingungsabhängige Alarme werden erzeugt, wenn die Bedingung wahr ist, und gelöscht, wenn die Bedingung bereinigt und der Vorgang vom Benutzer quittiert ist. Bedingungsunabhängige Alarme werden erzeugt, wenn ein Ereignis eintritt (Benachrichtigung), und der Benutzer ist für die Löschung des Alarms verantwortlich.

Ein Beispiel für einen bedingungsabhängigen Alarm ist eine Meldung des Typs *link down*. Wenn die Bedingung bereinigt ist (d. h. die Verbindung ist wieder aktiv), werden LED und Alarmrelais ausgeschaltet, falls Option `auto-clear` für automatisches Löschen aktiviert ist.

Beispiele für bedingungsunabhängige Alarme sind Meldungen des Typs *link up* und interne Konfigurationsfehler.

INHALT

- Abschnitt 5.6.3.1, „Alarme löschen“
- Abschnitt 5.6.3.2, „Alarme quittieren“

Abschnitt 5.6.3.1

Alarme löschen

Nicht bedingte Alarme müssen vom Benutzer gelöscht werden. Bedingte Alarme werden, sofern konfiguriert, automatisch gelöscht.

Um alle löschbaren, nicht bedingten Alarme zu löschen, geben Sie Folgendes ein:

```
admin clear-all-alarms
```

Alternativ können Sie, um einen einzelnen nicht bedingten Alarm zu löschen, Folgendes eingeben:

```
admin alarms active-alarms subsystem [ admin | cellmodem | chassis | eth | services | security | switch
| wan ] id event clear
```

Erläuterung:

- *id* ist die ID für den gewählten Alarm
- *event* ist die ID für das gewählte Ereignis

Abschnitt 5.6.3.2

Alarme quittieren

Um alle aktiven Alarme zu quittieren, geben Sie Folgendes ein:

```
admin acknowledge-all-alarms
```

Alternativ, um einen einzelnen Alarm zu quittieren, geben Sie Folgendes ein:

```
admin alarms active-alarms type id event acknowledge
```

Erläuterung:

- *type* ist die Art des Alarms Optionen sind u.a. `admin`, `cellmodem`, `chassis`, `eth`, `security`, `switch`, ein `wan`.
- *id* ist die ID für den gewählten Alarm.
- *event* ist die ID für das gewählte Ereignis.

Abschnitt 5.6.4

Konfigurieren eines Alarms

Während alle Alarme auf dem Gerät vorkonfiguriert sind, können bestimmte Alarme geändert und an die Anwendung angepasst werden. Dies beinhaltet die Änderung des Schweregrads und die Aktivierung/Deaktivierung bestimmter Funktionen.

HINWEIS
Die Parameter `failrelay-enable` *und* `led-enable` *sind für* ***Link-up****-Alarme nicht konfigurierbar.*

Um einen Alarm zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Konfigurieren Sie den Alarm, indem Sie Folgendes eingeben:

   ```
   admin alarm-config subsystem [ admin | cellmodem | chassis | eth | services | security | switch | wan ] alarm-list id
   ```

   Erläuterung: *id* ist die ID für den gewählten Alarm.
3. Konfigurieren Sie je nach Bedarf die folgenden Parameter:

   HINWEIS
   Je nach Alarmtyp sind bestimmte Parameter nicht verfügbar.

   HINWEIS
   Alarmbeschreibungen sind nicht konfigurierbar.

Parameter	Beschreibung
severity { severity }	**Zusammenfassung:** { emergency, alert, critical, error, warning, notice, info, debug } Der Schweregrad ist einer der Folgenden: emergency, alert, critical, error, warning, notice, info und debug. Bei einigen Alarmen kann dies nicht geändert werden. Dieser Parameter ist obligatorisch.
admin-enable	In deaktiviertem Zustand wird der Alarm nicht in der aktiven Liste aufgeführt und löst keinen LED/Ausfallrelais aus.
failrelay-enable	In aktiviertem Zustand aktiviert dieser Alarm den Ausfallrelais.
led-enable	Die Haupt-LED 'Alarm' leuchtet in aktiviertem Zustand rot, sobald dieser Alarm ausgelöst ist. In deaktiviertem Zustand wird die Haupt-LED 'Alarm' von diesem Alarm nicht beeinflusst.
auto-clear	Die LED und das Ausfallrelais werden in aktiviertem Zustand automatisch gelöscht, wenn der Zustand gelöst ist.

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 5.7
Benutzer verwalten

In RUGGEDCOM ROX II können bis zu drei Benutzerprofile lokal im Gerät konfiguriert werden. Jedem Profil ist eines der folgenden Zugangsrechte zugeordnet:

- Guest
- Operator
- Admin

Die Zugangsrechte erlauben oder verbieten dem Benutzer die Änderung von Einstellungen und die Ausführung verschiedener Befehle.

Rechte	Benutzertyp		
	Guest	Operator	Admin
Einstellungen ansehen	✓	✓	✓
Protokolle löschen	✓	✓	✓
Alarme zurücksetzen	×	✓	✓
Statistiken löschen	×	✓	✓
Basiseinstellungen ändern	×	✓	✓
Erweiterte Einstellungen ändern	×	×	✓
Befehle ausführen	×	×	✓

ACHTUNG!
Sicherheitsgefahr – Risiko eines unberechtigten Zugriffs und/oder einer unberechtigten Nutzung. Um einen unbefugten Zugriff auf das Gerät zu verhindern, ändern Sie vor der Inbetriebnahme des Geräts die voreingestellten Passwörter für alle Benutzer. Weitere Informationen finden Sie unter Abschnitt 5.8.2, „Ein Benutzer-Passwort/-Passphrase festlegen“.

INHALT

- Abschnitt 5.7.1, „Eine Liste der Benutzer anzeigen“
- Abschnitt 5.7.2, „Hinzufügen eines Benutzers“
- Abschnitt 5.7.3, „Einen Benutzer löschen“
- Abschnitt 5.7.4, „Benutzer überwachen“

Abschnitt 5.7.1
Eine Liste der Benutzer anzeigen

Um eine Liste der Benutzerkonten anzusehen, geben Sie Folgendes ein:

```
show running-config admin users
```

Falls Benutzer konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config admin users | tab
admin
```

```
 users
  userid
NAME    PASSWORD                              ROLE
------------------------------------------------------
admin   $1$LmRO$j7/q/wtlwjfUvbOVrbt4o.    administrator
guest   $1$uGztU0$6b7YS6gqwtrelTzA/2noQ. guest
oper    $1$eSsFfFMh$NEHgTHsU1T4RRz8sXNV2F1  operator
```

Falls keine Benutzerkonten konfiguriert wurden, fügen Sie nach Bedarf Benutzerkonten hinzu. Weitere Informationen finden Sie unter Abschnitt 5.7.2, „Hinzufügen eines Benutzers“.

Abschnitt 5.7.2
Hinzufügen eines Benutzers

Um ein neues Benutzerkonto hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie das Benutzerkonto hinzu, indem Sie Folgendes eingeben:

   ```
   admin users userid name role role
   ```

   Erläuterung:

   - *name* ist die Bezeichnung des Benutzerkontos
   - *role* ist die Funktion des Benutzers. Es gibt folgende Optionen: `Administrator`, `Bediener`und `Gast`.
3. Befolgen Sie die Anweisungen in Abschnitt 5.8.2, „Ein Benutzer-Passwort/-Passphrase festlegen“, um das Benutzerpasswort festzulegen.
4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.
5. [Optional] Weisen Sie dem Benutzerkonto einen Benutzer-Authentifizierungsschlüssel zu, damit der Benutzer auf das Gerät über SSH ohne Eingabe von Passwort/Passphrase zugreifen kann. Weitere Informationen finden Sie unter Abschnitt 6.5.2, „Benutzer-Authentifizierungsschlüssel verwalten“.

Abschnitt 5.7.3
Einen Benutzer löschen

Um ein Benutzerkonto zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie das Benutzerkonto durch Eingabe von:

   ```
   no admin users userid name
   ```

   Erläuterung:

   - *name* ist der Name des Benutzerkontos
3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 5.7.4

Benutzer überwachen

Im Gerät angemeldete Benutzer werden vonRUGGEDCOM ROX II überwacht und können über die Bildschirm CLI angezeigt werden. RUGGEDCOM ROX II ermöglicht Administratoren die Überwachung und die Abmeldung von Benutzern und das Senden von Meldungen an alle Benutzer.

Um eine Liste der Benutzer zu sehen, die aktuell im Gerät angemeldet sind, geben Sie Folgendes ein:

```
who
```

Eine Tabelle oder Liste ähnlich der Folgenden wird angezeigt:

```
ruggedcom# who
Session User  Context From          Proto Date     Mode
*147    admin cli     192.168.0.200 ssh   11:04:54 operational
 145    admin webui   192.168.0.200 https 10:51:05 operational
```

INHALT

- Abschnitt 5.7.4.1, „Benutzer aus dem Netzwerk abmelden“
- Abschnitt 5.7.4.2, „Meldungen an Benutzer senden“

Abschnitt 5.7.4.1

Benutzer aus dem Netzwerk abmelden

Um einen Benutzer im Gerät abzumelden, geben Sie Folgendes ein:

Geben Sie Folgendes ein:

```
logout [ [ session | number ] [ user | profile ] ]
```

Erläuterung:

- *number* ist die Nummer der Sitzung
- *profile* ist der Name des Benutzerprofils

Abschnitt 5.7.4.2

Meldungen an Benutzer senden

Um eine Meldung an alle Benutzer oder an einen bestimmten Benutzer zu senden, geben Sie Folgendes ein:

```
send [ profile | all ] message
```

Erläuterung:

- *profile* ist der Name des Benutzerprofils
- *message* ist die Meldung

Abschnitt 5.8

Verwalten von Passwörtern und Passphrasen

Der RUGGEDCOM ROX II setzt die Eingabe separater Passwörter bzw. Passphrasen zum Anmelden an den unterschiedlichen Gerätemodi (normaler, Boot-, Service- und Wartungsmodus) voraus. Standardpasswörter werden zu Beginn für jeden Benutzertyp konfiguriert. Es wird dringend empfohlen, diese vor der Inbetriebnahme des Geräts zu ändern.

HINWEIS
Eine Liste mit den Standardpasswörtern finden Sie in Abschnitt 2.1, „Voreingestellte Benutzernamen und Passwörter“.

Die Komplexität jedes Passworts bzw. jeder Passphrase kann durch den Benutzer ausgewählt bzw. vom Gerät durch einen Administrator vorgegeben werden. Erfüllt ein Benutzerpasswort bzw. eine Passphrase nicht die Passwortanforderungen, wird ein Alarm generiert. Beispiel:

```
Error: Supplied password is shorter than the minimum password length: 12
```

Im Allgemeinen sollten Passwörter bzw. Passphrasen aus Folgendem bestehen:

- Einem Kleinbuchstaben
- Einem Großbuchstaben
- Einer Ziffer
- Einem Sonderzeichen (z. B. !@#$%^&*()_+-={}[];:',<.>/?\|`~)

HINWEIS
Die Benutzerauthentifizierung kann ebenfalls über einen RADIUS- oder TACACS+-Server verifiziert werden. Sofern für Authentifizierung und Autorisierung aktiviert, können RADIUS- oder TACACS+-Server genutzt werden. Für weitere Informationen über das Konfigurieren eines RADIUS- oder TACACS +-Servers siehe Abschnitt 6.5.3, „Verwalten der RADIUS-Authentifizierung“ und Abschnitt 6.5.4, „Konfigurieren der TACACS+-Authentifizierung“.

ACHTUNG!
Sicherheitsgefahr – Risiko des unbefugten Zugriffs und/oder Missbrauchs. Um einen unbefugten Zugriff auf das Gerät zu verhindern, ändern Sie vor der Inbetriebnahme des Geräts die voreingestellten Passwörter.

ACHTUNG!
Zugriffsrisiko - Gefahr von Datenverlust. Vergessen Sie nicht die Passwörter für das Gerät. Wenn sowohl das Wartungs- als auch das Boot-Passwort vergessen wurden, muss das Gerät zur Reparatur an Siemens Canada Ltd zurückgeschickt werden. Dieser Service wird nicht durch die Gewährleistung abgedeckt. Um wieder Zugriff auf das Gerät zu erhalten, können je nach zu ergreifender Maßnahme Daten verloren gehen.

INHALT

- Abschnitt 5.8.1, „Komplexitätsregeln für Passwörter/Passphrasen konfigurieren“
- Abschnitt 5.8.2, „Ein Benutzer-Passwort/-Passphrase festlegen“
- Abschnitt 5.8.3, „Festlegen des Boot-Passworts bzw. der Boot-Passphrase“
- Abschnitt 5.8.4, „Festlegen des Wartungs-Passworts bzw. der Wartungs-Passphrase“

- Abschnitt 5.8.5, „Rücksetzen des Admin-Passworts bzw. der Admin-Passphrase“
- Abschnitt 5.8.6, „Boot-Passwort/-Passphrase zurücksetzen“
- Abschnitt 5.8.7, „Rücksetzen des Wartungs-Passworts bzw. der Wartungs-Passphrase“

Abschnitt 5.8.1

Komplexitätsregeln für Passwörter/Passphrasen konfigurieren

Es können spezifische Regeln für die Komplexität von Passwörtern/Passphrasen konfiguriert werden. Dazu zählen das Definieren der Passwort-/Passphrasenlänge und das Festlegen von Anforderungen für Sonderzeichen.

Um Komplexitätsregeln für alle Passwörter/Passphrasen zu konfigurieren, gehen Sie wie folgt vor:

HINWEIS
Die Komplexitätsregeln für Passwörter/Passphrasen gelten nicht für Passwörter/Passphrasen, die bereits am Gerät konfiguriert wurden.

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***admin » authentication » password-complexity*** und konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
minimum-length { minimum-length }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 1 und 128 **Standard:** 12 Mindestlänge des Passworts.
maximum-length { maximum-length }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 1 und 128 **Standard:** 128 Maximale Länge des Passworts.
uppercase-required	**Zusammenfassung:** { true, false } **Standard:** true Das Passwort muss mindestens einen Großbuchstaben enthalten.
lowercase-required	**Zusammenfassung:** { true, false } **Standard:** true Das Passwort muss mindestens einen Kleinbuchstaben enthalten.
digits-required	**Zusammenfassung:** { true, false } **Standard:** true Das Passwort muss mindestens eine Ziffer enthalten.
special-characters-required	**Zusammenfassung:** { true, false } **Standard:** true Das Passwort muss mindestens ein nicht-alphanumerisches Zeichen enthalten. Zulässige Zeichen sind "!@#$%^&*()_+-={}[];:',<.>/?|`~".

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 5.8.2

Ein Benutzer-Passwort/-Passphrase festlegen

Um für ein Benutzerprofil ein Passwort/eine Passphrase festzulegen, gehen Sie wie folgt vor:

HINWEIS
RUGGEDCOM ROX II unterstützt die folgenden Sonderzeichen in Passwörtern/Passphrasen: !@#$ %^&()_+-={}[];:',<.>/?\| `~.*

1. Geben Sie den folgenden Befehl ein und drücken Sie anschließend auf **Enter**:

   ```
   admin users userid profile set-password new-password
   ```

   Erläuterung: *profile* ist das Benutzerprofil (z. B. admin, oper oder guest)

2. Geben Sie auf Aufforderung das neue Passwort/die Passphrase ein und drücken Sie anschließend auf **Enter**:

   ```
   Value for 'new-password' (<string, min: 1 chars, max: 128 chars>):
   ```

3. Bei der nächsten Aufforderung geben Sie das neue Passwort/die Passphrase erneut ein und drücken anschließend auf **Enter**:

   ```
   Value for 'new-password-repeat' (<string, min: 1 chars, max: 128 chars>):
   ```

   Das Passwort/die Passphrase ist aktualisiert und die folgende Meldung wird angezeigt, wenn das Passwort/die Passphrase den Komplexitätsregeln für Passwörter entspricht:

   ```
   set-password-result success
   ```

Abschnitt 5.8.3

Festlegen des Boot-Passworts bzw. der Boot-Passphrase

Das Boot-Passwort bzw. die Boot-Passphrase gewährt Zugriff auf den BIST-Modus und den Servicemodus, die nur über die Befehlszeilenschnittstelle (CLI) aufrufbar sind. Weitere Informationen über diese Modi finden Sie Abschnitt 2.5.1, „Auf die verschiedenen CLI-Modi zugreifen“ .

ACHTUNG!
Sicherheitsgefahr – Risiko des unbefugten Zugriffs und/oder Missbrauchs. Eine Benutzerauthentifizierung ist für den Zugriff auf den BIST-Modus nicht erforderlich. Konfigurieren Sie ein Boot-Passwort bzw. eine Boot-Passphrase, um den erstmaligen Zugriff auf das Gerät zu kontrollieren.

Um das Boot-Passwort bzw. die Boot-Passphrase festzulegen, gehen Sie wie folgt vor:

1. Geben Sie den folgenden Befehl ein:

   ```
   admin authentication set-boot-password new-password
   ```

2. Bei erster Aufforderung geben Sie das neue Passwort bzw. die neue Passphrase ein und drücken anschließend auf **Enter**.
3. Bei zweiter Aufforderung geben Sie das neue Passwort bzw. die neue Passphrase erneut ein und drücken anschließend auf **Enter**.
4. Bei dritter Aufforderung geben Sie das alte Passwort bzw. die alte Passphrase ein und drücken anschließend auf **Enter**. Wenn das Boot-Passwort bzw. die Boot-Passphrase erstmalig festgelegt wird, dann bestätigen Sie nur mit **Enter**.

Beispiel:

```
ruggedcom(config)# admin authentication set-boot-password new-password
Value for 'new-password' (<string, min: 0 chars, max: 128 chars>): ***************
Value for 'new-password-repeat' (<string, min: 0 chars, max: 128 chars>): ***************
Value for 'old-password' (<string, min: 0 chars, max: 128 chars>): ***************
set-password-result success
```

Abschnitt 5.8.4

Festlegen des Wartungs-Passworts bzw. der Wartungs-Passphrase

Das Passwort bzw. die Passphrase für die Wartung gewährt Zugriff auf den Wartungsmodus, der nur über die Befehlszeilenschnittstelle (CLI) aufrufbar ist. Weitere Informationen über diesen Modus finden Sie Abschnitt 2.5.1, „Auf die verschiedenen CLI-Modi zugreifen“ .

ACHTUNG!
Konfigurationsrisiko - Gefahr der Datenbeschädigung. Der Wartungsmodus dient zur Fehlersuche und sollte nur von Siemens-Technikern verwendet werden. Daher ist dieser Modus nicht vollständig dokumentiert. Eine falsche Anwendung der im Wartungsmodus verfügbaren Befehle kann den Betriebszustand des Geräts beschädigen und es unzugänglich machen.

Um das Passwort für die Wartung festzulegen, gehen Sie wie folgt vor:

1. Legen Sie das Passwort bzw. die Passphrase für die Wartung fest, indem Sie Folgendes eingeben:

   ```
   admin authentication set-maint-password new-password
   ```

2. Bei erster Aufforderung geben Sie das neue Passwort bzw. die neue Passphrase ein und drücken anschließend auf **Enter**.
3. Bei zweiter Aufforderung geben Sie das neue Passwort bzw. die neue Passphrase erneut ein und drücken anschließend auf **Enter**.
4. Bei dritter Aufforderung geben Sie das alte Passwort bzw. die alte Passphrase ein und drücken anschließend auf **Enter**. Wenn das Boot-Passwort bzw. die Boot-Passphrase erstmalig festgelegt wird, dann bestätigen Sie nur mit **Enter**.

Beispiel:

```
ruggedcom(config)# admin authentication set-maint-password new-password
Value for 'new-password' (<string, min: 0 chars, max: 128 chars>): ***************
Value for 'new-password-repeat' (<string, min: 0 chars, max: 128 chars>): ***************
Value for 'old-password' (<string, min: 0 chars, max: 128 chars>): ***************
set-password-result success
```

Abschnitt 5.8.5

Rücksetzen des Admin-Passworts bzw. der Admin-Passphrase

Das Admin-Passwort bzw. die Admin-Passphrase ermöglicht den Zugriff auf die Web-Schnittstelle und die Befehlszeilenschnittstelle (CLI). Geht das Passwort verloren, so ist der Zugriff auf diese Schnittstellen solange nicht möglich, bis Passwort bzw. Passphrase direkt auf dem Gerät zurückgesetzt wurde.

HINWEIS
Das Admin-Passwort bzw. die Admin-Passphrase muss auf beiden Partitionen zurückgesetzt werden.

Um das Admin-Passwort bzw. die Admin-Passphrase zurückzusetzen, gehen Sie wie folgt vor:

1. Rufen Sie den Servicemodus auf. Weitere Informationen finden Sie unter Abschnitt 2.7.2, „Zugreifen auf den Servicemodus“.
2. Geben Sie **`root`** ein und drücken Sie **Enter**. Sie werden aufgefordert, ein Passwort einzugeben.
3. Geben Sie das Passwort bzw. die Passphrase ein, welche(s) dem Root-Profil zugewiesen ist, und bestätigen Sie mit **Enter**. Das Standardpasswort ist *admin*.
4. Geben Sie **`confd_cli`** ein und drücken Sie **Enter**.
5. Aktivieren Sie den Auto-Assistenten, indem Sie Folgendes eingeben:

   ```
   autowizard true
   ```

6. Geben Sie **`config`** ein und drücken Sie **Enter**.

   WICHTIG!
   Passwörter bzw. Passphrasen, die Sonderzeichen und Leerzeichen enthalten, müssen in Anführungszeichen (z. B. "password!2#") gesetzt werden.

7. Um das Admin-Passwort bzw. die Admin-Passphrase zurückzusetzen, geben Sie Folgendes ein:

   ```
   admin users userid admin set-password new-password new-password-passphrase new-password-repeat new-password-passphrase
   ```

   Sofern Sonderzeichen verwendet werden, setzen Sie das Passwort wie folgt in doppelte Anführungszeichen (“):

   HINWEIS
   Der RUGGEDCOM ROX II unterstützt folgende Sonderzeichen in Passwörtern bzw. Passphrasen: !@# $%^&()_+-={}[];:',<.>/?\| `~.*

   ```
   admin users userid admin set-password new-password new-password-passphrase new-password-repeat new-password-passphrase
   ```

   Erläuterung:

   - *`new-password-passphrase`* ist das neue Passwort bzw. die neue Passphrase. Stellen Sie sicher, dass das Passwort bzw. die Passphrase mit den für dieses Gerät konfigurierten Passwort-Komplexitätsregeln übereinstimmt.
8. Starten Sie das Gerät neu. Weitere Informationen finden Sie unter Abschnitt 4.6, „Gerät neu booten“.
9. Sobald das Gerät mit dem Neustart beginnt, drücken Sie auf **ESC**. Eine Liste der möglichen Boot-Modi wird für jede Partition angezeigt.

   ```
   ****Boot Partition 4****
    [4-0]: Debian GNU/Linux, kernel 3.0.0-2-8360e
    [4-1]: Debian GNU/Linux, kernel 3.0.0-2-8360e (BIST mode)
    [4-2]: Debian GNU/Linux, kernel 3.0.0-2-8360e (single-user mode)
    [4-3]: Debian GNU/Linux, kernel 3.0.0-2-8360e (service mode)

    ****Boot Partition 6****
    [6-0]: Debian GNU/Linux, kernel 3.0.0-2-8360e
    [6-1]: Debian GNU/Linux, kernel 3.0.0-2-8360e (BIST mode)
    [6-2]: Debian GNU/Linux, kernel 3.0.0-2-8360e (single-user mode)
    [6-3]: Debian GNU/Linux, kernel 3.0.0-2-8360e (service mode)
   ```

```
Auto booting [4-0], Hit [ESC] key to stop:  0
Welcome to the boot menu. Please select from the following options:

Enter [BootPartition-BootTarget] (e.g. '4.0') to boot.
'h' Show this help menu
'l' List the available boot targets
'c' Exit to the boot loader command line

Will reboot after 60 seconds of inactivity
:
```

HINWEIS
Im vorstehenden Beispiel gibt der Text `Auto booting [4-0]` *an, dass Boot Partition 4 die aktive Partition ist.*

10. Rufen Sie die inaktive Partition auf, indem Sie die zugehörige Zielnummer eingeben. Wenn beispielsweise Boot Partition 4 die aktive Partition ist, dann geben Sie **`6-0`** ein und bestätigen mit **Enter**, um Boot Partition 6 aufzurufen.
11. Wiederholen Sie Schritt 1 und Schritt 10, um das Passwort bzw. die Passphrase auf der inaktiven Partition zurückzusetzen, und wechseln Sie zur ursprünglichen Partition zurück.

Abschnitt 5.8.6
Boot-Passwort/-Passphrase zurücksetzen

Das Boot-Passwort bzw. die Passphrase erlaubt den Zugang zum BIST-Modus (über den Befehl **`maint-login`**) und den Servicebetrieb. Bei Verlust dieses Passworts bzw. dieser Passphrase ist kein Zugang zu diesen Betriebsarten mehr möglich und das Passwort bzw. die Passphrase muss direkt im Gerät zurückgesetzt werden.

Um das Boot-Passwort bzw. die Passphrase zurückzusetzen, gehen Sie wie folgt vor:

1. Melden Sie sich im Wartungsmodus an. Weitere Informationen finden Sie unter Abschnitt 2.7.3, „Auf den Wartungsmodus zugreifen“.
2. Löschen Sie das aktuelle Passwort bzw. die Passphrase durch Eingabe von:

   ```
   rox-delete-bootpwd --force
   ```

3. Geben Sie **`exit`** ein und drücken Sie **Enter**.
4. Legen Sie ein neues Passwort bzw. eine neue Passphrase fest. Weitere Informationen finden Sie unter Abschnitt 5.8.3, „Festlegen des Boot-Passworts bzw. der Boot-Passphrase“.

Abschnitt 5.8.7
Rücksetzen des Wartungs-Passworts bzw. der Wartungs-Passphrase

Das Passwort bzw. die Passphrase für die Wartung gewährt Zugriff auf den Wartungsmodus. Geht das Passwort bzw. die Passphrase verloren, so ist der Zugriff auf diesen Modus solange nicht möglich, bis Passwort bzw. Passphrase direkt auf dem Gerät zurückgesetzt wurde.

ACHTUNG!
Konfigurationsrisiko - Gefahr der Datenbeschädigung. Der Wartungsmodus dient zur Fehlersuche und sollte nur von Siemens Canada Ltd-Technikern verwendet werden. Daher ist dieser Modus nicht vollständig dokumentiert. Eine falsche Anwendung der in diesem Wartungsmodus verfügbaren Befehle kann den Betriebszustand des Geräts beschädigen und es unzugänglich machen.

HINWEIS
Das Passwort bzw. die Passphrase für die Wartung muss auf beiden Partitionen zurückgesetzt werden.

Um das Passwort bzw. die Passphrase für die Wartung zurückzusetzen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Setzen Sie das Passwort für die Wartung zurück, indem Sie ein neues Passwort festlegen. Weitere Informationen finden Sie unter Abschnitt 5.8.4, „Festlegen des Wartungs-Passworts bzw. der Wartungs-Passphrase“.
3. Starten Sie das Gerät neu. Weitere Informationen finden Sie unter Abschnitt 4.6, „Gerät neu booten“.
4. Sobald das Gerät mit dem Neustart beginnt, drücken Sie auf **ESC**. Eine Liste der möglichen Boot-Modi wird für jede Partition angezeigt.

```
****Boot Partition 4****
 [4-0]: Debian GNU/Linux, kernel 3.0.0-2-8360e
 [4-1]: Debian GNU/Linux, kernel 3.0.0-2-8360e (BIST mode)
 [4-2]: Debian GNU/Linux, kernel 3.0.0-2-8360e (single-user mode)
 [4-3]: Debian GNU/Linux, kernel 3.0.0-2-8360e (service mode)

 ****Boot Partition 6****
 [6-0]: Debian GNU/Linux, kernel 3.0.0-2-8360e
 [6-1]: Debian GNU/Linux, kernel 3.0.0-2-8360e (BIST mode)
 [6-2]: Debian GNU/Linux, kernel 3.0.0-2-8360e (single-user mode)
 [6-3]: Debian GNU/Linux, kernel 3.0.0-2-8360e (service mode)

 Auto booting [4-0], Hit [ESC] key to stop:  0
 Welcome to the boot menu. Please select from the following options:

 Enter [BootPartition-BootTarget] (e.g. '4.0') to boot.
 'h' Show this help menu
 'l' List the available boot targets
 'c' Exit to the boot loader command line

 Will reboot after 60 seconds of inactivity
 :
```

HINWEIS
Im vorstehenden Beispiel gibt der Text `Auto booting [4-0]` *an, dass Boot Partition 4 die aktive Partition ist.*

5. Rufen Sie die inaktive Partition auf, indem Sie die zugehörige Zielnummer eingeben. Wenn beispielsweise Boot Partition 4 die aktive Partition ist, dann geben Sie **6-0** ein und bestätigen mit **Enter**, um Boot Partition 6 aufzurufen.
6. Loggen Sie sich bei RUGGEDCOM ROX II ein. Weitere Informationen über das Anmelden am RUGGEDCOM ROX II finden Sie in Abschnitt 2.2, „Anmelden“.
7. Wiederholen Sie Schritt 1 und Schritt 5, um das Passwort bzw. die Passphrase auf der inaktiven Partition zurückzusetzen, und wechseln Sie zur ursprünglichen Partition zurück.

Abschnitt 5.9
Aufträge planen

Der RUGGEDCOM ROX II-Planer ermöglicht das Anlegen von Aufträgen, die die CLI-Befehle zu einem bestimmten Datum und einer bestimmten Uhrzeit oder nach bestimmten Konfigurationsänderungen ausführen. Typische Beispiele sind die Planung regelmäßiger Löschungen der Systemprotokolle oder regelmäßiger Dateiübertragungen an entfernte Server.

Es gibt zwei Arten geplanter Aufträge:

- **Periodische Aufträge** werden zu einem bestimmten Datum und einer bestimmten Uhrzeit ausgeführt.
- **Aufträge bei Konfigurationsänderungen** werden nur ausgeführt, wenn ein bestimmtes Ereignis eintritt.

INHALT

- Abschnitt 5.9.1, „Eine Liste der geplanten Aufträge anzeigen“
- Abschnitt 5.9.2, „Einen geplanten Auftrag hinzufügen“
- Abschnitt 5.9.3, „Einen geplanten Auftrag löschen“

Abschnitt 5.9.1
Eine Liste der geplanten Aufträge anzeigen

Um eine Liste geplanter Aufträge anzusehen, geben Sie Folgendes ein:

```
show running-config admin scheduler
```

Falls Aufträge konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config admin scheduler | tab
admin
 scheduler
  scheduled-jobs
                                          JOB           JOB
SCHEDULER JOB                JOB      JOB   DAY     JOB   DAY
NAME                JOB TYPE MINUTE   HOUR  MONTH   MONTH WEEK    JOB COMMAND
-------------------------------------------------------------------------------
Backup              periodic 1        -     -       -     Monday  backupconfig
Clear Message Log   periodic 5        5:00  1       1     Monday  clearmessagelog
```

Falls keine Aufträge konfiguriert wurden, fügen Sie je nach Bedarf Aufträge hinzu. Weitere Informationen finden Sie unter Abschnitt 5.9.2, „Einen geplanten Auftrag hinzufügen“.

Abschnitt 5.9.2
Einen geplanten Auftrag hinzufügen

Um einen geplanten Auftrag hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***admin » scheduler***.
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
{ scheduler-job-name }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 64 Zeichen Der Name des geplanten Auftrags Der Name kann bis zu 64 Zeichen lang sein.
job-type { job-type }	**Zusammenfassung:** { configchange, periodic } **Standard:** periodic Bestimmt, wann ein geplanter Auftrag gestartet wird: • periodic: Der Auftrag startet an einem bestimmten Datum zu einer festgelegten Uhrzeit. • configchange: Der Auftrag startet, wenn sich die Konfiguration ändert.
job-minute { job-minute }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 128 Zeichen **Standard:** 0 Legt bei periodischen Aufträgen die Minuten der Startzeit des Auftrags fest. Gültige Werte liegen im Bereich von 0 bis 59. Ist kein Wert festgelegt, nimmt der Scheduler den Standardwert 0 und startet den Auftrag stündlich. • Um einen einzelnen Wert festzulegen, geben Sie den Wert in das Feld ein. Um beispielsweise den Auftrag 10 Minuten nach der vollen Stunde zu starten, geben Sie 10 ein. • Um eine Liste mit Werten anzugeben, geben Sie die Werte in eine kommaseparierte Liste ein. Um beispielsweise den Auftrag 15, 30 und 45 Minuten nach der vollen Stunde zu starten, geben Sie 15,30,45 ein. • Um einen Wertebereich anzugeben, geben Sie den Bereich als kommaseparierte Werte ein. Um beispielsweise den Auftrag minütlich zwischen 30 und 45 Minuten nach der vollen Stunde zu starten, geben Sie 30-45 ein. Für configchange-Aufträge ist dieser Parameter nicht erforderlich.
job-hour { job-hour }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 64 Zeichen Legt bei periodischen Aufträgen die Stunden der Startzeit des Auftrags im 24-Stunden-Uhr-Format fest. Gültige Werte liegen im Bereich von 0 bis 23. Ist kein Wert festgelegt, wird der Auftrag stündlich zu der im Minutenfeld angegebenen Uhrzeit gestartet. • Um einen einzelnen Wert festzulegen, geben Sie den Wert in das Feld ein. Um beispielsweise den Auftrag um 17:00 Uhr zu starten, geben Sie 17 ein. • Um eine Liste mit Werten anzugeben, geben Sie die Werte in eine kommaseparierte Liste ein. Um beispielsweise den Auftrag um 9:00 Uhr, 12:00 Uhr und 17:00 Uhr zu starten, geben Sie 9,12,17 ein. • Um einen Wertebereich anzugeben, geben Sie den Bereich als kommaseparierte Werte ein. Um beispielsweise den Auftrag stündlich zwischen 9:00 Uhr und 17:00 Uhr zu starten, geben Sie 9-17 ein. Für configchange-Aufträge ist dieser Parameter nicht erforderlich.
job-day-month { job-day-month }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 64 Zeichen Legt bei periodischen Aufträgen den Tag des Monats fest, an dem der geplante Auftrag ausgeführt werden soll. Gültige Werte liegen im Bereich von 1 bis 31. Ist kein Wert festgelegt, wird der Auftrag täglich gestartet. • Um einen einzelnen Wert festzulegen, geben Sie den Wert in das Feld ein. Um beispielsweise den Auftrag am 10. Tag des Monats zu starten, geben Sie 10 ein. • Um eine Liste mit Werten anzugeben, geben Sie die Werte in eine kommaseparierte Liste ein. Um beispielsweise den Auftrag am ersten, fünfzehnten und dreißigsten Tag des Monats zu starten, geben Sie 10,15,30 ein. • Um einen Wertebereich anzugeben, geben Sie den Bereich als kommaseparierte Werte ein. Um beispielsweise den Auftrag vom 1. zum 15. Tag des Monats zu starten, geben Sie 1-15 ein. Für configchange-Aufträge ist dieser Parameter nicht erforderlich.
job-month { job-month }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 32 Zeichen Legt bei periodischen Aufträgen den Monat fest, in dem der geplante Auftrag ausgeführt werden soll. Gültige Werte liegen im Bereich von 1 bis 12. Ist kein Wert festgelegt, wird der Auftrag täglich gestartet.

Parameter	Beschreibung
	• Um einen einzelnen Wert festzulegen, geben Sie den Wert in das Feld ein. Um beispielsweise Februar als Monat festzulegen, geben Sie 2 ein. • Um eine Liste mit Werten anzugeben, geben Sie die Werte in eine kommaseparierte Liste ein. Um beispielsweise Januar, Juni und Dezember als Monate festzulegen, geben Sie 1,6,12 ein. • Um einen Wertebereich anzugeben, geben Sie den Bereich als kommaseparierte Werte ein. Um beispielsweise Januar bis Juni als Monate festzulegen, geben Sie 1-6 ein. Für configchange-Aufträge ist dieser Parameter nicht erforderlich.
job-day-week { job-day-week }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 16 Zeichen Legt bei periodischen Aufträgen den Wochentag fest, an dem der geplante Auftrag ausgeführt werden soll. Gültige Einträge liegen im Bereich von 0 bis 6, wobei 0 für Sonntag, 1 für Montag usw. steht. Ist kein Wert festgelegt, wird der Auftrag täglich gestartet. • Um einen einzelnen Wert festzulegen, geben Sie den Wert in das Feld ein. Um beispielsweise Montag als Wochentag festzulegen, geben Sie 1 ein. • Um eine Liste mit Werten anzugeben, geben Sie die Werte in eine kommaseparierte Liste ein. Um beispielsweise Freitag, Samstag und Sonntag als Wochentage festzulegen, geben Sie 5,6,0 ein. • Um einen Wertebereich anzugeben, geben Sie den Bereich als kommaseparierte Werte ein. Um beispielsweise Montag bis Freitag als Wochentage festzulegen, geben Sie 1-5 ein. Für configchange-Aufträge ist dieser Parameter nicht erforderlich.
job-command { job-command }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 1024 Zeichen Ein oder mehrere Befehle, der/die zur geplanten Zeit ausgeführt werden soll/sollen. Dieser Befehl speichert z. B. die aktive Konfiguration in eine Datei mit dem Namen 'myconfig': show running-config | save myconfig. Verwenden Sie keine interaktiven Befehle oder Befehle, die eine manuelle Reaktion oder Bestätigung erfordern. Bei ihrer Eingabe in die CLI muss die Zeichenkette des Befehls zwischen Anführungszeichen gesetzt werden. Bei ihrer Eingabe in die WebUI muss die Zeichenkette des Befehls nicht zwischen Anführungszeichen gesetzt werden. Dieser Parameter ist obligatorisch.

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 5.9.3

Einen geplanten Auftrag löschen

Um einen geplanten Auftrag zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den geplanten Auftrag durch Eingabe von:

```
no admin scheduler schedule-jobs name
```

Erläuterung:

- *`name`* ist die Bezeichnung des geplanten Auftrags

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

6 Sicherheit

Dieses Kapitel beschreibt, wie Sie die sicherheitsbezogenen Merkmale von RUGGEDCOM ROX II konfigurieren und verwalten können.

INHALT

- Abschnitt 6.1, „CLI-Sitzungen aktiveren und konfigurieren“
- Abschnitt 6.2, „SFTP-Sitzungen aktivieren und konfigurieren“
- Abschnitt 6.3, „Schutz vor Brute-Force-Angriffen aktivieren/deaktivieren“
- Abschnitt 6.4, „Port-Sicherheit verwalten“
- Abschnitt 6.5, „Benutzerauthentifizierungen verwalten“
- Abschnitt 6.6, „Zertifikate und Schlüssel verwalten“
- Abschnitt 6.7, „Verwalten von Firewalls“

Abschnitt 6.1

CLI-Sitzungen aktiveren und konfigurieren

Um CLI-Sitzungen zu aktivieren und zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***admin » cli*** und konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
enabled	**Zusammenfassung:** { true, false } **Standard:** true Ermöglicht es, das Gerät per CLI über SSH und serielle Konsole zu konfigurieren.
listen-ip { listen-ip }	**Zusammenfassung:** Eine Zeichenkette **Standard:** 0.0.0.0 Die IP-Adresse, an der die CLI CLI-Anfragen empfängt.
port { port }	**Zusammenfassung:** Eine vorzeichenlose 16-Bit-Ganzzahl zwischen 0 und 65535 **Standard:** 22 Der Port, an dem die CLI auf CLI-Anfragen wartet.
extra-ip-ports { extra-ip-ports }	**Zusammenfassung:** Eine Zeichenkette Die CLI empfängt auch an diesen IP-Adressen. Fügen Sie bei Port-Werten ':#' hinzu, um die nicht voreingestellten Port-Werte einzustellen (d. h. xxx.xxx.xxx.xxx:19343 [::] [::]:16000). Bei Verwendung der Standardadresse legen Sie keine empfangende Adresse mit dem gleichen Port fest.
max-sessions { max-sessions }	**Zusammenfassung:** eine vorzeichenlose 32-Bit-Ganzzahl **Standard:** 10

Parameter	Beschreibung
	Die maximale Anzahl gleichzeitiger CLI-Sitzungen.
idle-timeout { idle-timeout }	**Zusammenfassung:** Eine Zeichenkette **Standard:** PT30M Die maximale Dauer, bevor eine unbenutzte CLI-Sitzung beendet wird. Die voreingestellte Dauer beträgt 30 Minuten, bzw. PT30M Eine Timeout-Dauer von 1 Jahr, 1 Monat, 2 Stunden und 30 Sekunden würde als P1Y1MT2H30S wiedergegeben werden. Der Countdown startet nicht, solange das System auf eine Meldung wartet oder Commits ausstehen. Änderungen werden bis zur nächsten CLI-Sitzung nicht wirksam.
greeting { greeting }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 8192 Zeichen Stellt die Begrüßung ein, sie erscheint, sobald sich ein Benutzer in der CLI anmeldet. Die Zeichenkette muss in Anführungszeichen angegeben werden.

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 6.2

SFTP-Sitzungen aktivieren und konfigurieren

Um SFTP-Sitzungen zu aktivieren und zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***admin*** und konfigurieren Sie den/die folgenden Parameter nach Bedarf:

Parameter	Beschreibung
enabled	**Zusammenfassung:** { true, false } **Standard:** false Aktiviert/Deaktiviert die SFTP-Bedienoberfläche.
listen-ip { listen-ip }	**Zusammenfassung:** Eine Zeichenkette **Standard:** 0.0.0.0 Die IP-Adresse, an der das SFTP SFTP-Anfragen empfängt.
port { port }	**Zusammenfassung:** Eine vorzeichenlose 16-Bit-Ganzzahl zwischen 0 und 65535 **Standard:** 2222 Der Port, an dem das SFTP SFTP-Anfragen empfängt.
extra-ip-ports { extra-ip-ports }	**Zusammenfassung:** Eine Zeichenkette Das SFTP empfängt auch an diesen IP-Adressen. Fügen Sie bei Port-Werten ':#' hinzu, um die nicht voreingestellten Port-Werte einzustellen (d. h. xxx.xxx.xxx.xxx:19343 [::] [::]:16000). Bei Verwendung der Standardadresse legen Sie keine empfangende Adresse mit dem gleichen Port fest.
max-sessions { max-sessions }	**Zusammenfassung:** eine vorzeichenlose 32-Bit-Ganzzahl **Standard:** 10 Dieser Parameter wird nicht unterstützt und sämtliche Werte werden vom System ignoriert.

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 6.3

Schutz vor Brute-Force-Angriffen aktivieren/deaktivieren

RUGGEDCOM ROX II verfügt über einen Schutzmechanismus vor Brute-Force-Angriffen (BFA), um Angriffe über die CLI, Webschnittstelle und NETCONF zu verhindern. Dieser Mechanismus analysiert das Verhalten von externen Hosts, die versuchen, auf den SSH-Port zuzugreifen, und hierbei insbesondere die Anzahl der fehlgeschlagenen Anmeldungen. Nach 15 fehlgeschlagenen Anmeldeversuchen wird die IP-Adresse des Hosts 720 Sekunden bzw. 12 Minuten lang gesperrt. Der Bereich von 15 fehlgeschlagenen Anmeldeversuchen existiert, um verschiedene Verfahren für den Zugriff auf das Gerät zu berücksichtigen, insbesondere wenn dieselben oder unterschiedliche Ports im Verlauf einer Reihe fehlgeschlagener Anmeldeversuche verwendet werden.

WICHTIG!
Der BFA-Schutzmechanismus gilt nicht für SNMP. Befolgen Sie entsprechende Sicherheitsmaßnahmen beim Konfigurieren von SNMP. Beispiel:

- *Verwenden Sie SNMP nicht über das Internet*
- *Verwenden Sie eine Firewall, um den Zugriff auf SNMP zu begrenzen*
- *Verwenden Sie SNMPv1 nicht*

HINWEIS
Fehlgeschlagene Anmeldeversuche müssen innerhalb eines Zeitraums von 10 Minuten erfolgen, damit sie als bösartiges Verhalten betrachtet werden.

Sobald dieser Zeitraum abgelaufen ist, wird es dem Host erneut gestattet, auf das Gerät zuzugreifen. Setzt sich das bösartige Verhalten von derselben IP-Adresse fort (z. B. weitere 15 fehlgeschlagene Anmeldeversuche), wird die IP-Adresse erneut gesperrt, doch die gesperrte Zeit erhöht sich um den Faktor 1,5. Dies wird fortgesetzt, solange der Host das gleiche Verhalten wiederholt.

WICHTIG!
Durch Aktivieren, Deaktivieren oder Ändern der Konfiguration der Firewall wird der BFA-Schutzmechanismus zurückgesetzt, jedoch nicht deaktiviert. Alle Hosts, die zuvor gesperrt wurden, können sich wieder anmelden. Wenn mehrere Hosts gleichzeitig aktiv angreifen, kann dies zu einer verminderten Systemleistung führen.

Beim Start des BFA-Schutzes wird der folgende Syslog-Eintrag angezeigt:

```
Jun  5 09:36:34 ruggedcom firewallmgr[3644]: Enabling Brute Force Attack Protection
```

Wenn die Anmeldung eines Hosts fehlschlägt, erfolgt ein Eintrag in `auth.log`. Beispiel:

```
Jun  5 10:12:52 ruggedcom confd[3386]: audit user: admin/0 Provided bad password
Jun  5 10:12:52 ruggedcom rmfmgr[3512]: login failed, reason='Bad password', user ipaddr='172.11.150.1'
Jun  5 10:12:52 ruggedcom confd[3386]: audit user: admin/0 Failed to login over ssh: Bad password
```

`Auth.log` gibt auch an, welche IP-Adressen derzeit gesperrt sind:

```
Jun 5 14:43:04 ruggedrouter sshguard[24720]: Blocking 172.59.9.1:4 for >630secs: 60 danger in 5 attacks
over 70 seconds (all: 60d in 1 abuses over 70s).
```

HINWEIS
Informationen zum Anzeigen von `auth.log`*finden Sie unter* *Abschnitt 4.13.1, „Anzeigen von Protokollen“*.

Wenn der Standardalarm für Brute-Force-Angriffe aktiviert ist, löst ein Host, der die maximale Anzahl fehlgeschlagener Anmeldeversuche überschreitet, einen Alarm aus. Der Alarm wird solange in der Liste aktiver Alarme aufgeführt, bis er aufgelöst und quittiert wird.

```
ruggedcom# show admin alarms active-alarms | tab
           ALARM  EVENT
SUBSYSTEM  ID     ID     SEVERITY  DESCRIPTION
-------------------------------------------------------------------------
security   2      1      alert     BFA from IP 172.30.151.141 is blocked
```

Um den BFA-Schutzmechanismus zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Aktivieren Sie den BFA-Schutzmechanismus durch Eingabe von:

   ```
   security bruteforce enabled
   ```

   Oder deaktivieren Sie den BFA-Schutzmechanismus durch Eingabe von:

   ```
   no security bruteforce enabled
   ```
3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.
4. [Optional] Aktivieren oder deaktivieren Sie den Standardalarm für Brute-Force-Angriffe. Weitere Informationen finden Sie unter Abschnitt 5.6.4, „Konfigurieren eines Alarms“.

Abschnitt 6.4

Port-Sicherheit verwalten

Portsicherheit (oder Port Access Control) bietet die Möglichkeit, den Zugriff über einzelne Ports zu authentifizieren, entweder per IEEE 802.1x-Authentifizierung, statischer Authentifizierung anhand der MAC-Adresse oder beidem.

Mit der IEEE 802.1x Authentifizierung authentifiziert RUGGEDCOM ROX II ein Quellgerät gegen einen entfernten RADIUS-Authentifizierungsserver. Der Zugriff wird gewährt, wenn das Quellgerät die richtigen Zugangsdaten angibt.

RUGGEDCOM ROX II authentifiziert mithilfe statischer Autorisierung das Quellgerät anhand seiner MAC-Adresse. Der Zugriff wird gewährt, wenn die MAC-Adresse in der Tabelle "Static MAC Address" angezeigt wird.

HINWEIS
RUGGEDCOM ROX II unterstützt die Authentifizierung von nur einem Host pro Port mit der Einstellung für den Port-Sicherheits-Modus von `802.1x` *oder* `802.1x/MAC-Auth`.

HINWEIS
RUGGEDCOM ROX II unterstützt sowohl PEAP als auch EAP-MD5. PEAP ist sicherer und wird vor EAP-MD5 empfohlen.

WICHTIG!
Wenden Sie keine Port-Sicherheit auf Core-Switch-Verbindungen an. Die Port-Sicherheit wird am Ende des Netzwerks eingesetzt, um den Zugriff auf bestimmte Geräte zu beschränken.

INHALT

- Abschnitt 6.4.1, „Port-Sicherheitskonzepte“
- Abschnitt 6.4.2, „Konfigurieren der Port-Sicherheit“
- Abschnitt 6.4.3, „Anzeigen des Sicherheitszustands von Switched-Ethernet-Ports“

Abschnitt 6.4.1

Port-Sicherheitskonzepte

Dieser Abschnitt beschreibt einige wesentliche Konzepte für die Implementierung von Port-Sicherheit in RUGGEDCOM ROX II.

INHALT

- Abschnitt 6.4.1.1, „Statische Authentifizierung anhand der MAC-Adresse“
- Abschnitt 6.4.1.2, „IEEE 802.1x-Authentifizierung“
- Abschnitt 6.4.1.3, „IEEE 802.1x-Authentifizierung mit Authentifizierung anhand der MAC-Adresse“
- Abschnitt 6.4.1.4, „Zuweisen von VLANs zu Tunnelattributen“

Abschnitt 6.4.1.1

Statische Authentifizierung anhand der MAC-Adresse

Bei diesem Verfahren gleicht das Gerät die MAC-Quelladressen empfangener Frames mit den Inhalten in der Tabelle "Static MAC Address" ab. RUGGEDCOM ROX II unterstützt außerdem eine hochflexible Port-Sicherheits-Konfiguration, die Netzwerkadministratoren dabei hilft, das Feature in verschiedenen Netzwerkszenarien zu nutzen.

Eine statische MAC-Adresse kann konfiguriert werden, ohne dass explizit eine Portnummer angegeben ist. In diesem Fall wird die konfigurierte MAC-Adresse automatisch an dem Port autorisiert, an dem sie erkannt wird. Damit können die Geräte ohne Neukonfiguration an einen beliebigen sicheren Port des Switch angeschlossen werden.

Das Gerät kann auch so programmiert werden, dass es eine vorkonfigurierte Anzahl der ersten MAC-Quelladressen auf einem sicheren Port lernt (und damit autorisiert). Dadurch können die entsprechenden sicheren Adressen beim ersten Konfigurieren der Authentifizierung anhand der MAC-Adresse an einem Port erfasst werden. Diese MAC-Adressen werden automatisch in die Tabelle "Static MAC Address" eingefügt und bleiben dort, bis sie vom Benutzer explizit entfernt werden.

Abschnitt 6.4.1.2

IEEE 802.1x-Authentifizierung

Der Standard IEEE 802.1x definiert einen Mechanismus für portbasierte Netzwerkzugriffskontrolle und bietet eine Möglichkeit zur Authentifizierung und Autorisierung von Geräten, die an LAN-Ports angeschlossen sind.

Obwohl IEEE 802.1x hauptsächlich in drahtlosen Netzwerken verwendet wird, wird dieses Verfahren auch bei verdrahteten Switches eingesetzt.

Der Standard IEEE 802.1x definiert drei Hauptkomponenten für das Authentifizierungsverfahren: Supplicant, Authenticator und Authentifizierungsserver. RUGGEDCOM ROX II unterstützt die Authenticator-Komponente.

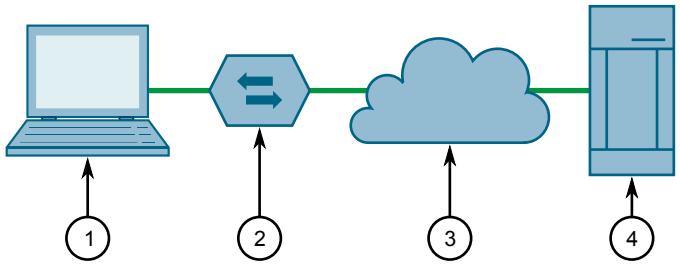


Abbildung 4: Allgemeine IEEE 802.1x-Topologie

1. Supplicant **2.** Authentificator-Gerät **3.** LAN **4.** Authentifizierungsserver

WICHTIG!
RUGGEDCOM ROX II unterstützt sowohl Protected Extensible Authentication Protocol (PEAP) als auch EAP-MD5. PEAP ist sicherer und wird empfohlen, wenn im Supplicant vorhanden.

IEEE 802.1x verwendet das Extensible Authentication Protocol (EAP), ein generisches PPP-Authentifizierungsprotokoll, das verschiedene Authentifizierungsverfahren unterstützt. EEE 802.1x definiert ein Protokoll für die Kommunikation zwischen dem Supplicant und dem Authenticator, das EAP over LAN (EAPOL) genannt wird.

RUGGEDCOM ROX II kommuniziert mit dem Authentifizierungsserver mithilfe von EAP über RADIUS

HINWEIS
Das Gerät unterstützt die Authentifizierung eines Hosts je Port.

HINWEIS
Wenn die MAC-Adresse des Hosts in der Tabelle "Static MAC Address" konfiguriert ist, wird er autorisiert, auch wenn die Hostauthentifizierung vom Authentifizierungsserver abgelehnt wird.

Abschnitt 6.4.1.3

IEEE 802.1x-Authentifizierung mit Authentifizierung anhand der MAC-Adresse

Dieses Verfahren, auch MAB (MAC-Authentication Bypass) genannt, wird häufig für Geräte wie VoIP-Telefone und Ethernet-Drucker verwendet, die das IEEE 802.1x-Protokoll nicht unterstützen. Mit diesem Verfahren können diese Geräte mit derselben Datenbankinfrastruktur wie in IEEE 802.1x authentifiziert werden.

IEEE 802.1x mit MAC-Authentication Bypass funktioniert folgendermaßen:

1. Das Gerät verbindet sich mit einem Switch-Port.
2. Der Switch lernt die MAC-Adresse des Geräts beim Empfang des ersten Frames vom Gerät (das Gerät sendet normalerweise bei erstmaligem Anschluss eine DHCP-Request-Nachricht).
3. Der Switch sendet eine EAP-Request-Nachricht an das Gerät und versucht, die IEEE 802.1x-Authentifizierung zu starten.

4. Der Switch bricht während des Wartens auf die EAP-Antwort ab, da das Gerät IEEE 802.1x nicht unterstützt.
5. Der Switch sendet eine Authentifizierungsnachricht an den Authentifizierungsserver, wobei die MAC-Adresse des Geräts als Benutzername und Passwort verwendet wird.
6. Der Switch authentifiziert das Gerät anhand der Antwort des Authentifizierungsservers bzw. weist es ab.

Abschnitt 6.4.1.4
Zuweisen von VLANs zu Tunnelattributen

Der RUGGEDCOM ROX II unterstützt das Zuweisen eines VLANs zu einem autorisierten Port mithilfe von Tunnelattributen gemäß RFC 3580 [http://tools.ietf.org/html/rfc3580], wenn der Sicherheitsmodus des Ports gesetzt ist auf `802.1x` oder `802.1x/MAC-Auth`.

In bestimmten Fällen ist es vorteilhaft, einen Port in ein bestimmtes VLAN zu platzieren, was vom Authentifizierungsergebnis abhängt. Beispiel:

- Um einem bestimmten Gerät zu gestatten, basierend auf seiner MAC-Adresse im selben VLAN zu bleiben während es sich innerhalb eines Netzwerks bewegt, konfigurieren Sie die Switches für den 802.1X/MAC-Auth-Modus.
- Um einem bestimmten Benutzer zu gestatten, basierend auf seinen Anmeldedaten im selben VLAN zu bleiben, wenn sich der Benutzer von verschiedenen Standorten aus anmeldet, konfigurieren Sie die Switches für den 802.1X-Modus.

Wenn der RADIUS-Server diese Funktion verwenden will, dann gibt er das gewünschte VLAN an, indem er Tunnelattribute in die Access-Accept-Nachricht aufnimmt. Der RADIUS-Server nutzt die folgenden Tunnelattribute für die VLAN-Zuweisung:

- Tunnel-Type=VLAN (13)
- Tunnel-Medium-Type=802
- Tunnel-Private-Group-ID=VLANID

Beachten Sie, dass die VLANID 12 Bits umfasst und einen Wert zwischen 1 und einschließlich 4094 hat. Die Tunnel-Private-Group-ID ist eine Zeichenkette gemäß RFC 2868 [http://tools.ietf.org/html/rfc2868] und der Integer-Wert der VLANID ist als Zeichenkette codiert.

Falls die Tunnelattribute nicht vom Authentifizierungsserver zurückgegeben werden, dann bleibt das dem Switch-Port zugewiesene VLAN unverändert.

Abschnitt 6.4.2
Konfigurieren der Port-Sicherheit

Um die Port-Sicherheit für einen Switched-Ethernet-Port zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***interface » switch » swport » {port} » port-security***, wobei *{port}* der Switched-Ethernet-Port ist.
3. Konfigurieren Sie die Portsicherheits-Einstellungen, indem Sie je nach Bedarf den/die folgenden Parameter konfigurieren:

Parameter	Beschreibung
security-mode { security-mode }	**Zusammenfassung:** { dot1x_mac_auth, dot1x, per_macaddress, off } **Standard:** off

Parameter	Beschreibung
	Aktiviert oder deaktiviert die Sicherheitsfunktionen für den Port. Die folgenden Arten der Zugriffskontrolle für den Port gibt es: • Statisch anhand der MAC-Adresse. Mit diesem Verfahren sollten berechtigte MAC-Adressen in der Tabelle Statische MAC-Adressen konfiguriert werden. Wenn einige MAC-Adressen im Voraus nicht bekannt sind (oder wenn der Port, hinter dem sie sich befinden werden, unbekannt ist), gibt es immer noch eine Option, um den Switch so zu konfigurieren, dass er eine bestimmte Anzahl von MAC-Adressen automatisch lernt. • Authentifikation nach Standard IEEE 802.1x. • IEEE 802.1X mit MAC-Authentifizierung, auch als MAB (MAC-Authentication Bypass) bekannt. Mit dieser Methode kann das Gerät Clients anhand der MAC-Adresse des Clients authentifizieren, wenn die IEEE 802.1X-Authentifizierung abläuft.
auto-learn { auto-learn }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 0 und 16 **Standard:** 0 Die maximale Anzahl an MAC-Adressen, die am Port dynamisch gelernt werden können. Wenn auf dem Port statische Adressen konfiguriert sind, ist die tatsächlich zulässige Anzahl der zu lernenden Adressen diese Anzahl minus die Anzahl der statischen MAC-Adressen.
shutdown-time { shutdown-time }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 1 und 86400 So lange ist eine Schnittstelle abzuschalten, wenn deren Sicherheit verletzt wurde.
admin-shutdown	Aktiviert/deaktiviert die administrative Abschaltung, wenn eine Verletzung der Sicherheit eintritt.

4. Konfigurieren Sie die IEEE 802.1x-Einstellungen, indem Sie je nach Bedarf den/die folgenden Parameter konfigurieren:

Parameter	Beschreibung
tx-period { tx-period }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 1 und 65535 **Standard:** 30 IEEE 802.1X PAE (Port Access Entity)-Parameter
quiet-period { quiet-period }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 0 und 65535 **Standard:** 60 Die Dauer ohne Versuche, einen Supplikanten zu erwerben, nachdem die Autorisierungssitzung fehlgeschlagen ist.
reauth-enable	Aktiviert oder deaktiviert die periodische Neuauthentifizierung.
reauth-period { reauth-period }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 60 und 86400 **Standard:** 3600 Die Dauer zwischen aufeinanderfolgenden Neuauthentifizierungen des Supplikants.
reauth-max { reauth-max }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 1 und 10 **Standard:** 2 Die Anzahl der zulässigen Neuauthentifizierungsversuche, bevor ein Port nicht mehr berechtigt ist.
supp-timeout { supp-timeout }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 1 und 300 **Standard:** 30 Die Dauer, um auf die Antwort des Supplikants auf das EAP-Paket des Authentifizierungsserver zu warten.
server-timeout { server-timeout }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 1 und 300 **Standard:** 30 Die Dauer, um auf die Antwort des Authentifizierungsserver auf das EAP-Paket des Supplikants zu warten.
max-request { max-request }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 1 und 10

Parameter	Beschreibung
	Standard: 2 Die maximale Anzahl an Wiederholungen, das EAP-Anfragenpaket des Authentifizierungsservers an den Supplikanten zu übertragen, bevor die Authentifizierungssitzung abläuft.

5. Wenn die IEEE 802.1x-Standardauthentifizierung oder IEEE 802.1x mit MAC-Authentifizierung ausgewählt ist, konfigurieren Sie einen primären und sekundären RADIUS-Server. Weitere Informationen finden Sie unter Abschnitt 6.5.3.3, „Eine RADIUS-Authentifizierung für Switched-Ethernet-Ports konfigurieren“.
6. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 6.4.3

Anzeigen des Sicherheitszustands von Switched-Ethernet-Ports

Um den Port-Sicherheitszustand aller Switched-Ethernet-Ports anzuzeigen, geben Sie Folgendes ein:

```
show interfaces switch swport port-security
```

Beispiel:

```
show interfaces switch swport port-security SLOT PORT STATUS ----------------------- swport 1 Unsecure
 swport 2 Unsecure swport 3 Unsecure swport 4 Unsecure swport 5 Unsecure swport 6 Unsecure
```

Um den Port-Sicherheitszustand eines bestimmten Switched-Ethernet-Ports anzuzeigen, geben Sie Folgendes ein:

```
show interfaces switch swport port port-security
```

Erläuterung:

- *`port`* ist die Nummer des Ports (oder eine Liste von Ports, wenn sie in einem Port-Trunk gebündelt sind) für das Modul.

Beispiel:

```
show interfaces switch swport 1 port-security port-security status Unsecure
```

Abschnitt 6.5

Benutzerauthentifizierungen verwalten

Dieser Abschnitt beschreibt, wie Benutzer authentifiziert werden können.

INHALT

- Abschnitt 6.5.1, „Einstellen des Benutzer-Authentifizierungsmodus“
- Abschnitt 6.5.2, „Benutzer-Authentifizierungsschlüssel verwalten“
- Abschnitt 6.5.3, „Verwalten der RADIUS-Authentifizierung“
- Abschnitt 6.5.4, „Konfigurieren der TACACS+-Authentifizierung“

Abschnitt 6.5.1

Einstellen des Benutzer-Authentifizierungsmodus

Der Benutzer-Authentifizierungsmodus regelt, ob Anmeldeversuche von Benutzern lokal, von einem RADIUS-Server oder von einem TACACS+-Server authentifiziert werden.

Um den Authentifizierungsmodus einzustellen, geben Sie Folgendes ein:

```
admin authentication mode [ localonly | radius_local | radius_then_local | tacacsplus_local |
tacacsplus_only ]
```

- Wenn **localonly** ausgewählt ist, dann werden Benutzer lokal authentifiziert, ungeachtet dessen, ob ein RADIUS-Server konfiguriert wurde.
- Wenn **radius_local** ausgewählt ist, dann werden Benutzer gegen den konfigurierten RADIUS-Server authentifiziert. Falls der RADIUS-Server nicht erreichbar ist, werden Benutzer lokal authentifiziert.
- Wenn **radius_then_local** ausgewählt ist, dann werden Benutzer zuerst gegen den konfigurierten RADIUS-Server authentifiziert. Falls die Benutzer nicht authentifiziert werden können, werden sie anschließend lokal authentifiziert.
- Wenn **tacacsplus_local** ausgewählt ist, dann werden Benutzer gegen den konfigurierten TACACS+-Server authentifiziert. Falls die Benutzer nicht authentifiziert werden können, werden sie anschließend lokal authentifiziert.
- Wenn **tacacsplus_only** ausgewählt ist, dann werden Benutzer gegen den konfigurierten TACACS+-Server authentifiziert. Falls die Benutzer nicht authentifiziert werden können, wird die Authentifizierung als fehlgeschlagen betrachtet und es werden keine weiteren Authentifizierungsversuche vorgenommen.

Abschnitt 6.5.2

Benutzer-Authentifizierungsschlüssel verwalten

Ein Benutzer-Authentifizierungsschlüssel ist der öffentliche Schlüssel in einem SSH-Schlüsselpaar. Ein Benutzer, der ein RUGGEDCOM ROX II-Benutzerkonto mit einem Authentifizierungsschlüssel verwendet, kann über Secure Shell (SSH) auf das Gerät zugreifen, ohne ein Passwort eingeben zu müssen, solange auf seiner Workstation der passende private Schlüssel gespeichert ist.

WICHTIG!
RUGGEDCOM ROX II akzeptiert nur öffentliche SSH2-RSA-Schlüssel. SSH1- oder DSA-Schlüssel werden nicht unterstützt.

INHALT

- Abschnitt 6.5.2.1, „Die einem Benutzer zugewiesenen Schlüssel bestimmen“
- Abschnitt 6.5.2.2, „Hinzufügen eines Benutzer-Authentifizierungsschlüssels“
- Abschnitt 6.5.2.3, „Einen Benutzerauthentifizierungsschlüssel löschen“
- Abschnitt 6.5.2.4, „Zuweisen/Trennen eines Benutzer-Authentifizierungsschlüssels“

Abschnitt 6.5.2.1

Die einem Benutzer zugewiesenen Schlüssel bestimmen

Um die Authentifizierungsschlüssel anzuzeigen, die einem Benutzerkonto zugewiesen sind, geben Sie Folgendes ein:

```
show runnging-config admin users userid name authorized-keys
```

Eine Liste wie im folgenden Beispiel wird angezeigt:

```
ruggedcom# show running-config admin users userid admin authorized-keys
admin
 users
  userid admin
   authorized-keys keyid key1
   !
  !
 !
!
```

Informationen über die Zuordnung von Schlüsseln zu Benutzerkonten finden Sie unter Abschnitt 6.5.2.4, „Zuweisen/Trennen eines Benutzer-Authentifizierungsschlüssels“.

Abschnitt 6.5.2.2

Hinzufügen eines Benutzer-Authentifizierungsschlüssels

Um dem Gerät einen Benutzer-Authentifizierungsschlüssel hinzuzufügen, gehen Sie wie folgt vor:

ACHTUNG!
Sicherheitsgefahr – Risiko des unbefugten Zugriffs und/oder Missbrauchs. Geben Sie den privaten Schlüssel weder außerhalb des Unternehmens noch an nicht vertrauenswürdiges Personal weiter. Der private Schlüssel wird zum Entschlüsseln der gesamten verschlüsselten Korrespondenz mit dem zugehörigen öffentlichen Schlüssel verwendet.

WICHTIG!
Es wird dringend empfohlen, eine Passphrase zur Verschlüsselung während der Schlüsselerstellung anzulegen. Diese Passphrase wird auf den privaten Schlüssel angewandt und hindert böswillige Benutzer am Zugriff auf dessen Inhalt.

HINWEIS
Es werden ausschließlich Schlüssel vom Typ SSH-2 RSA unterstützt.

1. Erstellen Sie auf der Workstation, die auf das Gerät zugreift, ein Paar RSA-basierter öffentlicher und privater SSH-Schlüssel durch Eingabe.
2. Öffnen Sie den öffentlichen Schlüssel und kopieren Sie seinen Inhalt.
3. Loggen Sie sich bei RUGGEDCOM ROX II ein. Weitere Informationen finden Sie unter Abschnitt 2.2, „Anmelden“.
4. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
5. Definieren Sie den Authentifizierungsschlüssel, indem Sie Folgendes eingeben:

   ```
   security crypto authorized-keys key
   ```

Erläuterung: *key* ist eine dem Authentifizierungsschlüssel zur einfachen Identifizierung zugewiesene Bezeichnung.

6. Geben Sie `contents` ein und drücken Sie anschließend auf **Enter**, um den Multiline-Modus aufzurufen.
7. Fügen Sie den Inhalt des öffentlichen Schlüssels ein und drücken Sie anschließend auf **Ctrl-D**. Beispiel:

```
ruggedcom(config)# security crypto authorized-keys key1 contents
(<string, min: 1 chars, max: 2048 chars>):
[Multiline mode, exit with ctrl-D.]
>{--contents--}
```

8. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.
9. Weisen Sie den neuen Authentifizierungsschlüssel einem oder mehreren Benutzerkonten zu. Weitere Informationen finden Sie unter Abschnitt 6.5.2.4, „Zuweisen/Trennen eines Benutzer-Authentifizierungsschlüssels“.

Abschnitt 6.5.2.3
Einen Benutzerauthentifizierungsschlüssel löschen

Um einen Benutzerauthentifizierungsschlüssel aus dem Gerät zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Trennen Sie den gewählten Authentifizierungsschlüssel vom/von den zugewiesenen Benutzerkonto/-konten. Weitere Informationen finden Sie unter Abschnitt 6.5.2.4, „Zuweisen/Trennen eines Benutzer-Authentifizierungsschlüssels“.
3. Löschen Sie den Authentifizierungsschlüssel, indem Sie Folgendes eingeben:

```
no security crypto authorized-keys key
```

Erläuterung: *key* ist die für eine einfache Identifizierung dem Authentifizierungsschlüssel zugewiesene Bezeichnung.

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 6.5.2.4
Zuweisen/Trennen eines Benutzer-Authentifizierungsschlüssels

Einer oder mehrere Authentifizierungsschlüssel können einem einzelnen Benutzerkonto zugewiesen werden, sodass Benutzer bei Bedarf von verschiedenen Workstations auf das Gerät zugreifen können.

WICHTIG!
Der passende öffentliche Schlüssel muss sich auf der Workstation des Benutzers befinden, sodass ein Anmelden auf dem Gerät ohne Passwort/Passphrase möglich ist.

» Zuweisen eines Authentifizierungsschlüssels

Um einem Benutzerkonto einen der auf dem Gerät verfügbaren Authentifizierungsschlüssel zuzuweisen, gehen Sie wie folgt vor:

1. Loggen Sie sich bei RUGGEDCOM ROX II ein. Weitere Informationen finden Sie unter Abschnitt 2.2, „Anmelden“.
2. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
3. Weisen Sie dem gewünschten Benutzerprofil einen Authentifizierungsschlüssel zu, indem Sie Folgendes eingeben:

   ```
   admin users name name authorized-keys key-id key
   ```

   Erläuterung:

   - *name* ist die Bezeichnung des Benutzerkontos
   - *key* ist die dem Authentifizierungsschlüssel zugewiesene Bezeichnung
4. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

» Trennen eines Authentifizierungsschlüssels

Um einen der Authentifizierungsschlüssel von einem Benutzerkonto zu trennen, gehen Sie wie folgt vor:

1. Loggen Sie sich bei RUGGEDCOM ROX II ein. Weitere Informationen finden Sie unter Abschnitt 2.2, „Anmelden“.
2. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
3. Trennen Sie den gewünschten Authentifizierungsschlüssel vom gewünschten Benutzerprofil, indem Sie Folgendes eingeben:

   ```
   no admin users name name authorized-keys key-id key
   ```

   Erläuterung:

   - *name* ist die Bezeichnung des Benutzerkontos
   - *key* ist die dem Authentifizierungsschlüssel zugewiesene Bezeichnung
4. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 6.5.3

Verwalten der RADIUS-Authentifizierung

RADIUS ist ein UDP-basiertes Protokoll für den Transport von Authentifizierungs-, Autorisierungs- und Konfigurationsinformationen zwischen einem Network Access Server (NAS), der seine Verbindungen authentifizieren möchte, und einem gemeinsamen Authentifizierungsserver. Es bietet zentrale Authentifizierung und Autorisierung für den Netzwerkzugriff.

RADIUS wird auch in Verbindung mit dem Standard IEEE 802.1x für Port-Sicherheit mit dem Extensible Authentication Protocol (EAP) verwendet.

HINWEIS
Weitere Informationen über das RADIUS-Protokoll finden Sie unter RFC 2865 [http://tools.ietf.org/html/rfc2865].

Weitere Informationen über das Extensible-Authentication-Protokoll (EAP) finden Sie unter RFC 3748 [http://tools.ietf.org/html/rfc3748].

WICHTIG!
*Der Benutzer-Authentifizierungsmodus muss auf **radius_local** oder tacacsplus_only gesetzt werden, damit Benutzer gegen den RADIUS-Server authentifiziert werden. Weitere Informationen über das Einstellen des Authentifizierungsmodus finden Sie unter Abschnitt 6.5.1, „Einstellen des Benutzer-Authentifizierungsmodus“.*

WICHTIG!
RADIUS-Nachrichten werden als UDP-Nachrichten gesendet. Der Switch und der RADIUS-Server müssen denselben Authentifizierungs- und Verschlüsselungsschlüssel verwenden.

In einer RADIUS-Zugriffsanfrage werden üblicherweise folgende Attribute und Werte vom RADIUS-Client an den RADIUS-Server gesendet:

Attribut	Wert
User-Name	{ Gast, Bediener, Admin }
User-Password	{ Passwort }
Service-Type	1
Vendor-Specific	Vendor-ID: 15004 Type: 1 Length: 11 String: RuggedCom

Ein RADIUS-Server kann auch zum Authentifizieren des Zugriffs an Ports mit aktivierter Sicherheit nach IEEE 802.1x verwendet werden. Wenn erforderlich, werden folgende Attribute vom RADIUS-Client an den RADIUS-Server gesendet:

Attribut	Wert
User-Name	{ Der Benutzername abgeleitet von der EAP-Identitätsantwort des Client }
NAS-IP-Address	{ Die IP-Adresse des Network Access Server }
Service-Type	2
Frame-MTU	1500
EAP-Message[a]	{ Eine bzw. mehrere vom authentifizierenden Peer empfangene Nachricht(en) }

[a] *Eine EAP-Nachricht ist ein Erweiterungsattribut für RADIUS nach RFC 2869 [http://freeradius.org/rfc/rfc2869.html#EAP-Message].*

Der primäre und sekundäre RADIUS-Server, die üblicherweise von einer gemeinsamen Datenbank aus operieren, können für Redundanz konfiguriert werden. Falls der erste Server nicht auf eine Authentifizierungsanfrage antwortet, wird die Anfrage an den zweiten Server weitergeleitet, bis eine positive/negative Quittierung empfangen wurde.

HINWEIS
Die RADIUS-Authentifizierungsaktivität wird erfasst in der Authentifizierungs-Protokolldatei `var/log/auth.log`. *Unter anderem werden Details zu jeder Authentifizierung einschließlich Zeitpunkt der Ausführung, Quelle und Ergebnis erfasst. Weitere Informationen über die Authentifizierungs-Protokolldatei finden Sie unter Abschnitt 4.13.1, „Anzeigen von Protokollen“.*

Der RUGGEDCOM ROX II unterstützt die RADIUS-Authentifizierung für die LOGIN- und PPP-Dienste. Es können verschiedene RADIUS-Server für die Authentifizierung beider Dienste unabhängig voneinander oder zusammen konfiguriert werden.

Der LOGIN-Dienst umfasst folgende Zugriffstypen:

- Lokaler Konsolenzugriff über den seriellen Port
- Dezentraler Shell-Zugriff über SSH und HTTPS
- Sichere Dateiübertragungen mit HTTPS, SCP und SFTP (basierend auf SSH)

Authentifizierungsanfragen für LOGIN-Dienste versuchen, RADIUS zuerst zu verwenden und lokale Authentifizierungseinstellungen werden ignoriert. Nur wenn keiner der konfigurierten RADIUS-Server (positiv/negativ) antwortet, authentifiziert der RUGGEDCOM ROX II Benutzer lokal.

Der PPP-Dienst steht für eingehende PPP-Verbindungen über ein Modem. Authentifizierungsanfragen an den PPP-Dienst verwenden nur RADIUS. Für den Fall, dass von den konfigurierten RADIUS-Servern keine Antwort empfangen wird, schließt der RUGGEDCOM ROX II die Authentifizierungsanfrage nicht ab.

INHALT

- Abschnitt 6.5.3.1, „Konfigurieren einer RADIUS-Authentifizierung für LOGIN-Services“
- Abschnitt 6.5.3.2, „Eine RADIUS-Authentifizierung für PPP-Services konfigurieren“
- Abschnitt 6.5.3.3, „Eine RADIUS-Authentifizierung für Switched-Ethernet-Ports konfigurieren“

Abschnitt 6.5.3.1

Konfigurieren einer RADIUS-Authentifizierung für LOGIN-Services

Um eine RADIUS-Authentifizierung für LOGIN-Services zu konfigurieren, gehen Sie wie folgt vor:

WICHTIG!
Bei Passwörtern wird zwischen Groß- und Kleinschreibung unterschieden.

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Geben Sie Folgendes ein:

```
admin authentication radius
```

3. [Optional] Wenn die Port-Sicherheit an beliebigen Ports aktiviert ist, konfigurieren Sie den/die folgenden Parameter, um Konflikte mit Firewall-Regeln/-Grundregeln zu vermeiden.

Parameter	Beschreibung
nas-ip-address { nas-ip-address }	**Zusammenfassung:** Eine Zeichenkette mit 7 bis 15 Zeichen oder eine Zeichenkette mit 6 bis 40 Zeichen Die NAS-IP-Adresse Diese als primäre IP-Adresse der Einheit festlegen.
nas-identifier { nas-identifier }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 64 Zeichen Die NAS-Kennung. Ist sie nicht festgelegt, wird der Hostname als NAS-Kennung verwendet.

4. Konfigurieren Sie den primären oder sekundären RADIUS-Server, indem Sie entweder **`primary`** oder **`secondary`** eingeben und konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
address { address }	**Zusammenfassung:** Eine Zeichenkette mit 7 bis 15 Zeichen oder eine Zeichenkette mit 6 bis 40 Zeichen Die IP-Adresse des Servers.
port-udp { port-udp }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 1 und 65535 **Standard:** 1812

Parameter	Beschreibung
	Der Netzanschluss des Servers.
password { password }	**Zusammenfassung:** Eine Zeichenkette Das Passwort des RADIUS-Servers.

5. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 6.5.3.2
Eine RADIUS-Authentifizierung für PPP-Services konfigurieren

Um eine RADIUS-Authentifizierung für PPP-Services zu konfigurieren, gehen Sie wie folgt vor:



WICHTIG!
Bei Passwörtern wird zwischen Groß- und Kleinschreibung unterschieden.

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Geben Sie Folgendes ein:

```
global ppp radius
```

3. Konfigurieren Sie den primären oder sekundären RADIUS-Server, indem Sie entweder **`primary`** oder **`secondary`** eingeben, und konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
address { address }	**Zusammenfassung:** Eine Zeichenkette mit 7 bis 15 Zeichen Die IPv4-Adresse des Servers.
port-udp { port-udp }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 1 und 65535 **Standard:** 1812
password { password }	**Zusammenfassung:** Eine Zeichenkette

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 6.5.3.3
Eine RADIUS-Authentifizierung für Switched-Ethernet-Ports konfigurieren

Um eine RADIUS-Authentifizierung für Switched-Ethernet-Ports zu konfigurieren, gehen Sie wie folgt vor:



WICHTIG!
Bei Passwörtern wird zwischen Groß- und Kleinschreibung unterschieden.

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Geben Sie Folgendes ein:

```
switch port-security radius
```

3. Konfigurieren Sie den primären oder sekundären RADIUS-Server, indem Sie entweder **`primary`** oder **`secondary`** eingeben, und konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
address { address }	**Zusammenfassung:** Eine Zeichenkette mit 7 bis 15 Zeichen Die IPv4-Adresse des Servers.
port-udp { port-udp }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 1 und 65535 **Standard:** 1812 Der IPv4-Port des Servers.
password { password }	**Zusammenfassung:** Eine Zeichenkette Das Passwort des Servers

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 6.5.4

Konfigurieren der TACACS+-Authentifizierung

TACACS+ (Terminal Access Controller Access-Control System Plus) ist ein TCP-basiertes Protokoll, das die Zugriffssteuerung für Router, Netzwerkzugangsserver und sonstige vernetzte Geräte über einen oder mehrere zentrale Server ermöglicht. TACACS+ bietet separate Authentifizierungs-, Autorisierungs- und Accounting-Dienste.

Der primäre und sekundäre TACACS+-Server, die üblicherweise von einer gemeinsamen Datenbank aus operieren, können für Redundanz konfiguriert werden. Falls der erste Server nicht auf eine Authentifizierungsanfrage antwortet, wird die Anfrage an den zweiten Server weitergeleitet, bis eine positive/negative Quittierung empfangen wurde.

WICHTIG!
*Der Benutzer-Authentifizierungsmodus muss auf **tacacsplus_local** oder **tacacsplus_only** gesetzt werden, damit Benutzer gegen den TACACS+-Server authentifiziert werden. Weitere Informationen über das Einstellen des Authentifizierungsmodus finden Sie unter Abschnitt 6.5.1, „Einstellen des Benutzer-Authentifizierungsmodus“.*

Um die TACACS+-Authentifizierung zu konfigurieren, gehen Sie wie folgt vor:

WICHTIG!
Bei Passwörtern wird zwischen Groß- und Kleinschreibung unterschieden.

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Geben Sie Folgendes ein:

```
admin authentication tacacsplus
```

3. Im Formular **Tacacsplus Server Privilege Settings** konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
admin-priv { admin-priv }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 5 Zeichen **Standard:** 15 Die Berechtigungsstufe(n) für Administrator (admin)-Benutzer. Optionen sind alle Zahlen zwischen 0 und 15 oder ein Bereich (z. B. 4-12).

Parameter	Beschreibung
oper-priv { oper-priv }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 5 Zeichen **Standard:** 2-14 Die Berechtigungsstufe(n) für Bediener (oper)-Benutzer. Optionen sind alle Zahlen zwischen 0 und 15 oder ein Bereich (z. B. 4-12).
guest-priv { guest-priv }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 5 Zeichen **Standard:** 1 Die Berechtigungsstufe(n) für Gast-Benutzer. Optionen sind alle Zahlen zwischen 0 und 15 oder ein Bereich (z. B. 4-12).

4. Im Formular **Primary Tacacsplus Server** konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
address { address }	**Zusammenfassung:** Eine Zeichenkette mit 7 bis 15 Zeichen oder eine Zeichenkette mit 6 bis 40 Zeichen Die IP-Adresse des TACACS+-Server.
port-tcp { port-tcp }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 1 und 65535 **Standard:** 49 Der zum Verbinden mit dem TACACS+-Server zu verwendende TCP-Port. Port 49 ist voreingestellt.
authentication-key { authentication-key }	**Zusammenfassung:** Eine Zeichenkette Der zur Ver- und Entschlüsselung von TACACS+-Verkehr zu verwendende Authentifizierungsschlüssel. Verwenden Sie nur ASCII-Zeichen.

5. Im Formular **Secondary Tacacsplus Server** konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
address { address }	**Zusammenfassung:** Eine Zeichenkette mit 7 bis 15 Zeichen oder eine Zeichenkette mit 6 bis 40 Zeichen Die IP-Adresse des TACACS+-Server.
port-tcp { port-tcp }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 1 und 65535 **Standard:** 49 Der zum Verbinden mit dem TACACS+-Server zu verwendende TCP-Port. Port 49 ist voreingestellt.
authentication-key { authentication-key }	**Zusammenfassung:** Eine Zeichenkette Der zur Ver- und Entschlüsselung von TACACS+-Verkehr zu verwendende Authentifizierungsschlüssel. Verwenden Sie nur ASCII-Zeichen.

6. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 6.6
Zertifikate und Schlüssel verwalten

RUGGEDCOM ROX II nutzt X.509v3-Zertifikate und -Schlüssel für den Aufbau sicherer Verbindungen für entfernte Logins (SSH) und den Web-Zugang (SSL).

Um die erste Konfiguration zu ermöglichen, werden alle RUGGEDCOM ROX II-Geräte mit einem Paar vorinstallierter Standardzertifikate und -schlüssel geliefert. Zertifikate und Schlüssel für TLS und SSH werden beim

erstmaligen Booten auch automatisch generiert und können durch benutzerdefinierte Zertifikate und Schlüssel ersetzt werden. Automatisch generierte Zertifikate sind selbst signiert.

Siemens empfiehlt, dass alle Zertifikate durch solche ersetzt werden, die von einer vertrauenswürdigen Zertifizierungsstelle signiert sind.

HINWEIS
Nur Benutzer mit Admin-Rechten können Zertifikate und Schlüssel im Gerät lesen/schreiben.

INHALT

- Abschnitt 6.6.1, „Den öffentlichen SSH/RSA-Schlüssel des lokalen Hosts anzeigen“
- Abschnitt 6.6.2, „Den Speicher für vertrauenswürdige Zertifikate verwalten“
- Abschnitt 6.6.3, „Zertifikate von Zertifizierungsstellen (CA) im Speicher für vertrauenswürdige Zertifikate verwalten“
- Abschnitt 6.6.4, „Zertifikate von Zertifizierungsstellen (CA) und CRLs verwalten“
- Abschnitt 6.6.5, „Private Schlüssel verwalten“
- Abschnitt 6.6.6, „Öffentliche Schlüssel verwalten“
- Abschnitt 6.6.7, „Zertifikate verwalten“

Abschnitt 6.6.1

Den öffentlichen SSH/RSA-Schlüssel des lokalen Hosts anzeigen

Um den öffentlichen SSH/RSA-Schlüssel des lokalen Hosts anzusehen, geben Sie Folgendes ein:

```
show security crypto local-host-ssh-rsa-public-key
```

Beispiel:

```
show security crypto local-host-ssh-rsa-public-key
local-host-ssh-rsa-public-key
 contents "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC0De8wvPyFpUGph9mwNXPcY3/
dwmQxIelGZe5Pt4laOZpeGOtuMSKqN15jcx29RcBasSdui5muLq8o+iBfDwjJw2q5WBBqyweXHgGYQGC58e7PQ5eYWIvu2L/
cgTpR3rCs4xTUh+URJYCTGEhh1V6jGOjuY8M3pO/iLPrwtZ066uyCqNoJLoptYnLfRDJu8AdWNdxLfXQsSv4XOB8hzYKekyg8bqsE/
w6b5MyE60Xc51f413PMicZz6WhBcuaqvutHxoIqCR6oI7fkLGGyWaeCzWUO02FplVfiJe1vTwAaa5+JAoSdPNzTJKrHvFE18SdEAlwpj4PMVIA7c
```

Abschnitt 6.6.2

Den Speicher für vertrauenswürdige Zertifikate verwalten

Der Speicher für vertrauenswürdige Zertifikate enthält eine umfangreiche Sammlung öffentlich zugänglicher X.509 v3 Root-Zertifikate. Sobald sie aktiviert und einer oder mehreren Zertifizierungsstellen (CA) zugeordnet sind, stehen diese Zertifikate für alle HTTPS- oder FTPS-Vorgänge zur Verfügung.

Eine Liste der Root-Zertifikate im Speicher finden Sie unter Abschnitt 6.6.2.3, „Liste der Stammzertifikate im Speicher der vertrauenswürdigen Zertifikate“.

HINWEIS
Der Speicher für vertrauenswürdige Zertifikate ist standardmäßig deaktiviert.

HINWEIS
Für bestimmte Funktionen wie IPsec-Tunnel können benutzerspezifische Zertifikate erforderlich sein. Weitere Informationen über das Hinzufügen benutzerspezifischer Zertifikate finden Sie unter Abschnitt 6.6.7.3, „Hinzufügen eines Zertifikats“.

INHALT

- Abschnitt 6.6.2.1, „Den Speicher für vertrauenswürdige Zertifikate konfigurieren“
- Abschnitt 6.6.2.2, „Den Speicher für vertrauenswürdige Zertifikate aktivieren/deaktivieren“
- Abschnitt 6.6.2.3, „Liste der Stammzertifikate im Speicher der vertrauenswürdigen Zertifikate“

Abschnitt 6.6.2.1

Den Speicher für vertrauenswürdige Zertifikate konfigurieren

Um den Speicher für vertrauenswürdige Zertifikate zu konfigurieren, gehen Sie wie folgt vor:

1. Vergewissern Sie sich, dass die erforderlichen Zertifikate der Zertifizierungsstelle und CRLs konfiguriert sind. Weitere Informationen finden Sie unter Abschnitt 6.6.4.3, „Hinzufügen eines CA-Zertifikats und der CRL“.
2. Aktivieren Sie den Speicher für vertrauenswürdige Zertifikate. Weitere Informationen finden Sie unter Abschnitt 6.6.2.2, „Den Speicher für vertrauenswürdige Zertifikate aktivieren/deaktivieren“.
3. Fügen Sie im Speicher Zertifikate der Zertifizierungsstelle hinzu, um die Authentizität der Root-Zertifikate zu bestätigen. Weitere Informationen finden Sie unter Abschnitt 6.6.3.2, „Ein Zertifikat von einer Zertifizierungsstelle zum Speicher für vertrauenswürdige Zertifikate hinzufügen“.

Abschnitt 6.6.2.2

Den Speicher für vertrauenswürdige Zertifikate aktivieren/deaktivieren

Um den Speicher für vertrauenswürdige Zertifikate zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Aktivieren oder deaktivieren Sie den Speicher für vertrauenswürdige Zertifikate, indem Sie Folgendes eingeben:

   Aktivieren

   ```
   admin system-ca-certificates use-public-ca-store
   ```

   Deaktivieren

   ```
   no admin system-ca-certificates use-public-ca-store
   ```

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 6.6.2.3

Liste der Stammzertifikate im Speicher der vertrauenswürdigen Zertifikate

Der Speicher der vertrauenswürdigen Zertifikate ergänzt bei Aktivierung die folgenden X.509 v3-Stammzertifikate:

- **spi-cacert-2008.crt**
  Subjektname: /C=US/ST=Indiana/L=Indianapolis/O=Software in the Public Interest/OU=hostmaster/CN=Certificate Authority/emailAddress=hostmaster@spi-inc.org
  Fingerabdruck: AF:70:88:43:83:82:02:15:CD:61:C6:BC:EC:FD:37:24:A9:90:43:1C
  Ausgabe: May 13 08:07:56 2008 GMT
  Ablauf: May 11 08:07:56 2018 GMT
- **Go_Daddy_Class_2_CA.crt**
  Subjektname: /C=US/O=The Go Daddy Group, Inc./OU=Go Daddy Class 2 Certification Authority
  Fingerabdruck: 27:96:BA:E6:3F:18:01:E2:77:26:1B:A0:D7:77:70:02:8F:20:EE:E4
  Ausgabe: Jun 29 17:06:20 2004 GMT
  Ablauf: Jun 29 17:06:20 2034 GMT
- **Staat_der_Nederlanden_EV_Root_CA**
  Subjektname: /C=NL/O=Staat der Nederlanden/CN=Staat der Nederlanden EV Root CA
  Fingerabdruck: 76:E2:7E:C1:4F:DB:82:C1:C0:A6:75:B5:05:BE:3D:29:B4:ED:DB:BB
  Ausgabe: Dec 8 11:19:29 2010 GMT
  Ablauf: Dec 8 11:10:28 2022 GMT
- **Certinomis_-_Root_CA**
  Subjektname: /C=FR/O=Certinomis/OU=0002 433998903/CN=Certinomis - Root CA
  Fingerabdruck: 9D:70:BB:01:A5:A4:A0:18:11:2E:F7:1C:01:B9:32:C5:34:E7:88:A8
  Ausgabe: Oct 21 09:17:18 2013 GMT
  Ablauf: Oct 21 09:17:18 2033 GMT
- **OISTE_WISeKey_Global_Root_GB_CA**
  Subjektname: /C=CH/O=WISeKey/OU=OISTE Foundation Endorsed/CN=OISTE WISeKey Global Root GB CA
  Fingerabdruck: 0F:F9:40:76:18:D3:D7:6A:4B:98:F0:A8:35:9E:0C:FD:27:AC:CC:ED
  Ausgabe: Dec 1 15:00:32 2014 GMT
  Ablauf: Dec 1 15:10:31 2039 GMT
- **QuoVadis_Root_CA**
  Subjektname: /C=BM/O=QuoVadis Limited/OU=Root Certification Authority/CN=QuoVadis Root Certification Authority
  Fingerabdruck: DE:3F:40:BD:50:93:D3:9B:6C:60:F6:DA:BC:07:62:01:00:89:76:C9
  Ausgabe: Mar 19 18:33:33 2001 GMT
  Ablauf: Mar 17 18:33:33 2021 GMT
- **DigiCert_Global_Root_G2**
  Subjektname: /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root G2

Fingerabdruck: DF:3C:24:F9:BF:D6:66:76:1B:26:80:73:FE:06:D1:CC:8D:4F:82:A4

Ausgabe: Aug 1 12:00:00 2013 GMT

Ablauf: Jan 15 12:00:00 2038 GMT

- **Entrust.net_Premium_2048_Secure_Server_CA**
  Subjektname: /O=Entrust.net/OU=www.entrust.net/CPS_2048 incorp. by ref. (limits liab.)/OU=(c) 1999 Entrust.net Limited/CN=Entrust.net Certification Authority (2048)

  Fingerabdruck: 50:30:06:09:1D:97:D4:F5:AE:39:F7:CB:E7:92:7D:7D:65:2D:34:31

  Ausgabe: Dec 24 17:50:51 1999 GMT

  Ablauf: Jul 24 14:15:12 2029 GMT
- **TÃœRKTRUST_Elektronik_Sertifika_Hizmet_SaÄŸlayÄ±cÄ±sÄ±_H5**
  Subjektname: /C=TR/L=Ankara/O=TxC3x9CRKTRUST Bilgi xC4xB0letixC5x9Fim ve BilixC5x9Fim GxC3xBCvenlixC4x9Fi Hizmetleri A.xC5x9E./CN=TxC3x9CRKTRUST Elektronik Sertifika Hizmet SaxC4x9FlayxC4xB1cxC4xB1sxC4xB1 H5

  Fingerabdruck: C4:18:F6:4D:46:D1:DF:00:3D:27:30:13:72:43:A9:12:11:C6:75:FB

  Ausgabe: Apr 30 08:07:01 2013 GMT

  Ablauf: Apr 28 08:07:01 2023 GMT
- **Verisign_Class_2_Public_Primary_Certification_Authority_-_G2**
  Subjektname: /C=US/O=VeriSign, Inc./OU=Class 2 Public Primary Certification Authority - G2/OU=(c) 1998 VeriSign, Inc. - For authorized use only/OU=VeriSign Trust Network

  Fingerabdruck: B3:EA:C4:47:76:C9:C8:1C:EA:F2:9D:95:B6:CC:A0:08:1B:67:EC:9D

  Ausgabe: May 18 00:00:00 1998 GMT

  Ablauf: Aug 1 23:59:59 2028 GMT
- **UTN_USERFirst_Email_Root_CA**
  Subjektname: /C=US/ST=UT/L=Salt Lake City/O=The USERTRUST Network/OU=http://www.usertrust.com/CN=UTN-USERFirst-Client Authentication and Email

  Fingerabdruck: B1:72:B1:A5:6D:95:F9:1F:E5:02:87:E1:4D:37:EA:6A:44:63:76:8A

  Ausgabe: Jul 9 17:28:50 1999 GMT

  Ablauf: Jul 9 17:36:58 2019 GMT
- **AC_RaÃz_CerticÃ¡mara_S.A.**
  Subjektname: /C=CO/O=Sociedad Cameral de CertificacixC3xB3n Digital - CerticxC3xA1mara S.A./CN=AC RaxC3xADz CerticxC3xA1mara S.A.

  Fingerabdruck: CB:A1:C5:F8:B0:E3:5E:B8:B9:45:12:D3:F9:34:A2:E9:06:10:D3:36

  Ausgabe: Nov 27 20:46:29 2006 GMT

  Ablauf: Apr 2 21:42:02 2030 GMT
- **IGC_A**
  Subjektname: /C=FR/ST=France/L=Paris/O=PM/SGDN/OU=DCSSI/CN=IGC/A/emailAddress=igca@sgdn.pm.gouv.fr

  Fingerabdruck: 60:D6:89:74:B5:C2:65:9E:8A:0F:C1:88:7C:88:D2:46:69:1B:18:2C

Ausgabe: Dec 13 14:29:23 2002 GMT

Ablauf: Oct 17 14:29:22 2020 GMT

- **Verisign_Class_1_Public_Primary_Certification_Authority**
  Subjektname: /C=US/O=VeriSign, Inc./OU=Class 1 Public Primary Certification Authority

  Fingerabdruck: CE:6A:64:A3:09:E4:2F:BB:D9:85:1C:45:3E:64:09:EA:E8:7D:60:F1

  Ausgabe: Jan 29 00:00:00 1996 GMT

  Ablauf: Aug 2 23:59:59 2028 GMT
- **AffirmTrust_Premium_ECC**
  Subjektname: /C=US/O=AffirmTrust/CN=AffirmTrust Premium ECC

  Fingerabdruck: B8:23:6B:00:2F:1D:16:86:53:01:55:6C:11:A4:37:CA:EB:FF:C3:BB

  Ausgabe: Jan 29 14:20:24 2010 GMT

  Ablauf: Dec 31 14:20:24 2040 GMT
- **Staat_der_Nederlanden_Root_CA_-_G3**
  Subjektname: /C=NL/O=Staat der Nederlanden/CN=Staat der Nederlanden Root CA - G3

  Fingerabdruck: D8:EB:6B:41:51:92:59:E0:F3:E7:85:00:C0:3D:B6:88:97:C9:EE:FC

  Ausgabe: Nov 14 11:28:42 2013 GMT

  Ablauf: Nov 13 23:00:00 2028 GMT
- **Swisscom_Root_CA_1**
  Subjektname: /C=ch/O=Swisscom/OU=Digital Certificate Services/CN=Swisscom Root CA 1

  Fingerabdruck: 5F:3A:FC:0A:8B:64:F6:86:67:34:74:DF:7E:A9:A2:FE:F9:FA:7A:51

  Ausgabe: Aug 18 12:06:20 2005 GMT

  Ablauf: Aug 18 22:06:20 2025 GMT
- **ComSign_CA**
  Subjektname: /CN=ComSign CA/O=ComSign/C=IL

  Fingerabdruck: E1:A4:5B:14:1A:21:DA:1A:79:F4:1A:42:A9:61:D6:69:CD:06:34:C1

  Ausgabe: Mar 24 11:32:18 2004 GMT

  Ablauf: Mar 19 15:02:18 2029 GMT
- **Sonera_Class_2_Root_CA**
  Subjektname: /C=FI/O=Sonera/CN=Sonera Class2 CA

  Fingerabdruck: 37:F7:6D:E6:07:7C:90:C5:B1:3E:93:1A:B7:41:10:B4:F2:E4:9A:27

  Ausgabe: Apr 6 07:29:40 2001 GMT

  Ablauf: Apr 6 07:29:40 2021 GMT
- **GeoTrust_Primary_Certification_Authority_-_G3**
  Subjektname: /C=US/O=GeoTrust Inc./OU=(c) 2008 GeoTrust Inc. - For authorized use only/CN=GeoTrust Primary Certification Authority - G3

  Fingerabdruck: 03:9E:ED:B8:0B:E7:A0:3C:69:53:89:3B:20:D2:D9:32:3A:4C:2A:FD

Ausgabe: Apr 2 00:00:00 2008 GMT

Ablauf: Dec 1 23:59:59 2037 GMT

- **Comodo_AAA_Services_root**
  Subjektname: /C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate Services

  Fingerabdruck: D1:EB:23:A4:6D:17:D6:8F:D9:25:64:C2:F1:F1:60:17:64:D8:E3:49

  Ausgabe: Jan 1 00:00:00 2004 GMT

  Ablauf: Dec 31 23:59:59 2028 GMT
- **DigiCert_Global_Root_G3**
  Subjektname: /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root G3

  Fingerabdruck: 7E:04:DE:89:6A:3E:66:6D:00:E6:87:D3:3F:FA:D9:3B:E8:3D:34:9E

  Ausgabe: Aug 1 12:00:00 2013 GMT

  Ablauf: Jan 15 12:00:00 2038 GMT
- **DST_ACES_CA_X6**
  Subjektname: /C=US/O=Digital Signature Trust/OU=DST ACES/CN=DST ACES CA X6

  Fingerabdruck: 40:54:DA:6F:1C:3F:40:74:AC:ED:0F:EC:CD:DB:79:D1:53:FB:90:1D

  Ausgabe: Nov 20 21:19:58 2003 GMT

  Ablauf: Nov 20 21:19:58 2017 GMT
- **Deutsche_Telekom_Root_CA_2**
  Subjektname: /C=DE/O=Deutsche Telekom AG/OU=T-TeleSec Trust Center/CN=Deutsche Telekom Root CA 2

  Fingerabdruck: 85:A4:08:C0:9C:19:3E:5D:51:58:7D:CD:D6:13:30:FD:8C:DE:37:BF

  Ausgabe: Jul 9 12:11:00 1999 GMT

  Ablauf: Jul 9 23:59:00 2019 GMT
- **TeliaSonera_Root_CA_v1**
  Subjektname: /O=TeliaSonera/CN=TeliaSonera Root CA v1

  Fingerabdruck: 43:13:BB:96:F1:D5:86:9B:C1:4E:6A:92:F6:CF:F6:34:69:87:82:37

  Ausgabe: Oct 18 12:00:50 2007 GMT

  Ablauf: Oct 18 12:00:50 2032 GMT
- **DST_Root_CA_X3**
  Subjektname: /O=Digital Signature Trust Co./CN=DST Root CA X3

  Fingerabdruck: DA:C9:02:4F:54:D8:F6:DF:94:93:5F:B1:73:26:38:CA:6A:D7:7C:13

  Ausgabe: Sep 30 21:12:19 2000 GMT

  Ablauf: Sep 30 14:01:15 2021 GMT
- **Comodo_Secure_Services_root**
  Subjektname: /C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=Secure Certificate Services

Fingerabdruck: 4A:65:D5:F4:1D:EF:39:B8:B8:90:4A:4A:D3:64:81:33:CF:C7:A1:D1

Ausgabe: Jan 1 00:00:00 2004 GMT

Ablauf: Dec 31 23:59:59 2028 GMT

- **TURKTRUST_Certificate_Services_Provider_Root_2007**
  Subjektname: /CN=TxC3x9CRKTRUST Elektronik Sertifika Hizmet SaxC4x9FlayxC4xB1cxC4xB1sxC4xB1/C=TR/L=Ankara/O=TxC3x9CRKTRUST Bilgi xC4xB0letixC5x9Fim ve BilixC5x9Fim GxC3xBCvenlixC4x9Fi Hizmetleri A.xC5x9E. (c) AralxC4xB1k 2007

  Fingerabdruck: F1:7F:6F:B6:31:DC:99:E3:A3:C8:7F:FE:1C:F1:81:10:88:D9:60:33

  Ausgabe: Dec 25 18:37:19 2007 GMT

  Ablauf: Dec 22 18:37:19 2017 GMT
- **Certplus_Class_2_Primary_CA**
  Subjektname: /C=FR/O=Certplus/CN=Class 2 Primary CA

  Fingerabdruck: 74:20:74:41:72:9C:DD:92:EC:79:31:D8:23:10:8D:C2:81:92:E2:BB

  Ausgabe: Jul 7 17:05:00 1999 GMT

  Ablauf: Jul 6 23:59:59 2019 GMT
- **IdenTrust_Public_Sector_Root_CA_1**
  Subjektname: /C=US/O=IdenTrust/CN=IdenTrust Public Sector Root CA 1

  Fingerabdruck: BA:29:41:60:77:98:3F:F4:F3:EF:F2:31:05:3B:2E:EA:6D:4D:45:FD

  Ausgabe: Jan 16 17:53:32 2014 GMT

  Ablauf: Jan 16 17:53:32 2034 GMT
- **EE_Certification_Centre_Root_CA**
  Subjektname: /C=EE/O=AS Sertifitseerimiskeskus/CN=EE Certification Centre Root CA/emailAddress=pki@sk.ee

  Fingerabdruck: C9:A8:B9:E7:55:80:5E:58:E3:53:77:A7:25:EB:AF:C3:7B:27:CC:D7

  Ausgabe: Oct 30 10:10:30 2010 GMT

  Ablauf: Dec 17 23:59:59 2030 GMT
- **Staat_der_Nederlanden_Root_CA**
  Subjektname: /C=NL/O=Staat der Nederlanden/CN=Staat der Nederlanden Root CA

  Fingerabdruck: 10:1D:FA:3F:D5:0B:CB:BB:9B:B5:60:0C:19:55:A4:1A:F4:73:3A:04

  Ausgabe: Dec 17 09:23:49 2002 GMT

  Ablauf: Dec 16 09:15:38 2015 GMT
- **S-TRUST_Universal_Root_CA**
  Subjektname: /C=DE/O=Deutscher Sparkassen Verlag GmbH/OU=S-TRUST Certification Services/CN=S-TRUST Universal Root CA

  Fingerabdruck: 1B:3D:11:14:EA:7A:0F:95:58:54:41:95:BF:6B:25:82:AB:40:CE:9A

  Ausgabe: Oct 22 00:00:00 2013 GMT

  Ablauf: Oct 21 23:59:59 2038 GMT

- **DigiCert_Global_Root_CA**
  Subjektname: /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root CA

  Fingerabdruck: A8:98:5D:3A:65:E5:E5:C4:B2:D7:D6:6D:40:C6:DD:2F:B1:9C:54:36

  Ausgabe: Nov 10 00:00:00 2006 GMT

  Ablauf: Nov 10 00:00:00 2031 GMT
- **DigiCert_Assured_ID_Root_CA**
  Subjektname: /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Assured ID Root CA

  Fingerabdruck: 05:63:B8:63:0D:62:D7:5A:BB:C8:AB:1E:4B:DF:B5:A8:99:B2:4D:43

  Ausgabe: Nov 10 00:00:00 2006 GMT

  Ablauf: Nov 10 00:00:00 2031 GMT
- **GlobalSign_ECC_Root_CA_-_R4**
  Subjektname: /OU=GlobalSign ECC Root CA - R4/O=GlobalSign/CN=GlobalSign

  Fingerabdruck: 69:69:56:2E:40:80:F4:24:A1:E7:19:9F:14:BA:F3:EE:58:AB:6A:BB

  Ausgabe: Nov 13 00:00:00 2012 GMT

  Ablauf: Jan 19 03:14:07 2038 GMT
- **AffirmTrust_Premium**
  Subjektname: /C=US/O=AffirmTrust/CN=AffirmTrust Premium

  Fingerabdruck: D8:A6:33:2C:E0:03:6F:B1:85:F6:63:4F:7D:6A:06:65:26:32:28:27

  Ausgabe: Jan 29 14:10:36 2010 GMT

  Ablauf: Dec 31 14:10:36 2040 GMT
- **USERTrust_RSA_Certification_Authority**
  Subjektname: /C=US/ST=New Jersey/L=Jersey City/O=The USERTRUST Network/CN=USERTrust RSA Certification Authority

  Fingerabdruck: 2B:8F:1B:57:33:0D:BB:A2:D0:7A:6C:51:F7:0E:E9:0D:DA:B9:AD:8E

  Ausgabe: Feb 1 00:00:00 2010 GMT

  Ablauf: Jan 18 23:59:59 2038 GMT
- **certSIGN_ROOT_CA**
  Subjektname: /C=RO/O=certSIGN/OU=certSIGN ROOT CA

  Fingerabdruck: FA:B7:EE:36:97:26:62:FB:2D:B0:2A:F6:BF:03:FD:E8:7C:4B:2F:9B

  Ausgabe: Jul 4 17:20:04 2006 GMT

  Ablauf: Jul 4 17:20:04 2031 GMT
- **ACCVRAIZ1**
  Subjektname: /CN=ACCVRAIZ1/OU=PKIACCV/O=ACCV/C=ES

  Fingerabdruck: 93:05:7A:88:15:C6:4F:CE:88:2F:FA:91:16:52:28:78:BC:53:64:17

  Ausgabe: May 5 09:37:37 2011 GMT

  Ablauf: Dec 31 09:37:37 2030 GMT

- **TÃœBÄ°TAK_UEKAE_KÃ¶k_Sertifika_Hizmet_SaÄŸlayÄ±cÄ±sÄ±_-_SÃ¼rÃ¼m_3**
  Subjektname: /C=TR/L=Gebze - Kocaeli/O=TxC3xBCrkiye Bilimsel ve Teknolojik AraxC5x9FtxC4xB1rma Kurumu - TxC3x9CBxC4xB0TAK/OU=Ulusal Elektronik ve Kriptoloji AraxC5x9FtxC4xB1rma EnstitxC3xBCsxC3xBC - UEKAE/OU=Kamu Sertifikasyon Merkezi/CN=TxC3x9CBxC4xB0TAK UEKAE KxC3xB6k Sertifika Hizmet SaxC4x9FlayxC4xB1cxC4xB1sxC4xB1 - SxC3xBCrxC3xBCm 3

  Fingerabdruck: 1B:4B:39:61:26:27:6B:64:91:A2:68:6D:D7:02:43:21:2D:1F:1D:96

  Ausgabe: Aug 24 11:37:07 2007 GMT

  Ablauf: Aug 21 11:37:07 2017 GMT
- **AddTrust_Qualified_Certificates_Root**
  Subjektname: /C=SE/O=AddTrust AB/OU=AddTrust TTP Network/CN=AddTrust Qualified CA Root

  Fingerabdruck: 4D:23:78:EC:91:95:39:B5:00:7F:75:8F:03:3B:21:1E:C5:4D:8B:CF

  Ausgabe: May 30 10:44:50 2000 GMT

  Ablauf: May 30 10:44:50 2020 GMT
- **AffirmTrust_Commercial**
  Subjektname: /C=US/O=AffirmTrust/CN=AffirmTrust Commercial

  Fingerabdruck: F9:B5:B6:32:45:5F:9C:BE:EC:57:5F:80:DC:E9:6E:2C:C7:B2:78:B7

  Ausgabe: Jan 29 14:06:06 2010 GMT

  Ablauf: Dec 31 14:06:06 2030 GMT
- **UTN_USERFirst_Hardware_Root_CA**
  Subjektname: /C=US/ST=UT/L=Salt Lake City/O=The USERTRUST Network/OU=http://www.usertrust.com/CN=UTN-USERFirst-Hardware

  Fingerabdruck: 04:83:ED:33:99:AC:36:08:05:87:22:ED:BC:5E:46:00:E3:BE:F9:D7

  Ausgabe: Jul 9 18:10:42 1999 GMT

  Ablauf: Jul 9 18:19:22 2019 GMT
- **Visa_eCommerce_Root**
  Subjektname: /C=US/O=VISA/OU=Visa International Service Association/CN=Visa eCommerce Root

  Fingerabdruck: 70:17:9B:86:8C:00:A4:FA:60:91:52:22:3F:9F:3E:32:BD:E0:05:62

  Ausgabe: Jun 26 02:18:36 2002 GMT

  Ablauf: Jun 24 00:16:12 2022 GMT
- **AddTrust_Public_Services_Root**
  Subjektname: /C=SE/O=AddTrust AB/OU=AddTrust TTP Network/CN=AddTrust Public CA Root

  Fingerabdruck: 2A:B6:28:48:5E:78:FB:F3:AD:9E:79:10:DD:6B:DF:99:72:2C:96:E5

  Ausgabe: May 30 10:41:50 2000 GMT

  Ablauf: May 30 10:41:50 2020 GMT
- **thawte_Primary_Root_CA**
  Subjektname: /C=US/O=thawte, Inc./OU=Certification Services Division/OU=(c) 2006 thawte, Inc. - For authorized use only/CN=thawte Primary Root CA

Fingerabdruck: 91:C6:D6:EE:3E:8A:C8:63:84:E5:48:C2:99:29:5C:75:6C:81:7B:81

Ausgabe: Nov 17 00:00:00 2006 GMT

Ablauf: Jul 16 23:59:59 2036 GMT

- **StartCom_Certification_Authority**
  Subjektname: /C=IL/O=StartCom Ltd./OU=Secure Digital Certificate Signing/CN=StartCom Certification Authority

  Fingerabdruck: 3E:2B:F7:F2:03:1B:96:F3:8C:E6:C4:D8:A8:5D:3E:2D:58:47:6A:0F

  Ausgabe: Sep 17 19:46:36 2006 GMT

  Ablauf: Sep 17 19:46:36 2036 GMT
- **StartCom_Certification_Authority_2**
  Subjektname: /C=IL/O=StartCom Ltd./OU=Secure Digital Certificate Signing/CN=StartCom Certification Authority

  Fingerabdruck: A3:F1:33:3F:E2:42:BF:CF:C5:D1:4E:8F:39:42:98:40:68:10:D1:A0

  Ausgabe: Sep 17 19:46:37 2006 GMT

  Ablauf: Sep 17 19:46:36 2036 GMT
- **Go_Daddy_Root_Certificate_Authority_-_G2**
  Subjektname: /C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com, Inc./CN=Go Daddy Root Certificate Authority - G2

  Fingerabdruck: 47:BE:AB:C9:22:EA:E8:0E:78:78:34:62:A7:9F:45:C2:54:FD:E6:8B

  Ausgabe: Sep 1 00:00:00 2009 GMT

  Ablauf: Dec 31 23:59:59 2037 GMT
- **DigiCert_Trusted_Root_G4**
  Subjektname: /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Trusted Root G4

  Fingerabdruck: DD:FB:16:CD:49:31:C9:73:A2:03:7D:3F:C8:3A:4D:7D:77:5D:05:E4

  Ausgabe: Aug 1 12:00:00 2013 GMT

  Ablauf: Jan 15 12:00:00 2038 GMT
- **Equifax_Secure_eBusiness_CA_1**
  Subjektname: /C=US/O=Equifax Secure Inc./CN=Equifax Secure eBusiness CA-1

  Fingerabdruck: DA:40:18:8B:91:89:A3:ED:EE:AE:DA:97:FE:2F:9D:F5:B7:D1:8A:41

  Ausgabe: Jun 21 04:00:00 1999 GMT

  Ablauf: Jun 21 04:00:00 2020 GMT
- **China_Internet_Network_Information_Center_EV_Certificates_Root**
  Subjektname: /C=CN/O=China Internet Network Information Center/CN=China Internet Network Information Center EV Certificates Root

  Fingerabdruck: 4F:99:AA:93:FB:2B:D1:37:26:A1:99:4A:CE:7F:F0:05:F2:93:5D:1E

  Ausgabe: Aug 31 07:11:25 2010 GMT

  Ablauf: Aug 31 07:11:25 2030 GMT

- **GeoTrust_Universal_CA_2**
  Subjektname: /C=US/O=GeoTrust Inc./CN=GeoTrust Universal CA 2

  Fingerabdruck: 37:9A:19:7B:41:85:45:35:0C:A6:03:69:F3:3C:2E:AF:47:4F:20:79

  Ausgabe: Mar 4 05:00:00 2004 GMT

  Ablauf: Mar 4 05:00:00 2029 GMT
- **Certinomis_-_AutoritÃ©_Racine**
  Subjektname: /C=FR/O=Certinomis/OU=0002 433998903/CN=Certinomis - AutoritxC3xA9 Racine

  Fingerabdruck: 2E:14:DA:EC:28:F0:FA:1E:8E:38:9A:4E:AB:EB:26:C0:0A:D3:83:C3

  Ausgabe: Sep 17 08:28:59 2008 GMT

  Ablauf: Sep 17 08:28:59 2028 GMT
- **NetLock_Notary_=Class_A=_Root**
  Subjektname: /C=HU/ST=Hungary/L=Budapest/O=NetLock Halozatbiztonsagi Kft./OU=Tanusitvanykiadok/CN=NetLock Kozjegyzoi (Class A) Tanusitvanykiado

  Fingerabdruck: AC:ED:5F:65:53:FD:25:CE:01:5F:1F:7A:48:3B:6A:74:9F:61:78:C6

  Ausgabe: Feb 24 23:14:47 1999 GMT

  Ablauf: Feb 19 23:14:47 2019 GMT
- **WoSign_China**
  Subjektname: /C=CN/O=WoSign CA Limited/CN=CA xE6xB2x83xE9x80x9AxE6xA0xB9xE8xAFx81xE4xB9xA6

  Fingerabdruck: 16:32:47:8D:89:F9:21:3A:92:00:85:63:F5:A4:A7:D3:12:40:8A:D6

  Ausgabe: Aug 8 01:00:01 2009 GMT

  Ablauf: Aug 8 01:00:01 2039 GMT
- **AffirmTrust_Networking**
  Subjektname: /C=US/O=AffirmTrust/CN=AffirmTrust Networking

  Fingerabdruck: 29:36:21:02:8B:20:ED:02:F5:66:C5:32:D1:D6:ED:90:9F:45:00:2F

  Ausgabe: Jan 29 14:08:24 2010 GMT

  Ablauf: Dec 31 14:08:24 2030 GMT
- **D-TRUST_Root_Class_3_CA_2_2009**
  Subjektname: /C=DE/O=D-Trust GmbH/CN=D-TRUST Root Class 3 CA 2 2009

  Fingerabdruck: 58:E8:AB:B0:36:15:33:FB:80:F7:9B:1B:6D:29:D3:FF:8D:5F:00:F0

  Ausgabe: Nov 5 08:35:58 2009 GMT

  Ablauf: Nov 5 08:35:58 2029 GMT
- **COMODO_Certification_Authority**
  Subjektname: /C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO Certification Authority

  Fingerabdruck: 66:31:BF:9E:F7:4F:9E:B6:C9:D5:A6:0C:BA:6A:BE:D1:F7:BD:EF:7B

  Ausgabe: Dec 1 00:00:00 2006 GMT

Ablauf: Dec 31 23:59:59 2029 GMT

- **CA_Disig_Root_R1**
  Subjektname: /C=SK/L=Bratislava/O=Disig a.s./CN=CA Disig Root R1

  Fingerabdruck: 8E:1C:74:F8:A6:20:B9:E5:8A:F4:61:FA:EC:2B:47:56:51:1A:52:C6

  Ausgabe: Jul 19 09:06:56 2012 GMT

  Ablauf: Jul 19 09:06:56 2042 GMT
- **thawte_Primary_Root_CA_-_G3**
  Subjektname: /C=US/O=thawte, Inc./OU=Certification Services Division/OU=(c) 2008 thawte, Inc. - For authorized use only/CN=thawte Primary Root CA - G3

  Fingerabdruck: F1:8B:53:8D:1B:E9:03:B6:A6:F0:56:43:5B:17:15:89:CA:F3:6B:F2

  Ausgabe: Apr 2 00:00:00 2008 GMT

  Ablauf: Dec 1 23:59:59 2037 GMT
- **AddTrust_External_Root**
  Subjektname: /C=SE/O=AddTrust AB/OU=AddTrust External TTP Network/CN=AddTrust External CA Root

  Fingerabdruck: 02:FA:F3:E2:91:43:54:68:60:78:57:69:4D:F5:E4:5B:68:85:18:68

  Ausgabe: May 30 10:48:38 2000 GMT

  Ablauf: May 30 10:48:38 2020 GMT
- **ACEDICOM_Root**
  Subjektname: /CN=ACEDICOM Root/OU=PKI/O=EDICOM/C=ES

  Fingerabdruck: E0:B4:32:2E:B2:F6:A5:68:B6:54:53:84:48:18:4A:50:36:87:43:84

  Ausgabe: Apr 18 16:24:22 2008 GMT

  Ablauf: Apr 13 16:24:22 2028 GMT
- **VeriSign_Class_3_Public_Primary_Certification_Authority_-_G5**
  Subjektname: /C=US/O=VeriSign, Inc./OU=VeriSign Trust Network/OU=(c) 2006 VeriSign, Inc. - For authorized use only/CN=VeriSign Class 3 Public Primary Certification Authority - G5

  Fingerabdruck: 4E:B6:D5:78:49:9B:1C:CF:5F:58:1E:AD:56:BE:3D:9B:67:44:A5:E5

  Ausgabe: Nov 8 00:00:00 2006 GMT

  Ablauf: Jul 16 23:59:59 2036 GMT
- **IdenTrust_Commercial_Root_CA_1**
  Subjektname: /C=US/O=IdenTrust/CN=IdenTrust Commercial Root CA 1

  Fingerabdruck: DF:71:7E:AA:4A:D9:4E:C9:55:84:99:60:2D:48:DE:5F:BC:F0:3A:25

  Ausgabe: Jan 16 18:12:23 2014 GMT

  Ablauf: Jan 16 18:12:23 2034 GMT
- **Juur-SK**
  Subjektname: /emailAddress=pki@sk.ee/C=EE/O=AS Sertifitseerimiskeskus/CN=Juur-SK

  Fingerabdruck: 40:9D:4B:D9:17:B5:5C:27:B6:9B:64:CB:98:22:44:0D:CD:09:B8:89

  Ausgabe: Aug 30 14:23:01 2001 GMT

Ablauf: Aug 26 14:23:01 2016 GMT

- **GlobalSign_Root_CA_-_R3**
  Subjektname: /OU=GlobalSign Root CA - R3/O=GlobalSign/CN=GlobalSign

  Fingerabdruck: D6:9B:56:11:48:F0:1C:77:C5:45:78:C1:09:26:DF:5B:85:69:76:AD

  Ausgabe: Mar 18 10:00:00 2009 GMT

  Ablauf: Mar 18 10:00:00 2029 GMT
- **Security_Communication_EV_RootCA1**
  Subjektname: /C=JP/O=SECOM Trust Systems CO.,LTD./OU=Security Communication EV RootCA1

  Fingerabdruck: FE:B8:C4:32:DC:F9:76:9A:CE:AE:3D:D8:90:8F:FD:28:86:65:64:7D

  Ausgabe: Jun 6 02:12:32 2007 GMT

  Ablauf: Jun 6 02:12:32 2037 GMT
- **Microsec_e-Szigno_Root_CA_2009**
  Subjektname: /C=HU/L=Budapest/O=Microsec Ltd./CN=Microsec e-Szigno Root CA 2009/emailAddress=info@e-szigno.hu

  Fingerabdruck: 89:DF:74:FE:5C:F4:0F:4A:80:F9:E3:37:7D:54:DA:91:E1:01:31:8E

  Ausgabe: Jun 16 11:30:18 2009 GMT

  Ablauf: Dec 30 11:30:18 2029 GMT
- **QuoVadis_Root_CA_3**
  Subjektname: /C=BM/O=QuoVadis Limited/CN=QuoVadis Root CA 3

  Fingerabdruck: 1F:49:14:F7:D8:74:95:1D:DD:AE:02:C0:BE:FD:3A:2D:82:75:51:85

  Ausgabe: Nov 24 19:11:23 2006 GMT

  Ablauf: Nov 24 19:06:44 2031 GMT
- **COMODO_RSA_Certification_Authority**
  Subjektname: /C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO RSA Certification Authority

  Fingerabdruck: AF:E5:D2:44:A8:D1:19:42:30:FF:47:9F:E2:F8:97:BB:CD:7A:8C:B4

  Ausgabe: Jan 19 00:00:00 2010 GMT

  Ablauf: Jan 18 23:59:59 2038 GMT
- **TC_TrustCenter_Class_3_CA_II**
  Subjektname: /C=DE/O=TC TrustCenter GmbH/OU=TC TrustCenter Class 3 CA/CN=TC TrustCenter Class 3 CA II

  Fingerabdruck: 80:25:EF:F4:6E:70:C8:D4:72:24:65:84:FE:40:3B:8A:8D:6A:DB:F5

  Ausgabe: Jan 12 14:41:57 2006 GMT

  Ablauf: Dec 31 22:59:59 2025 GMT
- **T-TeleSec_GlobalRoot_Class_2**
  Subjektname: /C=DE/O=T-Systems Enterprise Services GmbH/OU=T-Systems Trust Center/CN=T-TeleSec GlobalRoot Class 2

Fingerabdruck: 59:0D:2D:7D:88:4F:40:2E:61:7E:A5:62:32:17:65:CF:17:D8:94:E9

Ausgabe: Oct 1 10:40:14 2008 GMT

Ablauf: Oct 1 23:59:59 2033 GMT

- **CNNIC_ROOT**
  Subjektname: /C=CN/O=CNNIC/CN=CNNIC ROOT

  Fingerabdruck: 8B:AF:4C:9B:1D:F0:2A:92:F7:DA:12:8E:B9:1B:AC:F4:98:60:4B:6F

  Ausgabe: Apr 16 07:09:14 2007 GMT

  Ablauf: Apr 16 07:09:14 2027 GMT
- **COMODO_ECC_Certification_Authority**
  Subjektname: /C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO ECC Certification Authority

  Fingerabdruck: 9F:74:4E:9F:2B:4D:BA:EC:0F:31:2C:50:B6:56:3B:8E:2D:93:C3:11

  Ausgabe: Mar 6 00:00:00 2008 GMT

  Ablauf: Jan 18 23:59:59 2038 GMT
- **Trustis_FPS_Root_CA**
  Subjektname: /C=GB/O=Trustis Limited/OU=Trustis FPS Root CA

  Fingerabdruck: 3B:C0:38:0B:33:C3:F6:A6:0C:86:15:22:93:D9:DF:F5:4B:81:C0:04

  Ausgabe: Dec 23 12:14:06 2003 GMT

  Ablauf: Jan 21 11:36:54 2024 GMT
- **Starfield_Services_Root_Certificate_Authority_-_G2**
  Subjektname: /C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./CN=Starfield Services Root Certificate Authority - G2

  Fingerabdruck: 92:5A:8F:8D:2C:6D:04:E0:66:5F:59:6A:FF:22:D8:63:E8:25:6F:3F

  Ausgabe: Sep 1 00:00:00 2009 GMT

  Ablauf: Dec 31 23:59:59 2037 GMT
- **Hellenic_Academic_and_Research_Institutions_RootCA_2011**
  Subjektname: /C=GR/O=Hellenic Academic and Research Institutions Cert. Authority/CN=Hellenic Academic and Research Institutions RootCA 2011

  Fingerabdruck: FE:45:65:9B:79:03:5B:98:A1:61:B5:51:2E:AC:DA:58:09:48:22:4D

  Ausgabe: Dec 6 13:49:52 2011 GMT

  Ablauf: Dec 1 13:49:52 2031 GMT
- **RSA_Security_2048_v3**
  Subjektname: /O=RSA Security Inc/OU=RSA Security 2048 V3

  Fingerabdruck: 25:01:90:19:CF:FB:D9:99:1C:B7:68:25:74:8D:94:5F:30:93:95:42

  Ausgabe: Feb 22 20:39:23 2001 GMT

  Ablauf: Feb 22 20:39:23 2026 GMT

- **DigiCert_Assured_ID_Root_G3**
  Subjektname: /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Assured ID Root G3

  Fingerabdruck: F5:17:A2:4F:9A:48:C6:C9:F8:A2:00:26:9F:DC:0F:48:2C:AB:30:89

  Ausgabe: Aug 1 12:00:00 2013 GMT

  Ablauf: Jan 15 12:00:00 2038 GMT
- **NetLock_Arany_=Class_Gold=_FÅ‘tanÃ°sÃtvÃ¡ny**
  Subjektname: /C=HU/L=Budapest/O=NetLock Kft./OU=TanxC3xBAsxC3xADtvxC3xA1nykiadxC3xB3k (Certification Services)/CN=NetLock Arany (Class Gold) FxC5x91tanxC3xBAsxC3xADtvxC3xA1ny

  Fingerabdruck: 06:08:3F:59:3F:15:A1:04:A0:69:A4:6B:A9:03:D0:06:B7:97:09:91

  Ausgabe: Dec 11 15:08:21 2008 GMT

  Ablauf: Dec 6 15:08:21 2028 GMT
- **Sonera_Class_1_Root_CA**
  Subjektname: /C=FI/O=Sonera/CN=Sonera Class1 CA

  Fingerabdruck: 07:47:22:01:99:CE:74:B9:7C:B0:3D:79:B2:64:A2:C8:55:E9:33:FF

  Ausgabe: Apr 6 10:49:13 2001 GMT

  Ablauf: Apr 6 10:49:13 2021 GMT
- **GeoTrust_Primary_Certification_Authority_-_G2**
  Subjektname: /C=US/O=GeoTrust Inc./OU=(c) 2007 GeoTrust Inc. - For authorized use only/CN=GeoTrust Primary Certification Authority - G2

  Fingerabdruck: 8D:17:84:D5:37:F3:03:7D:EC:70:FE:57:8B:51:9A:99:E6:10:D7:B0

  Ausgabe: Nov 5 00:00:00 2007 GMT

  Ablauf: Jan 18 23:59:59 2038 GMT
- **Entrust_Root_Certification_Authority_-_EC1**
  Subjektname: /C=US/O=Entrust, Inc./OU=See www.entrust.net/legal-terms/OU=(c) 2012 Entrust, Inc. - for authorized use only/CN=Entrust Root Certification Authority - EC1

  Fingerabdruck: 20:D8:06:40:DF:9B:25:F5:12:25:3A:11:EA:F7:59:8A:EB:14:B5:47

  Ausgabe: Dec 18 15:25:36 2012 GMT

  Ausgabe: Dec 18 15:55:36 2037 GMT
- **Starfield_Class_2_CA**
  Subjektname: /C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification Authority

  Fingerabdruck: AD:7E:1C:28:B0:64:EF:8F:60:03:40:20:14:C3:D0:E3:37:0E:B5:8A

  Ausgabe: Jun 29 17:39:16 2004 GMT

  Ablauf: Jun 29 17:39:16 2034 GMT
- **Staat_der_Nederlanden_Root_CA_-_G2**
  Subjektname: /C=NL/O=Staat der Nederlanden/CN=Staat der Nederlanden Root CA - G2

  Fingerabdruck: 59:AF:82:79:91:86:C7:B4:75:07:CB:CF:03:57:46:EB:04:DD:B7:16

Ausgabe: Mar 26 11:18:17 2008 GMT

Ablauf: Mar 25 11:03:10 2020 GMT

- **Entrust_Root_Certification_Authority_-_G2**
  Subjektname: /C=US/O=Entrust, Inc./OU=See www.entrust.net/legal-terms/OU=(c) 2009 Entrust, Inc. - for authorized use only/CN=Entrust Root Certification Authority - G2

  Fingerabdruck: 8C:F4:27:FD:79:0C:3A:D1:66:06:8D:E8:1E:57:EF:BB:93:22:72:D4

  Ausgabe: Jul 7 17:25:54 2009 GMT

  Ablauf: Dec 7 17:55:54 2030 GMT
- **Camerfirma_Global_Chambersign_Root**
  Subjektname: /C=EU/O=AC Camerfirma SA CIF A82743287/OU=http://www.chambersign.org/CN=Global Chambersign Root

  Fingerabdruck: 33:9B:6B:14:50:24:9B:55:7A:01:87:72:84:D9:E0:2F:C3:D2:D8:E9

  Ausgabe: Sep 30 16:14:18 2003 GMT

  Ablauf: Sep 30 16:14:18 2037 GMT
- **S-TRUST_Authentication_and_Encryption_Root_CA_2005_PN**
  Subjektname: /C=DE/ST=Baden-Wuerttemberg (BW)/L=Stuttgart/O=Deutscher Sparkassen Verlag GmbH/CN=S-TRUST Authentication and Encryption Root CA 2005:PN

  Fingerabdruck: BE:B5:A9:95:74:6B:9E:DF:73:8B:56:E6:DF:43:7A:77:BE:10:6B:81

  Ausgabe: Jun 22 00:00:00 2005 GMT

  Ablauf: Jun 21 23:59:59 2030 GMT
- **NetLock_Business_=Class_B=_Root**
  Subjektname: /C=HU/L=Budapest/O=NetLock Halozatbiztonsagi Kft./OU=Tanusitvanykiadok/CN=NetLock Uzleti (Class B) Tanusitvanykiado

  Fingerabdruck: 87:9F:4B:EE:05:DF:98:58:3B:E3:60:D6:33:E7:0D:3F:FE:98:71:AF

  Ausgabe: Feb 25 14:10:22 1999 GMT

  Ablauf: Feb 20 14:10:22 2019 GMT
- **Baltimore_CyberTrust_Root**
  Subjektname: /C=IE/O=Baltimore/OU=CyberTrust/CN=Baltimore CyberTrust Root

  Fingerabdruck: D4:DE:20:D0:5E:66:FC:53:FE:1A:50:88:2C:78:DB:28:52:CA:E4:74

  Ausgabe: May 12 18:46:00 2000 GMT

  Ablauf: May 12 23:59:00 2025 GMT
- **Verisign_Class_1_Public_Primary_Certification_Authority_-_G3**
  Subjektname: /C=US/O=VeriSign, Inc./OU=VeriSign Trust Network/OU=(c) 1999 VeriSign, Inc. - For authorized use only/CN=VeriSign Class 1 Public Primary Certification Authority - G3

  Fingerabdruck: 20:42:85:DC:F7:EB:76:41:95:57:8E:13:6B:D4:B7:D1:E9:8E:46:A5

  Ausgabe: Oct 1 00:00:00 1999 GMT

  Ablauf: Jul 16 23:59:59 2036 GMT

- **ApplicationCA_-_Japanese_Government**
  Subjektname: /C=JP/O=Japanese Government/OU=ApplicationCA

  Fingerabdruck: 7F:8A:B0:CF:D0:51:87:6A:66:F3:36:0F:47:C8:8D:8C:D3:35:FC:74

  Ausgabe: Dec 12 15:00:00 2007 GMT

  Ablauf: Dec 12 15:00:00 2017 GMT
- **TÃœRKTRUST_Elektronik_Sertifika_Hizmet_SaÄŸlayÄ±cÄ±sÄ±_H6**
  Subjektname: /C=TR/L=Ankara/O=TxC3x9CRKTRUST Bilgi xC4xB0letixC5x9Fim ve BilixC5x9Fim GxC3xBCvenlixC4x9Fi Hizmetleri A.xC5x9E./CN=TxC3x9CRKTRUST Elektronik Sertifika Hizmet SaxC4x9FlayxC4xB1cxC4xB1sxC4xB1 H6

  Fingerabdruck: 8A:5C:8C:EE:A5:03:E6:05:56:BA:D8:1B:D4:F6:C9:B0:ED:E5:2F:E0

  Ausgabe: Dec 18 09:04:10 2013 GMT

  Ablauf: Dec 16 09:04:10 2023 GMT
- **CA_Disig_Root_R2**
  Subjektname: /C=SK/L=Bratislava/O=Disig a.s./CN=CA Disig Root R2

  Fingerabdruck: B5:61:EB:EA:A4:DE:E4:25:4B:69:1A:98:A5:57:47:C2:34:C7:D9:71

  Ausgabe: Jul 19 09:15:30 2012 GMT

  Ablauf: Jul 19 09:15:30 2042 GMT
- **Chambers_of_Commerce_Root_-_2008**
  Subjektname: /C=EU/L=Madrid (see current address at www.camerfirma.com/address)/serialNumber=A82743287/O=AC Camerfirma S.A./CN=Chambers of Commerce Root - 2008

  Fingerabdruck: 78:6A:74:AC:76:AB:14:7F:9C:6A:30:50:BA:9E:A8:7E:FE:9A:CE:3C

  Ausgabe: Aug 1 12:29:50 2008 GMT

  Ablauf: Jul 31 12:29:50 2038 GMT
- **DigiCert_Assured_ID_Root_G2**
  Subjektname: /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Assured ID Root G2

  Fingerabdruck: A1:4B:48:D9:43:EE:0A:0E:40:90:4F:3C:E0:A4:C0:91:93:51:5D:3F

  Ausgabe: Aug 1 12:00:00 2013 GMT

  Ablauf: Jan 15 12:00:00 2038 GMT
- **E-Tugra_Certification_Authority**
  Subjektname: /C=TR/L=Ankara/O=E-TuxC4x9Fra EBG BilixC5x9Fim Teknolojileri ve Hizmetleri A.xC5x9E./OU=E-Tugra Sertifikasyon Merkezi/CN=E-Tugra Certification Authority

  Fingerabdruck: 51:C6:E7:08:49:06:6E:F3:92:D4:5C:A0:0D:6D:A3:62:8F:C3:52:39

  Ausgabe: Mar 5 12:09:48 2013 GMT

  Ablauf: Mar 3 12:09:48 2023 GMT
- **thawte_Primary_Root_CA_-_G2**
  Subjektname: /C=US/O=thawte, Inc./OU=(c) 2007 thawte, Inc. - For authorized use only/CN=thawte Primary Root CA - G2

Fingerabdruck: AA:DB:BC:22:23:8F:C4:01:A1:27:BB:38:DD:F4:1D:DB:08:9E:F0:12

Ausgabe: Nov 5 00:00:00 2007 GMT

Ablauf: Jan 18 23:59:59 2038 GMT

- **WoSign**
  Subjektname: /C=CN/O=WoSign CA Limited/CN=Certification Authority of WoSign

  Fingerabdruck: B9:42:94:BF:91:EA:8F:B6:4B:E6:10:97:C7:FB:00:13:59:B6:76:CB

  Ausgabe: Aug 8 01:00:01 2009 GMT

  Ablauf: Aug 8 01:00:01 2039 GMT
- **Equifax_Secure_Global_eBusiness_CA**
  Subjektname: /C=US/O=Equifax Secure Inc./CN=Equifax Secure Global eBusiness CA-1

  Fingerabdruck: 7E:78:4A:10:1C:82:65:CC:2D:E1:F1:6D:47:B4:40:CA:D9:0A:19:45

  Ausgabe: Jun 21 04:00:00 1999 GMT

  Ablauf: Jun 21 04:00:00 2020 GMT
- **Actalis_Authentication_Root_CA**
  Subjektname: /C=IT/L=Milan/O=Actalis S.p.A./03358520967/CN=Actalis Authentication Root CA

  Fingerabdruck: F3:73:B3:87:06:5A:28:84:8A:F2:F3:4A:CE:19:2B:DD:C7:8E:9C:AC

  Ausgabe: Sep 22 11:22:02 2011 GMT

  Ablauf: Sep 22 11:22:02 2030 GMT
- **Camerfirma_Chambers_of_Commerce_Root**
  Subjektname: /C=EU/O=AC Camerfirma SA CIF A82743287/OU=http://www.chambersign.org/CN=Chambers of Commerce Root

  Fingerabdruck: 6E:3A:55:A4:19:0C:19:5C:93:84:3C:C0:DB:72:2E:31:30:61:F0:B1

  Ausgabe: Sep 30 16:13:43 2003 GMT

  Ablauf: Sep 30 16:13:44 2037 GMT
- **QuoVadis_Root_CA_1_G3**
  Subjektname: /C=BM/O=QuoVadis Limited/CN=QuoVadis Root CA 1 G3

  Fingerabdruck: 1B:8E:EA:57:96:29:1A:C9:39:EA:B8:0A:81:1A:73:73:C0:93:79:67

  Ausgabe: Jan 12 17:27:44 2012 GMT

  Ablauf: Jan 12 17:27:44 2042 GMT
- **Certum_Trusted_Network_CA**
  Subjektname: /C=PL/O=Unizeto Technologies S.A./OU=Certum Certification Authority/CN=Certum Trusted Network CA

  Fingerabdruck: 07:E0:32:E0:20:B7:2C:3F:19:2F:06:28:A2:59:3A:19:A7:0F:06:9E

  Ausgabe: Oct 22 12:07:37 2008 GMT

  Ablauf: Dec 31 12:07:37 2029 GMT
- **D-TRUST_Root_Class_3_CA_2_EV_2009**
  Subjektname: /C=DE/O=D-Trust GmbH/CN=D-TRUST Root Class 3 CA 2 EV 2009

Fingerabdruck: 96:C9:1B:0B:95:B4:10:98:42:FA:D0:D8:22:79:FE:60:FA:B9:16:83

Ausgabe: Nov 5 08:50:46 2009 GMT

Ablauf: Nov 5 08:50:46 2029 GMT

- **NetLock_Qualified_=Class_QA=_Root**
  Subjektname: /C=HU/L=Budapest/O=NetLock Halozatbiztonsagi Kft./OU=Tanusitvanykiadok/CN=NetLock Minositett Kozjegyzoi (Class QA) Tanusitvanykiado/emailAddress=info@netlock.hu

  Fingerabdruck: 01:68:97:E1:A0:B8:F2:C3:B1:34:66:5C:20:A7:27:B7:A1:58:E2:8F

  Ausgabe: Mar 30 01:47:11 2003 GMT

  Ablauf: Dec 15 01:47:11 2022 GMT
- **StartCom_Certification_Authority_G2**
  Subjektname: /C=IL/O=StartCom Ltd./CN=StartCom Certification Authority G2

  Fingerabdruck: 31:F1:FD:68:22:63:20:EE:C6:3B:3F:9D:EA:4A:3E:53:7C:7C:39:17

  Ausgabe: Jan 1 01:00:01 2010 GMT

  Ablauf: Dec 31 23:59:01 2039 GMT
- **Buypass_Class_2_CA_1**
  Subjektname: /C=NO/O=Buypass AS-983163327/CN=Buypass Class 2 CA 1

  Fingerabdruck: A0:A1:AB:90:C9:FC:84:7B:3B:12:61:E8:97:7D:5F:D3:22:61:D3:CC

  Ausgabe: Oct 13 10:25:09 2006 GMT

  Ablauf: Oct 13 10:25:09 2016 GMT
- **CA_WoSign_ECC_Root**
  Subjektname: /C=CN/O=WoSign CA Limited/CN=CA WoSign ECC Root

  Fingerabdruck: D2:7A:D2:BE:ED:94:C0:A1:3C:C7:25:21:EA:5D:71:BE:81:19:F3:2B

  Ausgabe: Nov 8 00:58:58 2014 GMT

  Ablauf: Nov 8 00:58:58 2044 GMT
- **XRamp_Global_CA_Root**
  Subjektname: /C=US/OU=www.xrampsecurity.com/O=XRamp Security Services Inc/CN=XRamp Global Certification Authority

  Fingerabdruck: B8:01:86:D1:EB:9C:86:A5:41:04:CF:30:54:F3:4C:52:B7:E5:58:C6

  Ausgabe: Nov 1 17:14:04 2004 GMT

  Ablauf: Jan 1 05:37:19 2035 GMT
- **Swisscom_Root_CA_2**
  Subjektname: /C=ch/O=Swisscom/OU=Digital Certificate Services/CN=Swisscom Root CA 2

  Fingerabdruck: 77:47:4F:C6:30:E4:0F:4C:47:64:3F:84:BA:B8:C6:95:4A:8A:41:EC

  Ausgabe: Jun 24 08:38:14 2011 GMT

  Ablauf: Jun 25 07:38:14 2031 GMT
- **Verisign_Class_3_Public_Primary_Certification_Authority_2**
  Subjektname: /C=US/O=VeriSign, Inc./OU=Class 3 Public Primary Certification Authority

Fingerabdruck: A1:DB:63:93:91:6F:17:E4:18:55:09:40:04:15:C7:02:40:B0:AE:6B

Ausgabe: Jan 29 00:00:00 1996 GMT

Ablauf: Aug 2 23:59:59 2028 GMT

- **TWCA_Root_Certification_Authority**
  Subjektname: /C=TW/O=TAIWAN-CA/OU=Root CA/CN=TWCA Root Certification Authority

  Fingerabdruck: CF:9E:87:6D:D3:EB:FC:42:26:97:A3:B5:A3:7A:A0:76:A9:06:23:48

  Ausgabe: Aug 28 07:24:33 2008 GMT

  Ablauf: Dec 31 15:59:59 2030 GMT
- **GeoTrust_Universal_CA**
  Subjektname: /C=US/O=GeoTrust Inc./CN=GeoTrust Universal CA

  Fingerabdruck: E6:21:F3:35:43:79:05:9A:4B:68:30:9D:8A:2F:74:22:15:87:EC:79

  Ausgabe: Mar 4 05:00:00 2004 GMT

  Ablauf: Mar 4 05:00:00 2029 GMT
- **VeriSign_Universal_Root_Certification_Authority**
  Subjektname: /C=US/O=VeriSign, Inc./OU=VeriSign Trust Network/OU=(c) 2008 VeriSign, Inc. - For authorized use only/CN=VeriSign Universal Root Certification Authority

  Fingerabdruck: 36:79:CA:35:66:87:72:30:4D:30:A5:FB:87:3B:0F:A7:7B:B7:0D:54

  Ausgabe: Apr 2 00:00:00 2008 GMT

  Ablauf: Dec 1 23:59:59 2037 GMT
- **Verisign_Class_3_Public_Primary_Certification_Authority_-_G2**
  Subjektname: /C=US/O=VeriSign, Inc./OU=Class 3 Public Primary Certification Authority - G2/OU=(c) 1998 VeriSign, Inc. - For authorized use only/OU=VeriSign Trust Network

  Fingerabdruck: 85:37:1C:A6:E5:50:14:3D:CE:28:03:47:1B:DE:3A:09:E8:F8:77:0F

  Ausgabe: May 18 00:00:00 1998 GMT

  Ablauf: Aug 1 23:59:59 2028 GMT
- **Buypass_Class_3_Root_CA**
  Subjektname: /C=NO/O=Buypass AS-983163327/CN=Buypass Class 3 Root CA

  Fingerabdruck: DA:FA:F7:FA:66:84:EC:06:8F:14:50:BD:C7:C2:81:A5:BC:A9:64:57

  Ausgabe: Oct 26 08:28:58 2010 GMT

  Ablauf: Oct 26 08:28:58 2040 GMT
- **GlobalSign_Root_CA**
  Subjektname: /C=BE/O=GlobalSign nv-sa/OU=Root CA/CN=GlobalSign Root CA

  Fingerabdruck: B1:BC:96:8B:D4:F4:9D:62:2A:A8:9A:81:F2:15:01:52:A4:1D:82:9C

  Ausgabe: Sep 1 12:00:00 1998 GMT

  Ablauf: Jan 28 12:00:00 2028 GMT

- **Verisign_Class_2_Public_Primary_Certification_Authority_-_G3**
  Subjektname: /C=US/O=VeriSign, Inc./OU=VeriSign Trust Network/OU=(c) 1999 VeriSign, Inc. - For authorized use only/CN=VeriSign Class 2 Public Primary Certification Authority - G3

  Fingerabdruck: 61:EF:43:D7:7F:CA:D4:61:51:BC:98:E0:C3:59:12:AF:9F:EB:63:11

  Ausgabe: Oct 1 00:00:00 1999 GMT

  Ablauf: Jul 16 23:59:59 2036 GMT
- **PSCProcert**
  Subjektname: /emailAddress=contacto@procert.net.ve/L=Chacao/ST=Miranda/OU=Proveedor de Certificados PROCERT/O=Sistema Nacional de Certificacion Electronica/C=VE/CN=PSCProcert

  Fingerabdruck: 70:C1:8D:74:B4:28:81:0A:E4:FD:A5:75:D7:01:9F:99:B0:3D:50:74

  Ausgabe: Dec 28 16:51:00 2010 GMT

  Ablauf: Dec 25 23:59:59 2020 GMT
- **QuoVadis_Root_CA_2**
  Subjektname: /C=BM/O=QuoVadis Limited/CN=QuoVadis Root CA 2

  Fingerabdruck: CA:3A:FB:CF:12:40:36:4B:44:B2:16:20:88:80:48:39:19:93:7C:F7

  Ausgabe: Nov 24 18:27:00 2006 GMT

  Ablauf: Nov 24 18:23:33 2031 GMT
- **T-TeleSec_GlobalRoot_Class_3**
  Subjektname: /C=DE/O=T-Systems Enterprise Services GmbH/OU=T-Systems Trust Center/CN=T-TeleSec GlobalRoot Class 3

  Fingerabdruck: 55:A6:72:3E:CB:F2:EC:CD:C3:23:74:70:19:9D:2A:BE:11:E3:81:D1

  Ausgabe: Oct 1 10:29:56 2008 GMT

  Ablauf: Oct 1 23:59:59 2033 GMT
- **SwissSign_Platinum_CA_-_G2**
  Subjektname: /C=CH/O=SwissSign AG/CN=SwissSign Platinum CA - G2

  Fingerabdruck: 56:E0:FA:C0:3B:8F:18:23:55:18:E5:D3:11:CA:E8:C2:43:31:AB:66

  Ausgabe: Oct 25 08:36:00 2006 GMT

  Ablauf: Oct 25 08:36:00 2036 GMT
- **Certum_Root_CA**
  Subjektname: /C=PL/O=Unizeto Sp. z o.o./CN=Certum CA

  Fingerabdruck: 62:52:DC:40:F7:11:43:A2:2F:DE:9E:F7:34:8E:06:42:51:B1:81:18

  Ausgabe: Jun 11 10:46:39 2002 GMT

  Ablauf: Jun 11 10:46:39 2027 GMT
- **EBG_Elektronik_Sertifika_Hizmet_SaÄŸlayÄ±cÄ±sÄ±**
  Subjektname: /CN=EBG Elektronik Sertifika Hizmet SaxC4x9FlayxC4xB1cxC4xB1sxC4xB1/O=EBG BilixC5x9Fim Teknolojileri ve Hizmetleri A.xC5x9E./C=TR

  Fingerabdruck: 8C:96:BA:EB:DD:2B:07:07:48:EE:30:32:66:A0:F3:98:6E:7C:AE:58

Ausgabe: Aug 17 00:21:09 2006 GMT

Ablauf: Aug 14 00:31:09 2016 GMT

- **Certigna**
  Subjektname: /C=FR/O=Dhimyotis/CN=Certigna

  Fingerabdruck: B1:2E:13:63:45:86:A4:6F:1A:B2:60:68:37:58:2D:C4:AC:FD:94:97

  Ausgabe: Jun 29 15:13:05 2007 GMT

  Ablauf: Jun 29 15:13:05 2027 GMT
- **SecureTrust_CA**
  Subjektname: /C=US/O=SecureTrust Corporation/CN=SecureTrust CA

  Fingerabdruck: 87:82:C6:C3:04:35:3B:CF:D2:96:92:D2:59:3E:7D:44:D9:34:FF:11

  Ausgabe: Nov 7 19:31:18 2006 GMT

  Ablauf: Dec 31 19:40:55 2029 GMT
- **SwissSign_Silver_CA_-_G2**
  Subjektname: /C=CH/O=SwissSign AG/CN=SwissSign Silver CA - G2

  Fingerabdruck: 9B:AA:E5:9F:56:EE:21:CB:43:5A:BE:25:93:DF:A7:F0:40:D1:1D:CB

  Ausgabe: Oct 25 08:32:46 2006 GMT

  Ablauf: Oct 25 08:32:46 2036 GMT
- **Taiwan_GRCA**
  Subjektname: /C=TW/O=Government Root Certification Authority

  Fingerabdruck: F4:8B:11:BF:DE:AB:BE:94:54:20:71:E6:41:DE:6B:BE:88:2B:40:B9

  Ausgabe: Dec 5 13:23:33 2002 GMT

  Ablauf: Dec 5 13:23:33 2032 GMT
- **WellsSecure_Public_Root_Certificate_Authority**
  Subjektname: /C=US/O=Wells Fargo WellsSecure/OU=Wells Fargo Bank NA/CN=WellsSecure Public Root Certificate Authority

  Fingerabdruck: E7:B4:F6:9D:61:EC:90:69:DB:7E:90:A7:40:1A:3C:F4:7D:4F:E8:EE

  Ausgabe: Dec 13 17:07:54 2007 GMT

  Ablauf: Dec 14 00:07:54 2022 GMT
- **AddTrust_Low-Value_Services_Root**
  Subjektname: /C=SE/O=AddTrust AB/OU=AddTrust TTP Network/CN=AddTrust Class 1 CA Root

  Fingerabdruck: CC:AB:0E:A0:4C:23:01:D6:69:7B:DD:37:9F:CD:12:EB:24:E3:94:9D

  Ausgabe: May 30 10:38:31 2000 GMT

  Ablauf: May 30 10:38:31 2020 GMT
- **DigiCert_High_Assurance_EV_Root_CA**
  Subjektname: /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert High Assurance EV Root CA

  Fingerabdruck: 5F:B7:EE:06:33:E2:59:DB:AD:0C:4C:9A:E6:D3:8F:1A:61:C7:DC:25

Ausgabe: Nov 10 00:00:00 2006 GMT

Ablauf: Nov 10 00:00:00 2031 GMT

- **VeriSign_Class_3_Public_Primary_Certification_Authority_-_G4**
  Subjektname: /C=US/O=VeriSign, Inc./OU=VeriSign Trust Network/OU=(c) 2007 VeriSign, Inc. - For authorized use only/CN=VeriSign Class 3 Public Primary Certification Authority - G4

  Fingerabdruck: 22:D5:D8:DF:8F:02:31:D1:8D:F7:9D:B7:CF:8A:2D:64:C9:3F:6C:3A

  Ausgabe: Nov 5 00:00:00 2007 GMT

  Ablauf: Jan 18 23:59:59 2038 GMT
- **Verisign_Class_1_Public_Primary_Certification_Authority_-_G2**
  Subjektname: /C=US/O=VeriSign, Inc./OU=Class 1 Public Primary Certification Authority - G2/OU=(c) 1998 VeriSign, Inc. - For authorized use only/OU=VeriSign Trust Network

  Fingerabdruck: 27:3E:E1:24:57:FD:C4:F9:0C:55:E8:2B:56:16:7F:62:F5:32:E5:47

  Ausgabe: May 18 00:00:00 1998 GMT

  Ablauf: Aug 1 23:59:59 2028 GMT
- **CFCA_EV_ROOT**
  Subjektname: /C=CN/O=China Financial Certification Authority/CN=CFCA EV ROOT

  Fingerabdruck: E2:B8:29:4B:55:84:AB:6B:58:C2:90:46:6C:AC:3F:B8:39:8F:84:83

  Ausgabe: Aug 8 03:07:01 2012 GMT

  Ablauf: Dec 31 03:07:01 2029 GMT
- **TWCA_Global_Root_CA**
  Subjektname: /C=TW/O=TAIWAN-CA/OU=Root CA/CN=TWCA Global Root CA

  Fingerabdruck: 9C:BB:48:53:F6:A4:F6:D3:52:A4:E8:32:52:55:60:13:F5:AD:AF:65

  Ausgabe: Jun 27 06:28:33 2012 GMT

  Ablauf: Dec 31 15:59:59 2030 GMT
- **SecureSign_RootCA11**
  Subjektname: /C=JP/O=Japan Certification Services, Inc./CN=SecureSign RootCA11

  Fingerabdruck: 3B:C4:9F:48:F8:F3:73:A0:9C:1E:BD:F8:5B:B1:C3:65:C7:D8:11:B3

  Ausgabe: Apr 8 04:56:47 2009 GMT

  Ablauf: Apr 8 04:56:47 2029 GMT
- **GeoTrust_Primary_Certification_Authority**
  Subjektname: /C=US/O=GeoTrust Inc./CN=GeoTrust Primary Certification Authority

  Fingerabdruck: 32:3C:11:8E:1B:F7:B8:B6:52:54:E2:E2:10:0D:D6:02:90:37:F0:96

  Ausgabe: Nov 27 00:00:00 2006 GMT

  Ablauf: Jul 16 23:59:59 2036 GMT
- **Equifax_Secure_CA**
  Subjektname: /C=US/O=Equifax/OU=Equifax Secure Certificate Authority

  Fingerabdruck: D2:32:09:AD:23:D3:14:23:21:74:E4:0D:7F:9D:62:13:97:86:63:3A

Ausgabe: Aug 22 16:41:51 1998 GMT

Ablauf: Aug 22 16:41:51 2018 GMT

- **Entrust_Root_Certification_Authority**
  Subjektname: /C=US/O=Entrust, Inc./OU=www.entrust.net/CPS is incorporated by reference/OU=(c) 2006 Entrust, Inc./CN=Entrust Root Certification Authority

  Fingerabdruck: B3:1E:B1:B7:40:E3:6C:84:02:DA:DC:37:D4:4D:F5:D4:67:49:52:F9

  Ausgabe: Nov 27 20:23:42 2006 GMT

  Ablauf: Nov 27 20:53:42 2026 GMT
- **Network_Solutions_Certificate_Authority**
  Subjektname: /C=US/O=Network Solutions L.L.C./CN=Network Solutions Certificate Authority

  Fingerabdruck: 74:F8:A3:C3:EF:E7:B3:90:06:4B:83:90:3C:21:64:60:20:E5:DF:CE

  Ausgabe: Dec 1 00:00:00 2006 GMT

  Ablauf: Dec 31 23:59:59 2029 GMT
- **QuoVadis_Root_CA_3_G3**
  Subjektname: /C=BM/O=QuoVadis Limited/CN=QuoVadis Root CA 3 G3

  Fingerabdruck: 48:12:BD:92:3C:A8:C4:39:06:E7:30:6D:27:96:E6:A4:CF:22:2E:7D

  Ablauf: Jan 12 20:26:32 2012 GMT

  Ausgabe: Jan 12 20:26:32 2042 GMT
- **Security_Communication_Root_CA**
  Subjektname: /C=JP/O=SECOM Trust.net/OU=Security Communication RootCA1

  Fingerabdruck: 36:B1:2B:49:F9:81:9E:D7:4C:9E:BC:38:0F:C6:56:8F:5D:AC:B2:F7

  Ausgabe: Sep 30 04:20:49 2003 GMT

  Ablauf: Sep 30 04:20:49 2023 GMT
- **Starfield_Root_Certificate_Authority_-_G2**
  Subjektname: /C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./CN=Starfield Root Certificate Authority - G2

  Fingerabdruck: B5:1C:06:7C:EE:2B:0C:3D:F8:55:AB:2D:92:F4:FE:39:D4:E7:0F:0E

  Ausgabe: Sep 1 00:00:00 2009 GMT

  Ablauf: Dec 31 23:59:59 2037 GMT
- **Cybertrust_Global_Root**
  Subjektname: /O=Cybertrust, Inc/CN=Cybertrust Global Root

  Fingerabdruck: 5F:43:E5:B1:BF:F8:78:8C:AC:1C:C7:CA:4A:9A:C6:22:2B:CC:34:C6

  Ausgabe: Dec 15 08:00:00 2006 GMT

  Ablauf: Dec 15 08:00:00 2021 GMT
- **Global_Chambersign_Root_-_2008**
  Subjektname: /C=EU/L=Madrid (see current address at www.camerfirma.com/address)/serialNumber=A82743287/O=AC Camerfirma S.A./CN=Global Chambersign Root - 2008

Fingerabdruck: 4A:BD:EE:EC:95:0D:35:9C:89:AE:C7:52:A1:2C:5B:29:F6:D6:AA:0C

Ausgabe: Aug 1 12:31:40 2008 GMT

Ablauf: Jul 31 12:31:40 2038 GMT

- **Comodo_Trusted_Services_root**
  Subjektname: /C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=Trusted Certificate Services

  Fingerabdruck: E1:9F:E3:0E:8B:84:60:9E:80:9B:17:0D:72:A8:C5:BA:6E:14:09:BD

  Ausgabe: Jan 1 00:00:00 2004 GMT

  Ablauf: Dec 31 23:59:59 2028 GMT
- **Secure_Global_CA**
  Subjektname: /C=US/O=SecureTrust Corporation/CN=Secure Global CA

  Fingerabdruck: 3A:44:73:5A:E5:81:90:1F:24:86:61:46:1E:3B:9C:C4:5F:F5:3A:1B

  Ausgabe: Nov 7 19:42:28 2006 GMT

  Ablauf: Dec 31 19:52:06 2029 GMT
- **SwissSign_Gold_CA_-_G2**
  Subjektname: /C=CH/O=SwissSign AG/CN=SwissSign Gold CA - G2

  Fingerabdruck: D8:C5:38:8A:B7:30:1B:1B:6E:D4:7A:E6:45:25:3A:6F:9F:1A:27:61

  Ausgabe: Oct 25 08:30:35 2006 GMT

  Ablauf: Oct 25 08:30:35 2036 GMT
- **NetLock_Express_=Class_C=_Root**
  Subjektname: /C=HU/L=Budapest/O=NetLock Halozatbiztonsagi Kft./OU=Tanusitvanykiadok/CN=NetLock Expressz (Class C) Tanusitvanykiado

  Fingerabdruck: E3:92:51:2F:0A:CF:F5:05:DF:F6:DE:06:7F:75:37:E1:65:EA:57:4B

  Ausgabe: Feb 25 14:08:11 1999 GMT

  Ablauf: Feb 20 14:08:11 2019 GMT
- **GlobalSign_ECC_Root_CA_-_R5**
  Subjektname: /OU=GlobalSign ECC Root CA - R5/O=GlobalSign/CN=GlobalSign

  Fingerabdruck: 1F:24:C6:30:CD:A4:18:EF:20:69:FF:AD:4F:DD:5F:46:3A:1B:69:AA

  Ausgabe: Nov 13 00:00:00 2012 GMT

  Ablauf: Jan 19 03:14:07 2038 GMT
- **Atos_TrustedRoot_2011**
  Subjektname: /CN=Atos TrustedRoot 2011/O=Atos/C=DE

  Fingerabdruck: 2B:B1:F5:3E:55:0C:1D:C5:F1:D4:E6:B7:6A:46:4B:55:06:02:AC:21

  Ausgabe: Jul 7 14:58:30 2011 GMT

  Ablauf: Dec 31 23:59:59 2030 GMT
- **Root_CA_Generalitat_Valenciana**
  Subjektname: /C=ES/O=Generalitat Valenciana/OU=PKIGVA/CN=Root CA Generalitat Valenciana

Fingerabdruck: A0:73:E5:C5:BD:43:61:0D:86:4C:21:13:0A:85:58:57:CC:9C:EA:46

Ausgabe: Jul 6 16:22:47 2001 GMT

Ablauf: Jul 1 15:22:47 2021 GMT

- **Hongkong_Post_Root_CA_1**
  Subjektname: /C=HK/O=Hongkong Post/CN=Hongkong Post Root CA 1

  Fingerabdruck: D6:DA:A8:20:8D:09:D2:15:4D:24:B5:2F:CB:34:6E:B2:58:B2:8A:58

  Ausgabe: May 15 05:13:14 2003 GMT

  Ablauf: May 15 04:52:29 2023 GMT
- **Security_Communication_RootCA2**
  Subjektname: /C=JP/O=SECOM Trust Systems CO.,LTD./OU=Security Communication RootCA2

  Fingerabdruck: 5F:3B:8C:F2:F8:10:B3:7D:78:B4:CE:EC:19:19:C3:73:34:B9:C7:74

  Ausgabe: May 29 05:00:39 2009 GMT

  Ablauf: May 29 05:00:39 2029 GMT
- **QuoVadis_Root_CA_2_G3**
  Subjektname: /C=BM/O=QuoVadis Limited/CN=QuoVadis Root CA 2 G3

  Fingerabdruck: 09:3C:61:F3:8B:8B:DC:7D:55:DF:75:38:02:05:00:E1:25:F5:C8:36

  Ausgabe: Jan 12 18:59:32 2012 GMT

  Ablauf: Jan 12 18:59:32 2042 GMT
- **OISTE_WISeKey_Global_Root_GA_CA**
  Subjektname: /C=CH/O=WISeKey/OU=Copyright (c) 2005/OU=OISTE Foundation Endorsed/CN=OISTE WISeKey Global Root GA CA

  Fingerabdruck: 59:22:A1:E1:5A:EA:16:35:21:F8:98:39:6A:46:46:B0:44:1B:0F:A9

  Ausgabe: Dec 11 16:03:44 2005 GMT

  Ablauf: Dec 11 16:09:51 2037 GMT
- **Verisign_Class_3_Public_Primary_Certification_Authority**
  Subjektname: /C=US/O=VeriSign, Inc./OU=Class 3 Public Primary Certification Authority

  Fingerabdruck: 74:2C:31:92:E6:07:E4:24:EB:45:49:54:2B:E1:BB:C5:3E:61:74:E2

  Ausgabe: Jan 29 00:00:00 1996 GMT

  Ablauf: Aug 1 23:59:59 2028 GMT
- **Microsec_e-Szigno_Root_CA**
  Subjektname: /C=HU/L=Budapest/O=Microsec Ltd./OU=e-Szigno CA/CN=Microsec e-Szigno Root CA

  Fingerabdruck: 23:88:C9:D3:71:CC:9E:96:3D:FF:7D:3C:A7:CE:FC:D6:25:EC:19:0D

  Ausgabe: Apr 6 12:28:44 2005 GMT

  Ablauf: Apr 6 12:28:44 2017 GMT
- **Izenpe.com**
  Subjektname: /C=ES/O=IZENPE S.A./CN=Izenpe.com

Fingerabdruck: 2F:78:3D:25:52:18:A7:4A:65:39:71:B5:2C:A2:9C:45:15:6F:E9:19

Ausgabe: Dec 13 13:08:28 2007 GMT

Ablauf: Dec 13 08:27:25 2037 GMT

- **Buypass_Class_2_Root_CA**
  Subjektname: /C=NO/O=Buypass AS-983163327/CN=Buypass Class 2 Root CA

  Fingerabdruck: 49:0A:75:74:DE:87:0A:47:FE:58:EE:F6:C7:6B:EB:C6:0B:12:40:99

  Ausgabe: Oct 26 08:38:03 2010 GMT

  Ablauf: Oct 26 08:38:03 2040 GMT
- **GeoTrust_Global_CA**
  Subjektname: /C=US/O=GeoTrust Inc./CN=GeoTrust Global CA

  Fingerabdruck: DE:28:F4:A4:FF:E5:B9:2F:A3:C5:03:D1:A3:49:A7:F9:96:2A:82:12

  Ausgabe: May 21 04:00:00 2002 GMT

  Ablauf: May 21 04:00:00 2022 GMT
- **GlobalSign_Root_CA_-_R2**
  Subjektname: /OU=GlobalSign Root CA - R2/O=GlobalSign/CN=GlobalSign

  Fingerabdruck: 75:E0:AB:B6:13:85:12:27:1C:04:F8:5F:DD:DE:38:E4:B7:24:2E:FE

  Ausgabe: Dec 15 08:00:00 2006 GMT

  Ablauf: Dec 15 08:00:00 2021 GMT
- **Certification_Authority_of_WoSign_G2**
  Subjektname: /C=CN/O=WoSign CA Limited/CN=Certification Authority of WoSign G2

  Fingerabdruck: FB:ED:DC:90:65:B7:27:20:37:BC:55:0C:9C:56:DE:BB:F2:78:94:E1

  Ausgabe: Nov 8 00:58:58 2014 GMT

  Ablauf: Nov 8 00:58:58 2044 GMT
- **Autoridad_de_Certificacion_Firmaprofesional_CIF_A62634068**
  Subjektname: /C=ES/CN=Autoridad de Certificacion Firmaprofesional CIF A62634068

  Fingerabdruck: AE:C5:FB:3F:C8:E1:BF:C4:E5:4F:03:07:5A:9A:E8:00:B7:F7:B6:FA

  Ausgabe: May 20 08:38:15 2009 GMT

  Ablauf: Dec 31 08:38:15 2030 GMT
- **EC-ACC**
  Subjektname: /C=ES/O=Agencia Catalana de Certificacio (NIF Q-0801176-I)/OU=Serveis Publics de Certificacio/OU=Vegeu https://www.catcert.net/verarrel (c)03/OU=Jerarquia Entitats de Certificacio Catalanes/CN=EC-ACC

  Fingerabdruck: 28:90:3A:63:5B:52:80:FA:E6:77:4C:0B:6D:A7:D6:BA:A6:4A:F2:E8

  Ausgabe: Jan 7 23:00:00 2003 GMT

  Ablauf: Jan 7 22:59:59 2031 GMT

- **USERTrust_ECC_Certification_Authority**
  Subjektname: /C=US/ST=New Jersey/L=Jersey City/O=The USERTRUST Network/CN=USERTrust ECC Certification Authority

  Fingerabdruck: D1:CB:CA:5D:B2:D5:2A:7F:69:3B:67:4D:E5:F0:5A:1D:0C:95:7D:F0

  Ausgabe: Feb 1 00:00:00 2010 GMT

  Ablauf: Jan 18 23:59:59 2038 GMT
- **Swisscom_Root_EV_CA_2**
  Subjektname: /C=ch/O=Swisscom/OU=Digital Certificate Services/CN=Swisscom Root EV CA 2

  Fingerabdruck: E7:A1:90:29:D3:D5:52:DC:0D:0F:C6:92:D3:EA:88:0D:15:2E:1A:6B

  Ausgabe: Jun 24 09:45:08 2011 GMT

  Ablauf: Jun 25 08:45:08 2031 GMT
- **CA_Disig**
  Subjektname: /C=SK/L=Bratislava/O=Disig a.s./CN=CA Disig

  Fingerabdruck: 2A:C8:D5:8B:57:CE:BF:2F:49:AF:F2:FC:76:8F:51:14:62:90:7A:41

  Ausgabe: Mar 22 01:39:34 2006 GMT

  Ablauf: Mar 22 01:39:34 2016 GMT
- **ePKI_Root_Certification_Authority**
  Subjektname: /C=TW/O=Chunghwa Telecom Co., Ltd./OU=ePKI Root Certification Authority

  Fingerabdruck: 67:65:0D:F1:7E:8E:7E:5B:82:40:A4:F4:56:4B:CF:E2:3D:69:C6:F0

  Ausgabe: Dec 20 02:31:27 2004 GMT

  Ablauf: Dec 20 02:31:27 2034 GMT
- **GeoTrust_Global_CA_2**
  Subjektname: /C=US/O=GeoTrust Inc./CN=GeoTrust Global CA 2

  Fingerabdruck: A9:E9:78:08:14:37:58:88:F2:05:19:B0:6D:2B:0D:2B:60:16:90:7D

  Ausgabe: Mar 4 05:00:00 2004 GMT

  Ablauf: Mar 4 05:00:00 2019 GMT
- **Verisign_Class_3_Public_Primary_Certification_Authority_-_G3**
  Subjektname: /C=US/O=VeriSign, Inc./OU=VeriSign Trust Network/OU=(c) 1999 VeriSign, Inc. - For authorized use only/CN=VeriSign Class 3 Public Primary Certification Authority - G3

  Fingerabdruck: 13:2D:0D:45:53:4B:69:97:CD:B2:D5:C3:39:E2:55:76:60:9B:5C:C6

  Ausgabe: Oct 1 00:00:00 1999 GMT

  Ablauf: Jul 16 23:59:59 2036 GMT

Abschnitt 6.6.3

Zertifikate von Zertifizierungsstellen (CA) im Speicher für vertrauenswürdige Zertifikate verwalten

Für eine vertrauenswürdige Verbindung zwischen dem Gerät und einem Endpunkt (z. B. Server, Portal usw.) fügen Sie im Speicher für vertrauenswürdige Zertifikate die erforderlichen Zertifikate hinzu.

INHALT

- Abschnitt 6.6.3.1, „Eine Liste der Zertifikate einer Zertifizierungsstelle (CA) im Speicher für vertrauenswürdige Zertifikate anzeigen“
- Abschnitt 6.6.3.2, „Ein Zertifikat von einer Zertifizierungsstelle zum Speicher für vertrauenswürdige Zertifikate hinzufügen“
- Abschnitt 6.6.3.3, „Ein Zertifikat einer Zertifizierungsstelle (CA) im Speicher für vertrauenswürdige Zertifikate löschen“

Abschnitt 6.6.3.1

Eine Liste der Zertifikate einer Zertifizierungsstelle (CA) im Speicher für vertrauenswürdige Zertifikate anzeigen

Um eine Liste der Zertifikate einer Zertifizierungsstelle (CA) im Speicher anzusehen, geben Sie Folgendes ein:

```
show admin system-ca-certificates configured-cas
```

Falls solche Zertifikate im Speicher hinzugefügt wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config admin system-ca-certificates configured-cas | tab
NAME
------
cert

!
```

Falls keine solchen Zertifikate im Speicher hinzugefügt wurden, fügen Sie je nach Bedarf Zertifikate hinzu. Weitere Informationen finden Sie unter Abschnitt 6.6.3.2, „Ein Zertifikat von einer Zertifizierungsstelle zum Speicher für vertrauenswürdige Zertifikate hinzufügen“.

Abschnitt 6.6.3.2

Ein Zertifikat von einer Zertifizierungsstelle zum Speicher für vertrauenswürdige Zertifikate hinzufügen

Um ein Zertifikat von einer Zertifizierungsstelle zum Speicher für vertrauenswürdige Zertifikate hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie das Zertifikat der Zertifizierungsstelle hinzu, indem Sie Folgendes eingeben:

   ```
   admin system-ca-certificates configured-cas certificate
   ```

   Erläuterung: *certificate* ist das ausgewählte Zertifikat der Zertifizierungsstelle.

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 6.6.3.3
Ein Zertifikat einer Zertifizierungsstelle (CA) im Speicher für vertrauenswürdige Zertifikate löschen

Um ein Zertifikat einer Zertifizierungsstelle (CA) im Speicher für vertrauenswürdige Zertifikate zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie das statische VLAN durch Eingabe von:

   ```
   no admin system-ca-certificates configured-cas certificate
   ```

   Erläuterung: *certificate* ist das ausgewählte Zertifikat der Zertifizierungsstelle.
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 6.6.4
Zertifikate von Zertifizierungsstellen (CA) und CRLs verwalten

Dieser Abschnitt beschreibt, wie Sie Zertifikate von Zertifizierungsstellen (CA) und Zertifikat-Widerrufslisten (CRLs) im Gerät ansehen, hinzufügen und löschen können.

INHALT

- Abschnitt 6.6.4.1, „Eine Liste der Zertifikate von Zertifizierungsstellen und CRLs anzeigen“
- Abschnitt 6.6.4.2, „Anzeigen des Status eines CA-Zertifikats und einer CRL“
- Abschnitt 6.6.4.3, „Hinzufügen eines CA-Zertifikats und der CRL“
- Abschnitt 6.6.4.4, „Ein CA-Zertifikat und eine CRL löschen“

Abschnitt 6.6.4.1
Eine Liste der Zertifikate von Zertifizierungsstellen und CRLs anzeigen

Um eine Liste der von einer Zertifizierungsstelle (CA) ausgestellten Zertifikate und die zugehörigen Zertifikat-Widerrufslisten (CRLs) anzusehen, geben Sie Folgendes ein:

```
show running-config security crypto ca
```

Falls Zertifikate konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config security crypto ca security crypto ca ca-cert key-cert-sign-certificate
 "{--contents--}" ! ! !
```

Falls keine Zertifikate konfiguriert wurden, fügen Sie je nach Bedarf Zertifikate hinzu. Weitere Informationen finden Sie unter Abschnitt 6.6.4.3, „Hinzufügen eines CA-Zertifikats und der CRL“.

Abschnitt 6.6.4.2

Anzeigen des Status eines CA-Zertifikats und einer CRL

Um den Status des CA-Zertifikats anzuzeigen, geben Sie Folgendes ein:

```
show security crypto ca certificate key-cert-sign-certificate-status
```

Erläuterung:

- *certificate* ist die Bezeichnung des Zertifikats

Diese Tabelleoder Liste liefert die folgenden Informationen:

Parameter	Beschreibung
issuer	**Zusammenfassung:** Eine Zeichenkette
subject	**Zusammenfassung:** Eine Zeichenkette
not-before	**Zusammenfassung:** Eine Zeichenkette Dieses Zertifikat ist vor diesem Datum ungültig.
not-after	**Zusammenfassung:** Eine Zeichenkette Dieses Zertifikat ist nach diesem Datum ungültig.

Um den Status einer Zertifikatsperrliste (CRL) anzuzeigen, die von einem separaten Zertifikat signiert wurde, geben Sie Folgendes ein:

```
show security crypto ca certificate crl-sign-certificate-status
```

Erläuterung:

- *certificate* ist die Bezeichnung des Zertifikats

Diese Tabelleoder Liste liefert die folgenden Informationen:

Parameter	Beschreibung
issuer	**Zusammenfassung:** Eine Zeichenkette
subject	**Zusammenfassung:** Eine Zeichenkette
not-before	**Zusammenfassung:** Eine Zeichenkette Dieses Zertifikat ist vor diesem Datum ungültig.
not-after	**Zusammenfassung:** Eine Zeichenkette Dieses Zertifikat ist nach diesem Datum ungültig.

Um den Status einer Zertifikatsperrliste (CRL) anzuzeigen, die nicht von einem separaten Zertifikat signiert wurde, geben Sie Folgendes ein:

```
show security crypto ca certificate crl-status
```

Erläuterung:

- *certificate* ist die Bezeichnung des Zertifikats

Diese Tabelleoder Liste liefert die folgenden Informationen:

Parameter	Beschreibung
issuer	**Zusammenfassung:** Eine Zeichenkette
this-update	**Zusammenfassung:** Eine Zeichenkette Die CRL wurde an diesem Datum und zu dieser Uhrzeit aktualisiert.

Parameter	Beschreibung
next-update	**Zusammenfassung:** Eine Zeichenkette Das Zertifikat muss an diesem Datum und zu dieser Uhrzeit aktualisiert werden.

Abschnitt 6.6.4.3

Hinzufügen eines CA-Zertifikats und der CRL

Um ein von einer Zertifizierungsstelle (Certified Authority, CA) ausgestelltes Zertifikat und die zugehörige Zertifikatesperrliste (Certificate Revocation List, CRL) hinzuzufügen, gehen Sie wie folgt vor:

HINWEIS
Nur Admin-Benutzer können Zertifikate und Schlüssel auf dem Gerät lesen/schreiben.

1. Aktivieren Sie den Auto-Assistenten, indem Sie Folgendes eingeben:

   ```
   autowizard true
   ```

2. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.

   HINWEIS
   *Bevor Sie den Inhalt des Zertifikats eingeben, starten Sie über **Esc+m** den Multiline-Modus. Drücken Sie **Strg+D**, um den Multiline-Modus nach dem Hinzufügen des Zertifikats wieder zu verlassen.*

3. Fügen Sie das Zertifikat der Zertifizierungsstelle hinzu, indem Sie Folgendes eingeben:

   ```
   security crypto ca certificate key-cert-sign-certificate contents
   ```

   Erläuterung:

   - *certificate* ist die Bezeichnung des Zertifikats
   - *contents* ist der Inhalt des Zertifikats

4. Fügen Sie die zugehörige Zertifikatesperrliste (CRL) hinzu.

   HINWEIS
   Große CRLs (über 100 KB) werden aktuell nicht unterstützt und das Hinzufügen/Anzeigen in der Konfiguration kann schwierig sein.

   HINWEIS
   *Bevor Sie den Inhalt der CRL eingeben, starten Sie über **Esc+m** den Multiline-Modus. Drücken Sie **Ctrl+d**, um den Multiline-Modus nach dem Hinzufügen der CRL wieder zu verlassen.*

   - Wird die CRL von einem separaten Zertifikat signiert, geben Sie Folgendes ein:

     ```
     security crypto ca certificate crl-sign-certificate contents
     ```

     Erläuterung:

     - *certificate* ist die Bezeichnung des Zertifikats
     - *contents* ist der Inhalt der signierten CRL

   - Wird die CRL nicht signiert, geben Sie Folgendes ein:

     ```
     security crypto ca certificate crl contents
     ```

Erläuterung:

- *certificate* ist die Bezeichnung des Zertifikats
- *contents* ist der Inhalt der CRL

5. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 6.6.4.4
Ein CA-Zertifikat und eine CRL löschen

Um ein von einer Zertifizierungsstelle (Certified Authority, CA) ausgestelltes Zertifikat und die zugehörige Zertifikatesperrliste (Certificate Revocation List, CRL) zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie das CA-Zertifikat und die zugehörige Zertifikatesperrliste (CRL), indem Sie Folgendes eingeben:

```
no security crypto ca certificate
```

Erläuterung:

- *certificate* ist die Bezeichnung des Zertifikats

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 6.6.5
Private Schlüssel verwalten

Dieser Abschnitt beschreibt, wie Sie private Schlüssel im Gerät ansehen, hinzufügen und löschen können.

HINWEIS
Private Schlüssel werden automatisch mit einer AES-CFB-128-Ziffer verschlüsselt, um sie vor dem Zugriff unbefugter Benutzer zu schützen.

INHALT

- Abschnitt 6.6.5.1, „Eine Liste der privaten Schlüssel anzeigen“
- Abschnitt 6.6.5.2, „Einen privaten Schlüssel hinzufügen“
- Abschnitt 6.6.5.3, „Einen privaten Schlüssel löschen“

Abschnitt 6.6.5.1
Eine Liste der privaten Schlüssel anzeigen

Um eine Liste unsignierter privater Schlüssel anzusehen, geben Sie Folgendes ein:

```
show running-config security crypto private-key
```

Falls private Schlüssel konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config security crypto private-key
```

```
security
 crypto
  private-key key
   algorithm rsa
   contents
   "{--contents--}"
  !
 !
!
```

Falls keine privaten Schlüssel konfiguriert wurden, fügen Sie je nach Bedarf Schlüssel hinzu. Weitere Informationen finden Sie unter Abschnitt 6.6.5.2, „Einen privaten Schlüssel hinzufügen“.

Abschnitt 6.6.5.2
Einen privaten Schlüssel hinzufügen

Um einen nicht signierten privaten Schlüssel hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den privaten Schlüssel hinzu, indem Sie Folgendes eingeben:

   ```
   security crypto private-key name
   ```

   Erläuterung:

   - *name* ist die Bezeichnung des privaten Schlüssels
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

   HINWEIS
   *Bevor Sie den Inhalt des Schlüssels eingeben, starten Sie über **Esc+m** den Multiline-Modus. Drücken Sie **Ctrl+d**, um den Multiline-Modus nach dem Hinzufügen des Schlüssels wieder zu verlassen*

Parameter	Beschreibung
algorithm { algorithm }	**Zusammenfassung:** { rsa, dsa, ssh-rsa } Der Schlüsseltyp. Dieser Parameter ist obligatorisch.
contents { contents }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 8192 Zeichen Der Inhalt des nicht signierten privaten Schlüssels. Dieser Parameter ist obligatorisch.

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 6.6.5.3
Einen privaten Schlüssel löschen

Um einen unsignierten privaten Schlüssel zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den privaten Schlüssel durch Eingabe von:

```
no security crypto private-key name
```

Erläuterung: *name* ist die Bezeichnung des privaten Schlüssels

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 6.6.6
Öffentliche Schlüssel verwalten

Dieser Abschnitt beschreibt, wie Sie öffentliche Schlüssel im Gerät verwalten können.

INHALT

- Abschnitt 6.6.6.1, „Eine Liste der öffentlichen Schlüssel anzeigen“
- Abschnitt 6.6.6.2, „Hinzufügen eines öffentlichen Schlüssels“
- Abschnitt 6.6.6.3, „Hinzufügen eines IPSec-formatierten öffentlichen Schlüssels“
- Abschnitt 6.6.6.4, „Einen öffentlichen Schlüssel löschen“

Abschnitt 6.6.6.1
Eine Liste der öffentlichen Schlüssel anzeigen

Um eine Liste unsignierter öffentlicher Schlüssel anzusehen, geben Sie Folgendes ein:

```
show running-config security crypto public-key
```

Falls öffentliche Schlüssel konfiguriert wurden, wird eine Tabelle oder Liste wie im folgenden Beispiel angezeigt:

```
ruggedcom# show running-config security crypto public-key
security
crypto
  public-key ipsec-generated
   algorithm        rsa
   contents         "{--contents--}"
   private-key-name ipsec-generated
  !
!
!
```

Falls keine öffentlichen Schlüssel konfiguriert wurden, fügen Sie je nach Bedarf Schlüssel hinzu. Weitere Informationen finden Sie unter Abschnitt 6.6.6.2, „Hinzufügen eines öffentlichen Schlüssels“.

Abschnitt 6.6.6.2
Hinzufügen eines öffentlichen Schlüssels

Um einen nicht signierten öffentlichen Schlüssel hinzuzufügen, gehen Sie wie folgt vor:

HINWEIS
Ordnen Sie den öffentlichen Schlüssel nicht dem privaten Schlüssel zu, wenn der öffentliche Schlüssel zu einem anderen Gerät gehört.

1. Stellen Sie sicher, dass der dem öffentlichen Schlüssel zugeordnete private Schlüssel hinzugefügt wurde. Weitere Informationen finden Sie unter Abschnitt 6.6.5.2, „Einen privaten Schlüssel hinzufügen“.
2. Aktivieren Sie den Auto-Assistenten, indem Sie Folgendes eingeben:

```
autowizard true
```

3. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
4. Fügen Sie den öffentlichen Schlüssel hinzu, indem Sie Folgendes eingeben:

```
security crypto public-key name
```

Erläuterung:

- *name* ist die Bezeichnung des öffentlichen Schlüssels

5. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

HINWEIS
*Bevor Sie den Inhalt des Schlüssels eingeben, starten Sie über **Esc+m** den Multiline-Modus. Drücken Sie **Strg+D**, um den Multiline-Modus nach dem Hinzufügen des Schlüssels wieder zu verlassen.*

Parameter	Beschreibung
algorithm { algorithm }	**Zusammenfassung:** { rsa, dsa, ssh-rsa } Der Algorithmus des Schlüssels. Dieser Parameter ist obligatorisch.
contents { contents }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 8192 Zeichen Der Inhalt des Schlüssels. Dieser Parameter ist obligatorisch.
private-key-name { private-key-name }	**Zusammenfassung:** Eine Zeichenkette Der Name des privaten Schlüssels zu diesem öffentlichen Schlüssel.

6. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 6.6.6.3
Hinzufügen eines IPSec-formatierten öffentlichen Schlüssels

IPSec-formatierte öffentliche Schlüssel von Systemen, die das Format Privacy-Enhanced Mail (PEM) nicht unterstützen (z. B. RUGGEDCOM-ROX-Geräte) können in den RUGGEDCOM ROX II importiert und automatisch konvertiert werden.

Nach dem Hinzufügen zur RUGGEDCOM ROX II-Datenbank ist der IPSec-formatierte öffentliche Schlüssel über das Formular **System Public Key** unter ***tunnel » ipsec » connection » {name} » {end}*** einsehbar, wobei *{name}* die Bezeichnung der Verbindung und *{end}* entweder das linke (lokaler Router) oder rechte (dezentraler Router) Verbindungsende ist. Der **Type** muss auf `rsasig` gesetzt werden, um den öffentlichen Schlüssel anzuzeigen.

Der öffentliche Schlüssel kann aus dem Formular **System Public Key** kopiert und einem anderen RUGGEDCOM ROX II-Gerät, wie nachstehend beschrieben, oder einem RUGGEDCOM-ROX-Gerät, hinzugefügt werden.

Um einen IPSec-formatierten öffentlichen Schlüssel hinzuzufügen und in das PEM-Format zu konvertieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass der gewünschte öffentliche Schlüssel hinzugefügt wurde. Weitere Informationen über das Hinzufügen von öffentlichen Schlüsseln finden Sie in Abschnitt 6.6.6.2, „Hinzufügen eines öffentlichen Schlüssels“.
2. Aktivieren Sie den Auto-Assistenten, indem Sie Folgendes eingeben:

   ```
   autowizard true
   ```
3. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
4. Geben Sie den folgenden Befehl ein:

   ```
   security crypto public-key name add-ipsec-formatted-public-key content
   ```

   Erläuterung:

   - *name* ist die Bezeichnung des öffentlichen Schlüssels

   Die CLI ruft den Multiline-Modus auf.
5. Geben Sie den Inhalt des öffentlichen Schlüssels ein und drücken Sie für jede neue Zeile auf **Enter**. Drücken Sie abschließend **Strg-D**. Die öffentlichen Schlüssel werden in das PEM-Format konvertiert und dem RUGGEDCOM ROX II hinzugefügt.
6. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 6.6.6.4
Einen öffentlichen Schlüssel löschen

Um einen unsignierten öffentlichen Schlüssel zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den öffentlichen Schlüssel durch Eingabe von:

   ```
   no security crypto public-key name
   ```

   Erläuterung: *name* ist die Bezeichnung des öffentlichen Schlüssels
3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 6.6.7
Zertifikate verwalten

Dieser Abschnitt beschreibt, wie Sie Zertifikate im Gerät verwalten können.

INHALT

- Abschnitt 6.6.7.1, „Eine Liste der Zertifikate anzeigen“
- Abschnitt 6.6.7.2, „Den Status eines Zertifikats anzeigen“
- Abschnitt 6.6.7.3, „Hinzufügen eines Zertifikats“
- Abschnitt 6.6.7.4, „Ein Zertifikat löschen“

Abschnitt 6.6.7.1
Eine Liste der Zertifikate anzeigen

Um eine Liste der Zertifikate anzusehen, geben Sie Folgendes ein:

```
show running-config security crypto certificate
```

Falls Zertifikate konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config security crypto certificate
security
 crypto
  certificate cert
   contents         "{--contents--}"
   private-key-name key
   ca-name          ca-cert
  !
 !
!
```

Falls keine Zertifikate konfiguriert wurden, fügen Sie je nach Bedarf Zertifikate hinzu. Weitere Informationen finden Sie unter Abschnitt 6.6.7.3, „Hinzufügen eines Zertifikats“.

Abschnitt 6.6.7.2
Den Status eines Zertifikats anzeigen

Um den Status eines Zertifikats anzusehen, geben Sie Folgendes ein:

```
show security crypto certificate certificate status
```

Erläuterung:

- *certificate* ist die Bezeichnung des Zertifikats

```
ruggedcom# show security crypto certificate ssl-cert status
status
 issuer     /C=CA/ST=Ontario/L=Concord/O=RuggedCom.com/OU=RC/CN=localhost.localdomain
 subject    /C=CA/ST=Ontario/L=Concord/O=RuggedCom.com/OU=RC/CN=localhost.localdomain
 not before 2017-01-06T18:45:49-00:00
 not after  2037-01-03T18:45:49-00:00
```

Diese Tabelle oder Liste liefert die folgenden Informationen:

Parameter	Beschreibung
issuer	**Zusammenfassung:** Eine Zeichenkette
subject	**Zusammenfassung:** Eine Zeichenkette
not-before	**Zusammenfassung:** Eine Zeichenkette Dieses Zertifikat ist vor diesem Datum ungültig.
not-after	**Zusammenfassung:** Eine Zeichenkette Dieses Zertifikat ist nach diesem Datum ungültig.

Abschnitt 6.6.7.3
Hinzufügen eines Zertifikats

Um ein Zertifikat hinzuzufügen, gehen Sie wie folgt vor:

HINWEIS
Nur Admin-Benutzer können Zertifikate und Schlüssel auf dem Gerät lesen/schreiben.

1. Stellen Sie sicher, dass die erforderlichen CA-Zertifikate und/oder privaten Schlüssel zum Gerät hinzugefügt wurden.
   - Weitere Informationen über das Hinzufügen von CA-Zertifikaten finden Sie in Abschnitt 6.6.4.3, „Hinzufügen eines CA-Zertifikats und der CRL“.
   - Weitere Informationen über das Hinzufügen von privaten Schlüsseln finden Sie in Abschnitt 6.6.5.2, „Einen privaten Schlüssel hinzufügen“.
2. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
3. Fügen Sie das Zertifikat hinzu, indem Sie Folgendes eingeben:

   ```
   security crypto certificate certificate
   ```

   Erläuterung: *certificate* ist die Bezeichnung des Zertifikats.
4. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

   HINWEIS
   *Bevor Sie den Inhalt des Zertifikats eingeben, starten Sie über **Esc+m** den Multiline-Modus. Drücken Sie **Strg+D**, um den Multiline-Modus nach dem Hinzufügen des Zertifikats wieder zu verlassen.*

Parameter	Beschreibung
contents { contents }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 8192 Zeichen Der Inhalt des Zertifikats. Dieser Parameter ist obligatorisch.
private-key-name { private-key-name }	**Zusammenfassung:** Eine Zeichenkette Der private Schlüssel zu diesem Zertifikat.
ca-name { ca-name }	**Zusammenfassung:** Eine Zeichenkette Das optionale CA-Zertifikat für dieses Zertifikat.

5. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 6.6.7.4
Ein Zertifikat löschen

Um ein Zertifikat zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie das Zertifikat, indem Sie Folgendes eingeben:

   ```
   no security crypto certificate certificate
   ```

Erläuterung:

- *certificate* ist die Bezeichnung des Zertifikats

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 6.7

Verwalten von Firewalls

Firewalls sind Softwaresysteme, die dem Schutz vor unbefugtem Zugriff auf oder von privaten Netzwerken dienen. Firewalls werden am häufigsten dafür eingesetzt, unbefugte Internet-Nutzer am Zugriff auf mit dem Internet verbundene private Netzwerke (Intranets) zu hindern.

Bei aktivierter RUGGEDCOM ROX II-Firewall agiert der Router als Gateway-Maschine, die alle in das Intranet eingehenden bzw. aus dem Intranet abgehenden Nachrichten passieren. Der Router untersucht jede Nachricht und blockiert jene Nachrichten, die die festgelegten Sicherheitskriterien nicht erfüllen. Der Router agiert auch als Proxy und verhindert die direkte Kommunikation zwischen Computern im Internet und Intranet. Proxy-Server können die Kommunikationsarten filtern, die zwischen zwei Computern zugelassen sind, und die Adressübersetzung ausführen.

HINWEIS

Die Firewall-Implementierung des RUGGEDCOM ROX II erhält alle hergestellten Verbindungen aufrecht. Dies gilt für das Hinzufügen, Löschen oder Ändern von Regeln sowie für das Hinzufügen, Löschen oder Ändern von Grundregeln. Bei der Anwendung neuer oder modifizierter Regeln bzw. Grundregeln wird für den Router sichtbarer früherer Verkehr möglicherweise noch als Verkehr mit gültigen Verbindungen gemäß Verbindungsverfolgungstabelle betrachtet. Beispiel:

a. Eine Regel für die Protokolle TCP und UDP wird angewandt.

b. Der Router erkennt sowohl den TCP- als auch den UDP-Datenverkehr, die sich für NAT qualifizieren.

c. Die Regel wird anschließend so modifiziert, dass nur UDP zugelassen wird.

d. Der Router erkennt noch immer TCP-Pakete (d.h. Pakete der erneuten Übertragung).

Starten Sie den Router bei Bedarf neu, um alle vorhandenen Verbindungsströme zu entfernen.

Der RUGGEDCOM ROX II besitzt ein zustandsbezogenes Firewall-System ("Netfilter"), ein Teilsystem des Linux-Kernels, der die Prüfung von IP-Paketen auf Sitzungsbasis ermöglicht.

Für weitere Informationen über Firewalls siehe Abschnitt 6.7.1, „Firewall-Konzepte“.

INHALT

- Abschnitt 6.7.1, „Firewall-Konzepte“
- Abschnitt 6.7.2, „Eine Liste der Firewalls anzeigen“
- Abschnitt 6.7.3, „Hinzufügen einer Firewall“
- Abschnitt 6.7.4, „Eine Firewall löschen“
- Abschnitt 6.7.5, „Betrieb mit mehreren Firewallkonfigurationen“
- Abschnitt 6.7.6, „Konfigurieren der Firewall für ein VPN“
- Abschnitt 6.7.7, „Die Firewall für ein VPN in einer entmilitarisierten Zone (DMZ) konfigurieren“
- Abschnitt 6.7.8, „Zonen verwalten“

- Abschnitt 6.7.9, „Schnittstellen verwalten“
- Abschnitt 6.7.10, „Hosts verwalten“
- Abschnitt 6.7.11, „Verwalten von Grundregeln“
- Abschnitt 6.7.12, „NAT-Einstellungen verwalten“
- Abschnitt 6.7.13, „Maskierungs- oder SNAT-Einstellungen verwalten“
- Abschnitt 6.7.14, „Regeln verwalten“
- Abschnitt 6.7.15, „Eine Firewall-Konfiguration überprüfen“
- Abschnitt 6.7.16, „Eine Firewall aktivieren/deaktivieren“

Abschnitt 6.7.1

Firewall-Konzepte

Dieser Abschnitt beschreibt einige wesentliche Konzepte für die Implementierung von Firewalls in RUGGEDCOM ROX II.

INHALT

- Abschnitt 6.7.1.1, „Zustandslose vs. zustandsorientierte Firewalls“
- Abschnitt 6.7.1.2, „Linux netfilter“
- Abschnitt 6.7.1.3, „Netzadressenübersetzung“
- Abschnitt 6.7.1.4, „Weiterleitung von Ports“
- Abschnitt 6.7.1.5, „Schutz gegen einen SYN-Flood-Angriff“
- Abschnitt 6.7.1.6, „Schutz gegen IP Spoofing“

Abschnitt 6.7.1.1

Zustandslose vs. zustandsorientierte Firewalls

Es gibt zwei Arten von Firewalls: zustandslose (stateless) und zustandsorientierte (stateful).

Zustandslose oder statische Firewalls treffen Entscheidungen ungeachtet der Historie des Datenverkehrs. Sie öffnen für den Verkehrstyp einfach einen Pfad auf Grundlage einer TCP- oder UDP-Portnummer. Zustandslose Firewalls sind relativ einfach und optimal für Web- und E-Mail-Verkehr. Jedoch haben zustandslose Firewalls einige Nachteile. Alle in der Firewall geöffneten Pfade sind immer offen und Verbindungen werden nicht nach externen Kriterien geöffnet oder geschlossen. Statische IP-Filter bieten keinerlei Authentifizierung.

Zustandsorientierte oder sitzungsbasierte Firewalls sorgen für eine erheblich höhere Komplexität des Firewall-Prozesses. Sie verfolgen den Status jeder Verbindung, untersuchen und testen jedes Paket (Verbindungsverfolgung) und erkennen und verwalten den gesamten Datenverkehr eines bestimmten Protokolls, der sich an den verbundenen TCP/UDP-Ports befindet.

Abschnitt 6.7.1.2

Linux netfilter

Netfilter ist ein Teilsystem des Linux-Kernels und eine zustandsbezogene Firewall, die es ermöglicht, IP-Pakete pro Sitzung zu untersuchen.

Netfilter verwendet Regelsätze; dies sind Sammlungen von Paketklassifizierungsregeln, mit denen das Ergebnis der Untersuchung eines bestimmten Pakets festgelegt wird. Die Regeln werden mit iptables definiert, einer generischen Tabellenstruktursyntax und Dienstprogramm für die Konfiguration und Steuerung von netfilter.

ROX implementiert eine IP-Firewall mit Hilfe einer strukturierten Benutzeroberfläche für die Konfiguration von iptables-Regeln und netfilter-Regelsätzen.

Abschnitt 6.7.1.3

Netzadressenübersetzung

Die Netzadressenübersetzung (NAT) erlaubt einem LAN die Verwendung eines Satzes an IP-Adressen für den internen Verkehr und einen zweiten Satz für den externen Verkehr. Die Netfilter-NAT-Funktion führt alle erforderlichen IP-Adressenübersetzungen aus, während der Verkehr zwischen Intranet und Internet geleitet wird. NAT wird unter Linux häufig als IP-Maskierung bezeichnet.

NAT stellt eine Art Firewall durch Ausblenden interner IP-Adressen bereit. Außerdem sorgt NAT dafür, dass ein Netzwerk mehr interne IP-Adressen verwendet. Da diese ausschließlich intern verwendet werden, können keine Konflikte mit von anderen Organisationen verwendeten IP-Adressen auftreten. Ein internes Netzwerk ist üblicherweise so konfiguriert, dass es einen oder mehrere reservierte Adressblöcke gemäß RFC1918 verwendet.

Tabelle: Reservierte IP-Adressblöcke nach RFC1918

IP-Netzwerk/Maske	Adressbereich
10.0.0.0/8	10.0.0.0 – 10.255.255.255
172.16.0.0/12	172.16.0.0 – 172.31.255.255
192.168.0.0/16	192.168.0.0 – 192.168.255.255

Wenn ein Paket von einem Host im internen Netzwerk das NAT-Gateway erreicht, werden seine Quelladresse und die TCP/UDP-Quellportnummer aufgezeichnet. Die Adress- und die Portnummer werden in die öffentliche IP-Adresse und eine nicht verwendete Portnummer an der öffentlichen Schnittstelle übersetzt. Wenn der Internet-Host auf das Paket des internen Host antwortet, wird er an die externe IP-Adresse des NAT-Gateway als die Übersetzungs-Portnummer verwiesen. Das NAT-Gateway durchsucht seine Tabellen und nimmt in Bezug auf das ausgehende Paket gegenteilige Änderungen vor. Anschließend leitet NAT das Antwortpaket an den internen Host weiter.

Die Übersetzung von ICMP-Paketen erfolgt in ähnlicher Weise, jedoch ohne Modifikation des Quellports.

NAT kann in statischen und dynamischen Modi verwendet werden. Das statische NAT (SNAT) maskiert die privaten IP-Adressen, indem jede interne Adresse in eine eindeutige externe Adresse übersetzt wird. Das dynamische NAT übersetzt alle internen Adressen in eine oder mehrere externe Adressen.

Abschnitt 6.7.1.4

Weiterleitung von Ports

Die Portweiterleitung bzw. Portumleitung gestattet, dass Datenverkehr aus dem Internet an einen Host hinter dem NAT-Gateway gesendet wird.

In vorherigen Beispielen wurden NAT-Prozesse beschrieben, bei denen Verbindungen vom Intranet zum Internet hergestellt wurden. In diesen Beispielen waren Adressen und Ports eindeutig.

Wenn versucht wird, Verbindungen vom Internet zum Intranet herzustellen, hat das NAT-Gateway mehrere Hosts im Intranet, die die Verbindung akzeptieren können. Es benötigt zusätzliche Informationen zur Identifikation des Hosts, um die Verbindung zu akzeptieren.

Im Folgenden wird angenommen, dass zwei Hosts, 192.168.1.10 und 192.168.1.20, sich hinter einem NAT-Gateway mit einer öffentlichen Schnittstelle 213.18.101.62 befinden. Wenn eine Verbindungsanfrage für HTTP-Port 80 an 213.18.101.62 ankommt, kann der NAT-Gateway die Anfrage an einen der Hosts weiterleiten (oder diese selbst akzeptieren). Die Port-Weiterleitung kann verwendet werden, um die Anfragen an Port 80 an den ersten Host umzuleiten.

Die Weiterleitung von Ports kann auch Portnummern neu zuordnen. Der zweite Host muss möglicherweise auf die HTTP-Anfragen antworten. Da die Verbindungen an Port 80 an den ersten Host geleitet werden, kann dem zweiten Host eine andere Portnummer (z. B. 8080) zugewiesen werden. Da die Anfragen am Gateway für Port 8080 ankommen, ordnet das Gateway die Portnummer zu 80 neu zu und leitet die Anfrage an den zweiten Host weiter.

Bei der Port-Weiterleitung wird auch die Quelladresse berücksichtigt. Eine weitere Möglichkeit zur Lösung des vorstehenden Problems besteht darin, zwei Hosts 200.0.0.1 und 200.0.0.2 zuzuordnen und das NAT-Gateway Anfragen an Port 80 von 200.0.0.1 bis 192.168.1.10 und von 200.0.0.2 bis 192.168.1.20 weiterleiten zu lassen.

Abschnitt 6.7.1.5
Schutz gegen einen SYN-Flood-Angriff

RUGGEDCOM ROX II reagiert auf SYN-Pakete nach dem TCP-Standard durch Rückgabe eines SYN-ACK-Pakets für offene Ports und eines RST-Pakets für geschlossene Ports. Wird das Gerät mit einer großen Menge an SYN-Paketen überflutet, kann der betroffene Port möglicherweise nicht mehr reagieren.

Um SYN-Überflutungsangriffe an geschlossenen Ports zu verhindern, ist die Firewall so einzustellen, dass jeglicher Verkehr zu geschlossenen Ports blockiert wird. Dies verhindert, dass SYN-Pakete den Kernel erreichen.

Siemens empfiehlt ferner, die hörenden Ports so einzustellen, dass IP-Adressen an getrennten Schnittstellen eingeschlossen sind. Zum Beispiel kann das Gerät eingestellt werden, um auf eine IP-Adresse an switch.0001 und fe-cm-1 zu hören. Damit wird sichergestellt, dass ein Port erreichbar bleibt, wenn der andere überflutet ist.

Abschnitt 6.7.1.6
Schutz gegen IP Spoofing

IP Spoofing ist eine Technik, mit der IP-Pakete mit einer falschen IP-Quelladresse erzeugt werden, um die Identität des Absenders zu verschleiern oder einen vertrauenswürdigen Host zu simulieren. Dies führt dazu, dass unbefugte Personen Zugang zu einem Netzwerk erhalten.

In RUGGEDCOM ROX II kann IP Spoofing verhindert werden durch die Aktivierung von *routefilter* und *logmartians* für die Firewall-Schnittstelle.

Informationen zum Aktivieren von *routefilter* und *logmartians*finden Sie unter Abschnitt 6.7.9.2, „Hinzufügen einer Schnittstelle“.

Abschnitt 6.7.2
Eine Liste der Firewalls anzeigen

Um eine Liste der Firewalls anzusehen, geben Sie Folgendes ein:

```
show running-config security firewall fwconfig
```

Falls Firewalls konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config security firewall fwconfig
```

```
security
 firewall
  fwconfig firewall1
  !
  fwconfig firewall2
  !
 !
!
```

Falls keine Firewalls konfiguriert wurden, fügen Sie je nach Bedarf Firewalls hinzu. Weitere Informationen finden Sie unter Abschnitt 6.7.3, „Hinzufügen einer Firewall“.

Abschnitt 6.7.3

Hinzufügen einer Firewall

Um eine neue Firewall hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie die Firewall hinzu, indem Sie Folgendes eingeben:

   ```
   security firewall fwconfig firewall
   ```

   Erläuterung:

   - *firewall* ist die Bezeichnung der Firewall
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
description { description }	**Zusammenfassung:** Eine Zeichenkette Eine optionale Beschreibungszeichenkette.

4. Fügen Sie der Firewall zugeordnete Schnittstellen hinzu. Weitere Informationen über das Hinzufügen von Schnittstellen finden Sie in Abschnitt 6.7.9.2, „Hinzufügen einer Schnittstelle“.
5. Fügen Sie Netzwerkzonen für die Firewall hinzu. Stellen Sie sicher, dass es eine Zone vom Typ **firewall** gibt. Weitere Informationen über das Hinzufügen von Netzwerkzonen finden Sie in Abschnitt 6.7.8.2, „Eine Zone hinzufügen“.
6. Weisen Sie jeder Zone eine Schnittstelle zu. Weitere Informationen über das Zuweisen von Schnittstellen zu Zonen finden Sie in Abschnitt 6.7.9.3, „Eine Schnittstelle zu einer Zone zuweisen“.
7. Stellen Sie die Standard-Grundregeln für die Verkehrssteuerung zwischen Zonen ein. Stellen Sie sicher, dass die Grundregeln möglichst einschränkend sind. Weitere Informationen über das Konfigurieren von Grundregeln finden Sie in Abschnitt 6.7.11, „Verwalten von Grundregeln“.
8. Konfigurieren Sie die Einstellungen für die Netzadressenübersetzung (NAT), Maskierung oder statische Netzadressenübersetzung (SNAT). Weitere Informationen über das Konfigurieren von NAT-Einstellungen finden Sie in Abschnitt 6.7.12, „NAT-Einstellungen verwalten“. Weitere Informationen über das Konfigurieren von Maskierungs- und/oder SNAT-Einstellungen finden Sie in Abschnitt 6.7.13, „Maskierungs- oder SNAT-Einstellungen verwalten“.
9. Falls Hosts im Netzwerk Sitzungen aus dem Internet akzeptieren müssen, konfigurieren Sie die Firewall so, dass sie die Zielnetzadressenübersetzung (DNAT) unterstützt. Weitere Informationen über das Konfigurieren von Hosts finden Sie in Abschnitt 6.7.10, „Hosts verwalten“.
10. Bei Bedarf konfigurieren Sie Regeln, die die Standard-Grundregeln aufheben. Weitere Informationen über das Konfigurieren von Regeln finden Sie in Abschnitt 6.7.14, „Regeln verwalten“.

11. Bei Bedarf konfigurieren Sie eine Unterstützung für das VPN. Weitere Informationen finden Sie unter:
    - Abschnitt 6.7.6, „Konfigurieren der Firewall für ein VPN“
    - Abschnitt 6.7.7, „Die Firewall für ein VPN in einer entmilitarisierten Zone (DMZ) konfigurieren“
12. Validieren Sie die Konfiguration. Weitere Informationen über das Validieren einer Firewall finden Sie in Abschnitt 6.7.15, „Eine Firewall-Konfiguration überprüfen“.
13. Aktivieren Sie die Firewall. Weitere Informationen finden Sie unter Abschnitt 6.7.16, „Eine Firewall aktivieren/deaktivieren“.
14. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 6.7.4
Eine Firewall löschen

Um eine Firewall zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die Firewall durch Eingabe von:

   ```
   no security firewall fwconfig firewall
   ```

   Erläuterung: *`firewall`* ist die Bezeichnung der Firewall.
3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 6.7.5
Betrieb mit mehreren Firewallkonfigurationen

Mit dem RUGGEDCOM ROX II können die Benutzer mehrere Firewallkonfigurationen erstellen und in einer Konfiguration arbeiten, während eine weitere aktiv ist.

Um eine Konfiguration als Betriebskonfiguration und eine andere als aktive Konfiguration einzustellen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Legen Sie die Betriebskonfiguration fest, indem Sie Folgendes eingeben:

   ```
   security firewall work-config name
   ```

   Erläuterung:
   - *`name`* ist die Bezeichnung der Firewallkonfiguration
3. Legen Sie die aktive Konfiguration fest, indem Sie Folgendes eingeben:

   ```
   security firewall active-config name
   ```

   Erläuterung:
   - *`name`* ist die Bezeichnung der Firewallkonfiguration
4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 6.7.6

Konfigurieren der Firewall für ein VPN

Um eine Firewall für ein auf Grundregeln basierendes VPN zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass eine grundlegende Firewall konfiguriert wurde. Für weitere Informationen über das Konfigurieren einer Firewall siehe Abschnitt 6.7.3, „Hinzufügen einer Firewall“.
2. Stellen Sie sicher, dass Zonen für lokalen, Netzwerk- und VPN-Verkehr konfiguriert wurden. Für weitere Informationen über das Verwalten von Zonen siehe Abschnitt 6.7.8, „Zonen verwalten“.
3. Stellen Sie sicher, dass eine Zone mit der Bezeichnung *Any* vorhanden und vom Typ IPSec ist. Für weitere Informationen über das Verwalten von Zonen siehe Abschnitt 6.7.8, „Zonen verwalten“.
4. Konfigurieren Sie die Schnittstelle, die den verschlüsselten IPSec-Verkehr überträgt. Stellen Sie sicher, dass sie der Zone *Any* zugeordnet ist, da diese den Verkehr für alle Zonen übertragen wird. Weitere Informationen über das Zuweisen von Schnittstellen zu Zonen finden Sie in Abschnitt 6.7.9.3, „Eine Schnittstelle zu einer Zone zuweisen“.
5. Konfigurieren Sie einen Host für die Schnittstelle, die den unverschlüsselten IPSec-Verkehr überträgt. Stellen Sie sicher, dass die VPN-Zone der Schnittstelle zugeordnet ist. Wenn VPN-Tunnel zu mehreren dezentralen Standorten erforderlich sind, stellen Sie sicher, dass ein Hosteintrag für jeden vorhanden ist oder bilden Sie ein einziges Subnetz. Weitere Informationen über das Konfigurieren von Hosts finden Sie in Abschnitt 6.7.10, „Hosts verwalten“.
6. Konfigurieren Sie einen zweiten Host für die Schnittstelle, die den verschlüsselten IPSec-Verkehr überträgt. Stellen Sie sicher, dass die Schnittstelle der Netzwerkzone zugeordnet ist, und geben Sie eine größere Subnetzmaske (z. B. 0.0.0.0/0) ein. Weitere Informationen über das Konfigurieren von Hosts finden Sie in Abschnitt 6.7.10, „Hosts verwalten“.

> **HINWEIS**
> *Der VPN-Host muss vor dem Netzwerkhost spezifiziert werden, sodass das spezifischere VPN-Zonen-Subnetz zuerst geprüft werden kann.*

Im Folgenden sehen Sie einige Beispiele für mögliche Hostkonfigurationen:

Host	Interface	Subnetz	IPsec-Zone
vpn	W1ppp	192.168.1.0/24	Ja
net	W1ppp	0.0.0.0/0	Nein

7. Konfigurieren Sie Regeln mit den folgenden Parametereinstellungen für die Protokolle UDP, Authentication Header (AH) und Encapsulation Security Payload (ESP):

> **HINWEIS**
> *Das IPsec-Protokoll arbeitet am UDP-Port 500 mit den Protokollen Authentication Header (AH) und Encapsulation Security Payload (ESP). Die Firewall ist derart zu konfigurieren, dass sie diesen Verkehr übernimmt und somit das IPsec-Protokoll unterstützt.*

Aktion	Quellzone	Zielzone	Protokoll	Ziel-Port
Übernehmen	net	fw	ah	—
Übernehmen	net	fw	esp	—
Übernehmen	net	fw	udp	500

Weitere Informationen über das Konfigurieren von Regeln finden Sie in Abschnitt 6.7.14, „Regeln verwalten“.

8. Konfigurieren Sie die folgende Regel, um zu erlauben, dass Verkehr von Libreswan, dem IPSec-Daemon, die Firewall passiert.

HINWEIS
Der an der Firewall ankommende IPSec-Verkehr wird an Libreswan, den IPSec-Daemon, geleitet. Libreswan entschlüsselt den Verkehr und leitet ihn zurück zur Firewall an derselben Schnittstelle, die ihn ursprünglich empfangen hat. Eine Regel ist erforderlich, damit der Verkehr die Firewall von dieser Schnittstelle aus passieren kann.

Aktion	Quellzone	Zielzone	Protokoll	Ziel-Port
Übernehmen	vpn	loc	—	—

Weitere Informationen über das Konfigurieren von Regeln finden Sie in Abschnitt 6.7.14, „Regeln verwalten“.

Abschnitt 6.7.7

Die Firewall für ein VPN in einer entmilitarisierten Zone (DMZ) konfigurieren

Wenn die Firewall VPN-Verkehr an ein anderes Gerät weiterleiten muss, z. B. ein VPN-Gerät in einer entmilitarisierten Zone (DMZ), dann sind eine DMZ und besondere Regeln erforderlich.

Um eine Firewall für ein VPN in einer DMZ zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass eine grundlegende Firewall konfiguriert wurde. Für weitere Informationen über das Konfigurieren einer Firewall siehe Abschnitt 6.7.3, „Hinzufügen einer Firewall“.
2. Stellen Sie sicher, dass es eine Zone mit der Bezeichnung *dmz* gibt. Für weitere Informationen über das Verwalten von Zonen siehe Abschnitt 6.7.8, „Zonen verwalten“.
3. Konfigurieren Sie Regeln mit den folgenden Parametereinstellungen für die Protokolle UDP, Authentication Header (AH) und Encapsulation Security Payload (ESP):

HINWEIS
Das IPsec-Protokoll arbeitet am UDP-Port 500 mit den Protokollen Authentication Header (AH) und Encapsulation Security Payload (ESP). Die Firewall ist derart zu konfigurieren, dass sie diesen Verkehr übernimmt und somit das IPsec-Protokoll unterstützt.

Aktion	Quell-Zone	Ziel-Zone	Protokoll	Ziel-Port
Übernehmen	Net	dmz	Ah	—
Übernehmen	Net	dmz	Esp	—
Übernehmen	Net	dmz	UDP	500
Übernehmen	dmz	Net	Ah	—
Übernehmen	dmz	Net	Esp	—
Übernehmen	dmz	Net	Udp	500

Für weitere Informationen über das Konfigurieren von Regeln siehe Abschnitt 6.7.14, „Regeln verwalten“.

Abschnitt 6.7.8
Zonen verwalten

Eine Netzwerkzone ist eine Anzahl von Schnittstellen, für die Weiterleitungsentscheidungen getroffen werden. Gängige Zonen sind:

Zone	Beschreibung
Net	Das Internet
Loc	Das lokale Netzwerk
DMZ	Entmilitarisierte Zone
Fw	Die Firewall selbst
Vpn1	IPsec-Verbindungen über w1ppp
Vpn2	IPsec-Verbindungen über w2ppp

Neue Zonen können bei Bedarf hinzugefügt werden. Gehört beispielsweise jede Ethernet-Schnittstelle zum lokalen Netzwerk, wäre bei einer Sperrung des Verkehrs vom Internet zum lokalen Netzwerk der Verkehr zu allen Ethernet-Schnittstellen gesperrt. Ist der Zugriff zum Internet jedoch nur für bestimmte Ethernet-Schnittstellen erforderlich, so kann eine neue Zone für diese Schnittstellen eingerichtet werden.

INHALT

- Abschnitt 6.7.8.1, „Eine Liste der Zonen anzeigen“
- Abschnitt 6.7.8.2, „Eine Zone hinzufügen“
- Abschnitt 6.7.8.3, „Eine Zone löschen“

Abschnitt 6.7.8.1
Eine Liste der Zonen anzeigen

Um eine Liste der Zonen anzusehen, geben Sie Folgendes ein:

```
show running-config security firewall fwconfig firewall fwzone
```

Erläuterung:

- *firewall* ist die Bezeichnung der Firewall

Falls Zonen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config security firewall fwconfig fwzone
security
 firewall
  fwconfig firewall
   fwzone fw
    type        firewall
    description FirewallZone
   !
   fwzone man
    description IPv4Zone
   !
  !
 !
!
```

Falls keine Zonen konfiguriert wurden, fügen Sie je nach Bedarf Zonen hinzu. Weitere Informationen finden Sie unter Abschnitt 6.7.8.2, „Eine Zone hinzufügen“.

Abschnitt 6.7.8.2
Eine Zone hinzufügen

Um zur Firewall eine neue Zone hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie die Zone hinzu, indem Sie Folgendes eingeben:

   ```
   security firewall fwconfig firewall fwzone zone
   ```

   Erläuterung:

   - *firewall* ist die Bezeichnung der Firewall
   - *zone* ist die Bezeichnung der Zone
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
iptype { iptype }	**Zusammenfassung:** { ipv4, ipv6, ipv4ipv6 } **Standard:** ipv4 Typ des Internetprotokolls - beide verwenden, wenn keine Adressen eingesetzt sind, ansonsten IPv4- und IPv6-Regeln für jede Art von verwendeten Adressen definieren.
type46 { type46 }	**Zusammenfassung:** { ip, ipsec, firewall } **Standard:** ip Zonentypen, die sowohl für IPv4 als auch IPv6 gelten: einfache IP, Firewall oder IPSec
type6 { type6 }	**Zusammenfassung:** { ipv6, ipsec, firewall } **Standard:** ipv6 Zonentypen sind einfaches IPv6, Firewall oder IPSec
type { type }	**Zusammenfassung:** { ipv4, ipsec, firewall } **Standard:** ipv4 Zonentypen sind einfaches IPv4, Firewall oder IPSec
description { description }	**Zusammenfassung:** Eine Zeichenkette (Optional) Die Beschreibungszeichenkette für diese Zone

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 6.7.8.3
Eine Zone löschen

Um eine Zone zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die Zone, indem Sie Folgendes eingeben:

   ```
   no security firewall fwconfig firewall fwzone name
   ```

   Erläuterung:

- *firewall* ist die Bezeichnung der Firewall
- *name* ist die Bezeichnung der Zone

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 6.7.9
Schnittstellen verwalten

Firewall-Schnittstellen sind die LAN- und WAN-Schnittstellen, die für den Router verfügbar sind. Jede Schnittstelle muss sich in einer Zone des Netzwerks befinden. Unterstützt eine Schnittstelle mehr als eine Zone, muss ihre Zone als *undefined* markiert werden, und die Schnittstelle muss mit Hilfe des Host-Setups der Zone für jedes Subnetz an der Schnittstelle eine Zone definieren.

Tabelle: Beispiel

Schnittstelle	Zone
Switch.0001	Loc
Switch.0002	Loc
Switch.0003	Beliebig
Switch.0004	DMZ
W1ppp	net

INHALT

- Abschnitt 6.7.9.1, „Eine Liste der Schnittstellen anzeigen“
- Abschnitt 6.7.9.2, „Hinzufügen einer Schnittstelle“
- Abschnitt 6.7.9.3, „Eine Schnittstelle zu einer Zone zuweisen“
- Abschnitt 6.7.9.4, „Eine Broadcast-Adresse konfigurieren“
- Abschnitt 6.7.9.5, „Eine Schnittstelle löschen“

Abschnitt 6.7.9.1
Eine Liste der Schnittstellen anzeigen

Um eine Liste der Schnittstellen anzusehen, geben Sie Folgendes ein:

```
show running-config security firewall fwconfig firewall fwinterface
```

Erläuterung: *firewall* ist die Bezeichnung der Firewall.

Falls Schnittstellen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config security firewall fwconfig fwinterface
security
 firewall
  fwconfig firewall
   fwinterface fe-cm-1
    zone man
    description Interface
```

```
    !
   !
  !
 !
```

Falls keine Schnittstellen konfiguriert wurden, fügen Sie je nach Bedarf Schnittstellen hinzu. Weitere Informationen finden Sie unter Abschnitt 6.7.9.2, „Hinzufügen einer Schnittstelle“.

Abschnitt 6.7.9.2
Hinzufügen einer Schnittstelle

Um eine Schnittstelle für eine Firewall zu konfigurieren, gehen Sie wie folgt vor:

1. Zeigen Sie die Liste der verfügbaren Schnittstellen an, indem Sie Folgendes eingeben:

   ```
   show running-config ip
   ```

2. Merken Sie sich die Bezeichnung der gewählten Schnittstelle.
3. Rufen Sie den Konfigurationsmodus auf, indem Sie Folgendes eingeben:

   ```
   config
   ```

4. Fügen Sie die Schnittstelle hinzu, indem Sie Folgendes eingeben:

   ```
   security firewall fwconfig firewall fwinterface name
   ```

   Erläuterung:

   - *firewall* ist die Bezeichnung der Firewall
   - *name* ist die Bezeichnung der Schnittstelle

5. Konfigurieren Sie die Schnittstelleneinstellungen, indem Sie die folgenden Befehle eingeben:

Parameter	Beschreibung
iptype { iptype }	**Zusammenfassung:** { ipv4, ipv6, ipv4ipv6 } **Standard:** ipv4 Typ des Internetprotokolls - beide verwenden, wenn keine Adressen eingesetzt sind, ansonsten IPv4- und IPv6-Regeln für jede Art von verwendeten Adressen definieren.
description { description }	**Zusammenfassung:** Eine Zeichenkette (Optional) Die Beschreibungszeichenkette für diese Schnittstelle.

Parameter	Beschreibung
arp_filter	NUR IPv4 - Siehe zusätzliche Info. Antwortet das Gerät nur auf ARP-Anforderungen für konfigurierte IP-Adressen (Dies ist seit ROX 2.3.0 systemweit permanent aktiviert und diese Option hat keine Auswirkungen mehr).
routeback	IPv4 und IPv6 - Verkehr auf dieser Schnittstelle kann über die gleiche Schnittstelle zurückgeleitet werden.
tcpflags	IPv4 und IPv6. Illegale Kombinationen von TCP-Flags verworfen und auf der info-Ebene protokolliert.
dhcp	IPv4 und IPv6 - Ermöglicht den Ein- und Ausgang von DHCP-Datagrammen in die und aus der Schnittstelle.
norfc1918	Derzeit nicht implementiert
routefilter	IPv4 und IPv6 - Aktiviert Spoofing-Schutz "/rpfilter/"

Parameter	Beschreibung
proxyarp	NUR IPv4 - Aktiviert Proxy-ARP.
maclist	Derzeit nicht implementiert
nosmurfs	NUR IPv4 - Pakete mit einer Broadcast-Adresse als Quelle verworfen und auf der info-Ebene protokolliert.
logmartians	NUR IPv4 - Protokollierung von Paketen mit unmöglichen Quelladressen.

6. Weisen Sie die Schnittstelle einer vordefinierten Zone zu oder kennzeichnen Sie die zugewiesene Zone als undefiniert. Für weitere Informationen über das Zuweisen der Schnittstelle zu einer Zone siehe Abschnitt 6.7.9.3, „Eine Schnittstelle zu einer Zone zuweisen“.
7. Konfigurieren Sie eine Broadcast-Adresse für die Schnittstelle. Weitere Informationen über das Konfigurieren Sie eine Broadcast-Adresse finden Sie unter Abschnitt 6.7.9.4, „Eine Broadcast-Adresse konfigurieren“.
8. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 6.7.9.3
Eine Schnittstelle zu einer Zone zuweisen

Um eine Schnittstelle zu einer vordefinierten Zone zuzuweisen oder um die Zone als undefiniert zu kennzeichnen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***security » firewall » fwconfig » {firewall} » fwinterface{interface} » zone***, wobei *{firewall}* die Bezeichnung der Firewall und *{interface}* die Bezeichnung der Schnittstelle ist.
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
predefined-zone { predefined-zone }	**Zusammenfassung:** Eine Zeichenkette Eine vordefinierte Zone
undefined-zone	Dies wird zusammen mit den Definitionen der Hosts verwendet.

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 6.7.9.4
Eine Broadcast-Adresse konfigurieren

Um für eine Schnittstelle eine Broadcast-Adresse zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***security » firewall » fwconfig » {firewall} » fwinterface{interface} » broadcast-addr***, wobei *{firewall}* die Bezeichnung der Firewall und *{interface}* die Bezeichnung der Schnittstelle ist.
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
ipv4-address { ipv4-address }	**Zusammenfassung:** Eine Zeichenkette

Parameter	Beschreibung
	IPv4-Adresse für eine Broadcast-Adresse.
detect	Automatische Erkennung der Broadcast-Adresse(n).
none	Die Voreinstellung.

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 6.7.9.5
Eine Schnittstelle löschen

Um eine Schnittstelle zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie das Interface, indem Sie Folgendes eingeben:

```
no security firewall fwconfig firewall fwinterface name
```

Erläuterung:

- *`firewall`* ist die Bezeichnung der Firewall
- *`name`* ist die Bezeichnung der Schnittstelle

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 6.7.10
Hosts verwalten

Hosts dienen dazu, einzelnen Hosts oder Subnetzen (wenn die Schnittstelle mehrere Subnetze unterstützt) Zonen zuzuordnen. Die Firewall kann somit ein Paket empfangen und an das gleiche Gerät umleiten, an dem es empfangen wurde. Diese Funktionalität ist für VPN-Konfigurationen sinnvoll, um den VPN-Verkehr getrennt vom anderen Verkehr an der Schnittstelle, über die der VPN-Verkehr läuft, zu verwalten.

Tabelle: Beispiel

Zone	Schnittstelle	IP-Adresse oder Netzwerk
Local	Switch.0003	10.0.0.0/8
Guests	Switch.0003	192.168.0.0/24

INHALT

- Abschnitt 6.7.10.1, „Eine Liste der Hosts anzeigen“
- Abschnitt 6.7.10.2, „Hinzufügen eines Hosts“
- Abschnitt 6.7.10.3, „Einen Host löschen“

Abschnitt 6.7.10.1
Eine Liste der Hosts anzeigen

Um eine Liste der Hosts anzusehen, geben Sie Folgendes ein:

```
show running-config security firewall fwconfig firewall fwhost
```

Erläuterung:

- *firewall* ist die Bezeichnung der Firewall

Falls Hosts konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config security firewall fwconfig firewall1 fwhost
security
 firewall
  fwconfig firewall1
   fwhost host1
    zone      man
    interface fe-cm-1
    no ipaddress
    no description
   !
  !
 !
!
```

Falls keine Hosts konfiguriert wurden, fügen Sie je nach Bedarf Hosts hinzu. Weitere Informationen finden Sie unter Abschnitt 6.7.10.2, „Hinzufügen eines Hosts“.

Abschnitt 6.7.10.2
Hinzufügen eines Hosts

Um der Firewall einen neuen Host hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den Host hinzu, indem Sie Folgendes eingeben:

   ```
   security firewall fwconfig firewall fwhost name
   ```

   Erläuterung:

   - *firewall* ist die Bezeichnung der Firewall
   - *name* ist die Bezeichnung des Hosts
3. Konfigurieren Sie den Host, indem Sie die folgenden Befehle eingeben:

Parameter	Beschreibung
ipsec	**Zusammenfassung:** { true, false } **Standard:** false

Parameter	Beschreibung
iptype { iptype }	**Zusammenfassung:** { ipv4, ipv6, ipv4ipv6 } **Standard:** ipv4 Typ des Internetprotokolls - beide verwenden, wenn keine Adressen eingesetzt sind, ansonsten IPv4- und IPv6-Regeln für jede Art von verwendeten Adressen definieren.
zone { zone }	**Zusammenfassung:** Eine Zeichenkette Eine vordefinierte Zone

Parameter	Beschreibung
	Dieser Parameter ist obligatorisch.
interface { interface }	**Zusammenfassung:** Eine Zeichenkette Vordefinierte Schnittstelle, der optionale IPs und/oder Netzwerke hinzugefügt werden können. Dieser Parameter ist obligatorisch.
ipaddress { ipaddress }	**Zusammenfassung:** Eine Zeichenkette Zusätzliche IP-Adressen oder -Netzwerke - kommasepariert oder ein Bereich im "low.address-high.address"-Format
description { description }	**Zusammenfassung:** Eine Zeichenkette (Optional) Die Beschreibungszeichenkette für diesen Host.

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 6.7.10.3
Einen Host löschen

Um einen Host zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den Host, indem Sie Folgendes eingeben:

```
no security firewall fwconfig firewall fwhost name
```

   Erläuterung:

   - *`firewall`* ist die Bezeichnung der Firewall
   - *`name`* ist die Bezeichnung des Hosts

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 6.7.11
Verwalten von Grundregeln

Grundregeln legen die Standardaktionen beim Herstellen einer Verbindung zwischen verschiedenen Firewall-Zonen fest. Jede Grundregel besteht aus einer Quellzone, einer Zielzone und einer Aktion, die bei eingehender Verbindungsanfrage ausgeführt wird.

Das folgende Beispiel zeigt die Grundregeln für das Herstellen von Verbindungen zwischen einem lokalen Netzwerk und dem Internet.

Grundregel	Quellzone	Zielzone	Aktion
1	Loc	Net	ACCEPT
2	Net	All	DROP
3	All	All	REJECT

Jede Grundregel steuert die Verbindung zwischen der Quell- und der Zielzone. Die erste Grundregel akzeptiert alle Verbindungsanfragen vom lokalen Netzwerk zum Internet. Die zweite Grundregel legt alle Verbindungsanfragen vom Internet zu einem beliebigen Gerät im Netzwerk ab bzw. ignoriert diese. Die dritte Grundregel lehnt alle anderen Verbindungsanfragen ab und sendet ein Paket vom Typ "TCP RST" oder "ICMP destination-unreachable" an den Client.

Die Reihenfolge der Grundregeln ist wichtig. Wenn die letzte Grundregel im vorstehenden Beispiel die erste Grundregel wäre, würde die Firewall alle Verbindungsanfragen ablehnen.

HINWEIS
Quell- und Zielzone müssen konfiguriert werden, bevor eine Grundregel erstellt werden kann. Für weitere Informationen über Zonen siehe Abschnitt 6.7.8, „Zonen verwalten“.

HINWEIS
Grundregeln für bestimmte Hosts oder Datenverkehrstypen können durch Regeln aufgehoben werden. Weitere Informationen über Regeln finden Sie in Abschnitt 6.7.14, „Regeln verwalten“.

INHALT

- Abschnitt 6.7.11.1, „Eine Liste der Grundregeln anzeigen“
- Abschnitt 6.7.11.2, „Eine Regel hinzufügen“
- Abschnitt 6.7.11.3, „Die Quellzone konfigurieren“
- Abschnitt 6.7.11.4, „Die Zielzone konfigurieren“
- Abschnitt 6.7.11.5, „Eine Regel löschen“

Abschnitt 6.7.11.1

Eine Liste der Grundregeln anzeigen

Um eine Liste der Grundregeln anzusehen, geben Sie Folgendes ein:

```
show running-config security firewall fwconfig firewall fwpolicy
```

Erläuterung:

- *firewall* ist die Bezeichnung der Firewall

Falls Grundregeln konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config security firewall fwconfig firewall1 fwpolicy
security
 firewall
  fwconfig firewall1
   fwpolicy p1
    description Policy
   !
  !
 !
!
```

Falls keine Grundregeln konfiguriert wurden, fügen Sie nach Bedarf Grundregeln hinzu. Weitere Informationen finden Sie unter Abschnitt 6.7.11.2, „Eine Regel hinzufügen“.

Abschnitt 6.7.11.2
Eine Regel hinzufügen

Um für die Firewall eine Regel zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie die Regel hinzu, indem Sie Folgendes eingeben:

   ```
   security firewall fwconfig firewall fwpolicy policy
   ```

   Erläuterung:

   - *firewall* ist die Bezeichnung der Firewall
   - *policy* ist die Bezeichnung der Regel
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
iptype { iptype }	**Zusammenfassung:** { ipv4, ipv6, ipv4ipv6 } **Standard:** ipv4 Typ des Internetprotokolls - beide verwenden, wenn keine Adressen eingesetzt sind, ansonsten IPv4- und IPv6-Regeln für jede Art von verwendeten Adressen definieren.
policy { policy }	**Zusammenfassung:** { accept, drop, reject, continue } **Standard:** reject Ein Standardvorgang zum Verbindungsaufbau zwischen unterschiedlichen Zonen.
log-level { log-level }	**Zusammenfassung:** { none, debug, info, notice, warning, error, critical, alert, emergency } **Standard:** none (Optional) Bestimmt, ob Protokollierung stattfindet und auf welcher Ebene.
description { description }	**Zusammenfassung:** Eine Zeichenkette (Optional) Die Beschreibungszeichenkette für diese Grundregel.

4. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 6.7.11.3
Die Quellzone konfigurieren

Um die Quellzone für eine Firewall-Regel zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***security » firewall » fwconfig » {firewall} » fwpolicy » {policy} » source-zone***, wobei *{firewall}* die Bezeichnung der Firewall und *{policy}* die Bezeichnung der Regel ist.
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
predefined-zone { predefined-zone }	**Zusammenfassung:** Eine Zeichenkette
all	

4. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 6.7.11.4
Die Zielzone konfigurieren

Um die Zielzone für eine Firewall-Grundregel zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
predefined-zone { predefined-zone }	**Zusammenfassung:** Eine Zeichenkette
all	

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 6.7.11.5
Eine Regel löschen

Um eine Regel zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die Regel, indem Sie Folgendes eingeben:

```
no security firewall fwconfig firewall fwpolicy policy
```

Erläuterung:

- *`firewall`* ist die Bezeichnung der Firewall
- *`policy`* ist die Bezeichnung der Regel

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 6.7.12
NAT-Einstellungen verwalten

Mit Hilfe von NAT-Einträgen kann eine 1:1-Entsprechung zwischen einer externen Adresse auf der Firewall und der RFC1918-Adresse eines Hosts hinter der Firewall festgelegt werden. Dies wird häufig genutzt, um Verbindungen zu einem internen Server von außerhalb des Netzwerks zu ermöglichen.

HINWEIS
DNAT (Destination Network Address Translation) kann durch Konfigurieren der Zielzone in einer Regel eingerichtet werden. Weitere Informationen über Regeln finden Sie unter Abschnitt 6.7.14, „Regeln verwalten“.

INHALT

- Abschnitt 6.7.12.1, „Eine Liste der NAT-Einstellungen anzeigen“
- Abschnitt 6.7.12.2, „Hinzufügen einer NAT-Einstellung“
- Abschnitt 6.7.12.3, „Eine NAT-Einstellung löschen“

Abschnitt 6.7.12.1

Eine Liste der NAT-Einstellungen anzeigen

Um eine Liste der NAT-Einstellungen anzuzeigen, geben Sie Folgendes ein:

```
show running-config security firewall firewall fwnat
```

Erläuterung:

- *firewall* ist die Bezeichnung der Firewall

Falls NAT-Einstellungen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config security firewall fwconfig firewall1 fwnat
security
 firewall
  fwconfig firewall1
   fwnat n1
    external-addr 172.30.150.10
    interface     fe-cm-1
    internal-addr 192.168.1.100
    no description
   !
   fwnat fwmasq
    external-addr 172.30.159.5
    interface     fe-cm-1
    internal-addr 193.168.1.1
    no description
   !
  !
 !
!
```

Falls keine NAT-Einstellungen konfiguriert wurden, fügen Sie je nach Bedarf NAT-Einstellungen hinzu. Weitere Informationen finden Sie unter Abschnitt 6.7.12.2, „Hinzufügen einer NAT-Einstellung“.

Abschnitt 6.7.12.2

Hinzufügen einer NAT-Einstellung

Um einen Netzadressenübersetzungs-(NAT)-Eintrag zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den Eintrag hinzu, indem Sie Folgendes eingeben:

   ```
   security firewall fwconfig firewall fwnat name
   ```

   Erläuterung:

   - *firewall* ist die Bezeichnung der Firewall
   - *name* ist die Bezeichnung des NAT-Eintrags
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
external-addr { external-addr }	**Zusammenfassung:** Eine Zeichenkette Die externe IP-Adresse. Die Adresse darf kein DNS-Name sein. Externe IP-Adressen müssen der Schnittstelle manuell hinzugefügt werden. Dieser Parameter ist obligatorisch.

Parameter	Beschreibung
interface { interface }	**Zusammenfassung:** Eine Zeichenkette Eine Schnittstelle mit einer externen IP-Adresse. Dieser Parameter ist obligatorisch.
ipalias	IP-Alias für NAT-Regel erstellen.
internal-addr { internal-addr }	**Zusammenfassung:** Eine Zeichenkette Interne IP-Adresse. Die Adresse darf kein DNS-Name sein. Dieser Parameter ist obligatorisch.
limit-interface	Übersetzung nur von der festgelegten Schnittstelle aus wirksam.
local	Übersetzung vom Firewall-System aus wirksam.
description { description }	**Zusammenfassung:** Eine Zeichenkette (Optional) Die Beschreibungszeichenkette für diesen NAT-Eintrag.

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 6.7.12.3
Eine NAT-Einstellung löschen

Um einen NAT-Eintrag zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den Eintrag, indem Sie Folgendes eingeben:

```
no security firewall fwconfig firewall fwnat name
```

Erläuterung:

- *`firewall`* ist die Bezeichnung der Firewall
- *`name`* ist die Bezeichnung des NAT-Eintrags

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 6.7.13
Maskierungs- oder SNAT-Einstellungen verwalten

Maskierung und SNAT (Source Network Address Translation) sind Formen der dynamischen Netzwerkadressenübersetzung NAT (Network Address Translation). Beide verbergen ein Subnetzwerk hinter einer einzigen öffentlichen IP-Adresse.

Maskierung wird verwendet, wenn der ISP eine dynamische IP-Adresse bereitstellt. SNAT wird verwendet, wenn der ISP eine statische IP-Adresse bereitstellt.

INHALT

- Abschnitt 6.7.13.1, „Eine Liste der Maskierungs- oder SNAT-Einstellungen anzeigen“
- Abschnitt 6.7.13.2, „Hinzufügen von Maskierungs- oder SNAT-Einstellungen“

- Abschnitt 6.7.13.3, „Eine Maskierungs- oder SNAT-Einstellung löschen“

Abschnitt 6.7.13.1
Eine Liste der Maskierungs- oder SNAT-Einstellungen anzeigen

Um eine Liste der Maskierungs- oder SNAT-Einstellungen anzuzeigen, geben Sie Folgendes ein:

```
show running-config security firewall fwconfig firewall fwmasq
```

Erläuterung:

- *firewall* ist die Bezeichnung der Firewall

Falls Maskierungs- oder SNAT-Einstellungen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config security firewall fwconfig firewall2 fwmasq
security
 firewall
  fwconfig firewall2
   fwmasq SNAT
    out-interface fe-cm-1
    no out-interface-specifics
    source-hosts  192.168.1.0/24
    address       172.30.15.10
    no description
   !
   fwmasq Masq
    out-interface fe-cm-1
    no out-interface-specifics
    source-hosts  192.168.0.0/24
    no address
    no description
   !
  !
 !
!
```

Falls keine Maskierungs- oder SNAT-Einstellungen konfiguriert wurden, fügen Sie je nach Bedarf Maskierungs- oder SNAT-Einstellungen hinzu. Weitere Informationen finden Sie unter Abschnitt 6.7.13.2, „Hinzufügen von Maskierungs- oder SNAT-Einstellungen“.

Abschnitt 6.7.13.2
Hinzufügen von Maskierungs- oder SNAT-Einstellungen

Um Maskierungs- oder SNAT-Regeln hinzuzufügen, gehen Sie wie folgt vor:

HINWEIS
Die Maskierung setzt voraus, dass die zum Maskieren verwendete IP-Adresse zum Router gehören muss. Beim Konfigurieren der SNAT-Adresse während der Maskierung muss die SNAT-Adresse eine der IP-Adressen an der OUT-Schnittstelle sein.

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie die Maskierungs- oder SNAT-Einstellung hinzu, indem Sie Folgendes eingeben:

   ```
   security firewall fwconfig firewall fwmasq name
   ```

   Erläuterung:

- *firewall* ist die Bezeichnung der Firewall
- *name* ist die Bezeichnung der Maskierungs- oder SNAT-Einstellung

3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
iptype { iptype }	**Zusammenfassung:** { ipv4, ipv6, ipv4ipv6 } **Standard:** ipv4 Typ des Internetprotokolls - beide verwenden, wenn keine Adressen eingesetzt sind, ansonsten IPv4- und IPv6-Regeln für jede Art von verwendeten Adressen definieren.
out-interface { out-interface }	**Zusammenfassung:** Eine Zeichenkette Eine Liste ausgehender Schnittstellen - gewöhnlich die Internet-Schnittstelle. Dieser Parameter ist obligatorisch.
out-interface-specifics { out-interface-specifics }	**Zusammenfassung:** Eine Zeichenkette (Optional) Eine Liste ausgehender Schnittstellen- spezifischer IP-Ziele für die ausgehende Schnittstelle.
ipalias	IP-Alias für NAT-Regel erstellen.
source-hosts { source-hosts }	**Zusammenfassung:** Eine Zeichenkette Subnetzbereich oder mit Kommata getrennte Liste der Hosts (IPs) Dieser Parameter ist obligatorisch.
address { address }	**Zusammenfassung:** Eine Zeichenkette (Optional) Wenn hier eine Adresse angegeben wird, wird SNAT verwendet und wird die Quelladresse sein.
description { description }	**Zusammenfassung:** Eine Zeichenkette (Optional) Die Beschreibungszeichenkette für diesen masq-Eintrag.

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 6.7.13.3
Eine Maskierungs- oder SNAT-Einstellung löschen

Um eine Maskierungs- oder SNAT-Einstellung zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die Maskierungs- oder SNAT-Einstellung, indem Sie Folgendes eingeben:

```
no security firewall fwconfig firewall fwmasq name
```

Erläuterung:

- *firewall* ist die Bezeichnung der Firewall
- *name* ist die Bezeichnung der Maskierungs- oder SNAT-Einstellung

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 6.7.14

Regeln verwalten

Regeln legen Ausnahmen von den Standardregeln der Firewall für bestimmte Verkehrstypen, Quellen oder Ziele fest. Jede Regel legt bestimmte Kriterien fest. Wenn ein eingehendes Paket diese Kriterien erfüllt, werden die Standard-Regeln übergangen und die mit der Regel festgelegte Aktion ausgeführt.

INHALT

- Abschnitt 6.7.14.1, „Eine Liste der Regeln anzeigen“
- Abschnitt 6.7.14.2, „Eine Regel hinzufügen“
- Abschnitt 6.7.14.3, „Die Quellzone konfigurieren“
- Abschnitt 6.7.14.4, „Die Zielzone konfigurieren“
- Abschnitt 6.7.14.5, „Eine Regel löschen“

Abschnitt 6.7.14.1

Eine Liste der Regeln anzeigen

Um eine Liste der Regeln anzusehen, geben Sie Folgendes ein:

```
show running-config security firewall fwconfig firewall fwrule
```

Erläuterung:

- *`firewall`* ist die Bezeichnung der Firewall

Falls Regeln konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config security firewall fwconfig firewall1 fwrule
security
 firewall
  fwconfig firewall1
   fwrule Rule1
    action accept
    source-zone man
    destination-zone man
    no description
   !
   fwrule Rule2
    action accept
    source-zone man
    destination-zone man
    no description
   !
  !
 !
!
```

Falls keine Regeln konfiguriert wurden, fügen Sie je nach Bedarf Regeln hinzu. Weitere Informationen finden Sie unter Abschnitt 6.7.14.2, „Eine Regel hinzufügen“.

Abschnitt 6.7.14.2
Eine Regel hinzufügen

Um eine Regel für eine Firewall zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie die Regel hinzu, indem Sie Folgendes eingeben:

```
security firewall fwconfig firewall fwrule rule
```

   Erläuterung:

   - *firewall* ist die Bezeichnung der Firewall
   - *rule* ist die Bezeichnung der Regel

3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

HINWEIS
Bei der Anwendung neuer Regeln wird für den Router sichtbarer früherer Verkehr möglicherweise noch als Verkehr mit gültigen Verbindungen gemäß Verbindungsverfolgungs-Tabelle betrachtet. Beispiel:

a. Eine Regel für die Protokolle TCP und UDP wird angewandt.

b. Der Router erkennt sowohl den TCP- als auch den UDP-Datenverkehr, die sich für NAT qualifizieren.

c. Die Regel wird anschließend so modifiziert, dass nur UDP zugelassen wird.

d. Der Router erkennt noch immer TCP-Pakete (d.h. Pakete der erneuten Übertragung).

Starten Sie den Router bei Bedarf neu, um alle vorhandenen Verbindungsströme zu entfernen.

Parameter	Beschreibung
iptype { iptype }	**Zusammenfassung:** { ipv4, ipv6, ipv4ipv6 } **Standard:** ipv4 Typ des Internetprotokolls - beide verwenden, wenn keine Adressen eingesetzt sind, ansonsten IPv4- und IPv6-Regeln für jede Art von verwendeten Adressen definieren.
action { action }	**Zusammenfassung:** { accept, drop, reject, continue, redirect, dnat-, dnat } **Standard:** reject Die letztliche Aktion für eingehende Pakete, die die Regel erfüllen.
source-zone-hosts { source-zone-hosts }	**Zusammenfassung:** Eine Zeichenkette (Optional) Kommaseparierte Host-IPs zu einer vorgegebenen Quellzone hinzufügen.
destination-zone-hosts { destination-zone-hosts }	**Zusammenfassung:** Eine Zeichenkette (Optional) Kommaseparierte Host-IPs zu einer vorgegebenen Zielzone hinzufügen - kann ":port" für DNAT oder REDIRECT enthalten.
log-level { log-level }	**Zusammenfassung:** { none, debug, info, notice, warning, error, critical, alert, emergency } **Standard:** none (Optional) Bestimmt, ob Protokollierung stattfindet und auf welcher Ebene.
protocol { protocol }	**Zusammenfassung:** { tcp, udp, icmp, all } oder eine Zeichenkette **Standard:** all Protokoll, das diese Regel erfüllen muss.
source-ports { source-ports }	**Zusammenfassung:** Eine Zeichenkette **Standard:** none

Parameter	Beschreibung
	(Optional) Der/Die TCP/UDP-Port(s), von dem/denen die Verbindung hergestellt wurde. Default: alle Ports. Einen einzelnen Port oder eine Liste kommaseparierter Ports hinzufügen
destination-ports { destination-ports }	**Zusammenfassung:** Eine Zeichenkette **Standard:** none (Optional) Der/Die TCP/UDP-Port(s), zu dem/denen die Verbindung aufgebaut wurde. Default: alle Ports. Einen einzelnen Port oder eine Liste kommaseparierter Ports hinzufügen
original-destination { original-destination }	**Zusammenfassung:** { None } oder eine Zeichenkette **Standard:** none (Optional) Die IP-Zieladresse in der Verbindungsanforderung, die von der Firewall empfangen wurde.
description { description }	**Zusammenfassung:** Eine Zeichenkette (Optional) Die Beschreibungszeichenkette für diese Regel.

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 6.7.14.3
Die Quellzone konfigurieren

Um die Quellzone für eine Firewall-Regel zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***security » firewall » fwconfig » {firewall} » fwrule{rule} » source-zone***, wobei *{firewall}* die Bezeichnung der Firewall und *{rule}* die Bezeichnung der Regel ist.
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
predefined-zone { predefined-zone }	**Zusammenfassung:** Eine Zeichenkette Eine vordefinierte Zone
other { other }	**Zusammenfassung:** Eine Zeichenkette Benutzerspezifische Definition eingeben - kann eine kommaseparierte Liste der Zonen sein.
all	Alle Zonen

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 6.7.14.4
Die Zielzone konfigurieren

Um die Zielzone für eine Firewall-Regel zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
predefined-zone { predefined-zone }	**Zusammenfassung:** Eine Zeichenkette Eine vordefinierte Zone
other { other }	**Zusammenfassung:** Eine Zeichenkette Eine undefinierte Zone (Zeichenkette).
all	Alle Zonen

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 6.7.14.5
Eine Regel löschen

Um eine Regel zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die Regel, indem Sie Folgendes eingeben:

```
no security firewall fwconfig firewall fwrule rule
```

Erläuterung:

- *`firewall`* ist die Bezeichnung der Firewall
- *`rule`* ist die Bezeichnung der Regel

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 6.7.15
Eine Firewall-Konfiguration überprüfen

Um eine Firewall-Konfiguration zu überprüfen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Legen Sie die Firewall als Arbeitskonfiguration fest durch Eingabe von:

```
security firewall work-config name
```

Erläuterung:

- *`name`* ist die Bezeichnung der Firewall-Konfiguration

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern. Das System prüft die Firewall-Konfiguration und zeigt die Ergebnisse an.

Abschnitt 6.7.16
Eine Firewall aktivieren/deaktivieren

Um eine Firewall zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

WICHTIG!
Beim Aktivieren oder Deaktivieren wird der Schutzmechanismen vor Brute-Force-Angriffen zurückgesetzt - aber nicht deaktiviert, sofern er er zuvor aktiviert war. Alle Hosts, die zuvor blockiert wurden, können sich wieder anmelden. Wenn mehrere Hosts gleichzeitig aktiv angreifen, kann dies zu einer verminderten Systemleistung führen.

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Aktivieren Sie die Firewall, indem Sie Folgendes eingeben:

   ```
   security firewall enable
   ```

   Oder deaktivieren Sie die Firewall, indem Sie dem Befehl *no* voranstellen:

   ```
   no security firewall enable
   ```

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

7 IP-Adresszuweisung

Dieses Kapitel beschreibt Funktionen in Verbindung mit der Zuweisung von IP-Adressen, wie DHCP und DNS.

INHALT

- Abschnitt 7.1, „IP-Adressen für routingfähige Schnittstellen verwalten“
- Abschnitt 7.2, „Verwalten des DHCP Relay Agent (IPv4)“
- Abschnitt 7.3, „Den DHCP-Server verwalten“
- Abschnitt 7.4, „Statische DNS verwalten“
- Abschnitt 7.5, „Dynamic DNS (DDNS) verwalten“

Abschnitt 7.1

IP-Adressen für routingfähige Schnittstellen verwalten

Dieser Abschnitt beschreibt, wie Sie IP-Adressen für routingfähige Schnittstellen verwalten können.

INHALT

- Abschnitt 7.1.1, „Kalkulation für routingfähige Schnittstellen konfigurieren“
- Abschnitt 7.1.2, „Statistiken für routingfähige Schnittstellen anzeigen“
- Abschnitt 7.1.3, „IPv4-Adressen verwalten“
- Abschnitt 7.1.4, „IPv6-Adressen verwalten“
- Abschnitt 7.1.5, „Konfigurieren der IPv6 Neighbor Discovery“
- Abschnitt 7.1.6, „IPv6-Netzwerkpräfixe verwalten“

Abschnitt 7.1.1

Kalkulation für routingfähige Schnittstellen konfigurieren

Um die Kalkulation für routingfähige Schnittstellen zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Stellen Sie die Kalkulation durch folgende Eingabe ein:

   ```
   ip interface bandwidth cost
   ```

   Erläuterung:

- *interface* ist die Bezeichnung der routingfähigen Schnittstelle
- *cost* ist der in den Selbstkostenberechnungen verwendete Wert für die routingfähige logische Schnittstelle, in Kbaud

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.1.2
Statistiken für routingfähige Schnittstellen anzeigen

Um die grundlegenden Statistiken für alle routingfähigen Schnittstellen anzuzeigen, geben Sie Folgendes ein:

```
show interfaces ip
```

Eine Tabelle oder Liste ähnlich dem folgenden Beispiel wird angezeigt:

```
ruggedcom# show interfaces ip
interfaces ip dummy0
 admin state down
 state       down
 pointopoint false
 receive
  bytes   0
  packets 0
  errors  0
  dropped 0
 transmit
  bytes      0
  packets    0
  errors     0
  dropped    0
  collisions 0
interfaces ip fe-cm-1
.
.
.
```

Diese Tabelle oder Liste liefert die folgenden Informationen:

Parameter	Beschreibung
admin-state	**Zusammenfassung:** { not set, up, down, testing, unknown, dormant, notPresent, lowerLayerDown } Der Verwaltungszustand des Ports. Dieser Parameter ist obligatorisch.
state	**Zusammenfassung:** { not set, up, down, testing, unknown, dormant, notPresent, lowerLayerDown } Zeigt, ob die Verbindung verfügbar ("up") oder nicht verfügbar ("down") ist. Dieser Parameter ist obligatorisch.
pointopoint	**Zusammenfassung:** { true, false } Die Punkt-zu-Punkt-Verbindung. Dieser Parameter ist obligatorisch.
bytes	**Zusammenfassung:** Eine vorzeichenlose 64-Bit-Ganzzahl Die Anzahl empfangener Bytes. Dieser Parameter ist obligatorisch.

Parameter	Beschreibung
packets	**Zusammenfassung:** Eine vorzeichenlose 64-Bit-Ganzzahl Die Anzahl der empfangenen Pakete. Dieser Parameter ist obligatorisch.
errors	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl der empfangenen Fehler-Pakete. Dieser Parameter ist obligatorisch.
dropped	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl der Pakete, die vom empfangenden Gerät verworfen wurden. Dieser Parameter ist obligatorisch.
bytes	**Zusammenfassung:** Eine vorzeichenlose 64-Bit-Ganzzahl Die Anzahl übertragener Bytes. Dieser Parameter ist obligatorisch.
packets	**Zusammenfassung:** Eine vorzeichenlose 64-Bit-Ganzzahl Die Anzahl der übertragenen Pakete. Dieser Parameter ist obligatorisch.
errors	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl der übertragenen Fehler-Pakete. Dieser Parameter ist obligatorisch.
dropped	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl der Pakete, die vom übertragenden Gerät verworfen wurden. Dieser Parameter ist obligatorisch.
collisions	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl der Collisions, die am Port erkannt wurden. Dieser Parameter ist obligatorisch.

Abschnitt 7.1.3

IPv4-Adressen verwalten

Dieser Abschnitt beschreibt, wie Sie IPv4-Adressen für routingfähige Schnittstellen verwalten können.

INHALT

- Abschnitt 7.1.3.1, „Eine Liste der IPv4-Adressen anzeigen“
- Abschnitt 7.1.3.2, „Eine IPv4-Adresse hinzufügen“
- Abschnitt 7.1.3.3, „Eine IPv4-Adresse löschen“

Abschnitt 7.1.3.1

Eine Liste der IPv4-Adressen anzeigen

Um eine Liste der IPv4-Adressen für eine routingfähige Schnittstelle anzusehen, geben Sie Folgendes ein:

```
show running-config ip interface ipv4
```

Erläuterung:

- *interface* ist die Bezeichnung der Schnittstelle

Falls Adressen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config ip ipv4 | tab
IFNAME       IPADDRESS         PEER
-------------------------------------
dummy0
             1.1.1.1/32        -
fe-cm-1
             192.168.0.12/24   -
             172.30.150.12/19  -
switch.0001
switch.0011
             192.168.11.1/24   -
switch.0012
             192.168.12.1/24   -
switch.0014
             192.168.14.1/24   -
```

Falls keine Adressen konfiguriert wurden, fügen Sie je nach Bedarf Adressen hinzu. Weitere Informationen finden Sie unter Abschnitt 7.1.3.2, „Eine IPv4-Adresse hinzufügen“.

Abschnitt 7.1.3.2
Eine IPv4-Adresse hinzufügen

Um eine IPv4-Adresse zu einer routingfähigen Schnittstelle hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie die Adresse hinzu, indem Sie Folgendes eingeben:

   ```
   ip interface ipv4 address address peer peer
   ```

   Erläuterung:

   - *interface* ist die Bezeichnung der Schnittstelle
   - *address* ist die IPv4-Adresse und das Präfix
   - *peer* ist die Peer-IPv4-Adresse
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.1.3.3
Eine IPv4-Adresse löschen

Um eine IPv4-Adresse für eine routingfähige Schnittstelle zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die Adresse, indem Sie Folgendes eingeben:

   ```
   no ip interface ipv4 address address
   ```

   Erläuterung:

   - *address* ist die IPv4-Adresse

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.1.4
IPv6-Adressen verwalten

Dieser Abschnitt beschreibt, wie Sie IPv6-Adressen für routingfähige Schnittstellen verwalten können.

INHALT

- Abschnitt 7.1.4.1, „Eine Liste der IPv6-Adressen anzeigen“
- Abschnitt 7.1.4.2, „Eine IPv6-Adresse hinzufügen“
- Abschnitt 7.1.4.3, „Eine IPv6-Adresse löschen“

Abschnitt 7.1.4.1
Eine Liste der IPv6-Adressen anzeigen

Um eine Liste der IPv6-Adressen für eine routingfähige Schnittstelle anzusehen, geben Sie Folgendes ein:

```
show running-config ip interface ipv6 address
```

Erläuterung:

- *`interface`* ist die Bezeichnung der Schnittstelle

Falls Adressen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config ip dummy0 ipv6 address
ip dummy0
 ipv6
  address 2001:db8:a0b:12f0::1/24
  !
  address 2001:db9:a2C:25f0::2/24
  !
 !
!
```

Falls keine Adressen konfiguriert wurden, fügen Sie je nach Bedarf Adressen hinzu. Weitere Informationen finden Sie unter Abschnitt 7.1.4.2, „Eine IPv6-Adresse hinzufügen“.

Abschnitt 7.1.4.2
Eine IPv6-Adresse hinzufügen

Um eine IPv6-Adresse zu einer routingfähigen Schnittstelle hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie die Adresse hinzu, indem Sie Folgendes eingeben:

   ```
   ip interface ipv6 address address
   ```

   Erläuterung:

   - *`interface`* ist die Bezeichnung der Schnittstelle

- *address* ist die IPv6-Adresse

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.1.4.3
Eine IPv6-Adresse löschen

Um eine IPv6-Adresse für eine routingfähige Schnittstelle zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die Adresse, indem Sie Folgendes eingeben:

```
no ip interface ipv6 address address
```

Erläuterung:

- *interface* ist die Bezeichnung der Schnittstelle
- *address* ist die IPv6-Adresse

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.1.5
Konfigurieren der IPv6 Neighbor Discovery

Das Neighbor-Discovery-(ND)-Protokoll dient in IPv6 als Ersatz für IPv4 ARP-Nachrichten. Das Protokoll nutzt ICMPv6-Nachrichten für unterschiedliche Zwecke, einschließlich:

- Finden einer Link-Layer-Adresse eines Nachbarn
- Erkennen benachbarter Router
- Feststellen von Änderungen in der Link-Layer-Adresse
- Feststellen eines Ausfalls eines Nachbarn
- Senden von Netzwerkinformationen von Routern an Hosts, dazu gehören Hop-Grenze, MTU-Größe, Bestimmung des an einer Verbindung verwendeten Netzwerkpräfixes, automatische Adressenkonfiguration und Informationen zur Standardroute.

Das Neighbor-Discovery-Protokoll nutzt fünf Arten von ICMPv6-Nachrichten:

- **Router Solicitation (ICMPv6-Typ 133)**

  Diese Nachricht wird von Hosts als Anfrage für eine Router-Advertisement-Nachricht an Router gesendet. Sie verwendet eine Multicast-Zieladresse (z. B. FF02:2).

- **Router-Advertisement-Nachrichten (ICMPv6-Typ 134)**

  Diese Nachricht wird von Routern verwendet, um die eigene Existenz in einem Netzwerk anzukündigen. Diese Nachricht umfasst Netzwerkinformationen im Zusammenhang mit IPv6-Präfixen, Standardroute, MTU-Größe, Hop-Limit und Autokonfigurationsmerker. Sie verwendet eine Multicast-Zieladresse (z. B. FF02:1).

- **Neighbor-Solicitation-Nachrichten (ICMPv6-Typ 135)**

  Diese Nachricht wird von Hosts gesendet, um die Existenz eines anderen Hosts auf derselben Verbindung festzustellen. Ziel ist es, die Link-Layer eines benachbarten Knoten zu finden.

- **Neighbor-Advertisement-Nachrichten (ICMPv6-Typ 136)**

  Diese Nachricht wird von Hosts gesendet, um die Existenz eines Hosts anzuzeigen, und enthält Informationen über die eigene Link-Layer-Adresse.

- **Redirect-Nachrichten (ICMPv6-Typ 137)**

  Diese Nachricht wird von einem Router gesendet, um einen Host über einen besseren Router zum Erreichen einer bestimmten Zieladresse zu informieren.

Neighbor Discovery muss an allen für IPv6 aktivierten Ethernet-Schnittstellen konfiguriert sein.

Um Einstellungen für IPv6 Neighbor Discovery zu aktivieren und zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Geben Sie den folgenden Befehl ein:

   ```
   ip interface ipv6 nd
   ```

   Erläuterung:

   - *interface* ist die Bezeichnung der Schnittstelle
3. Konfigurieren Sie das Neighbor Discovery, indem Sie je nach Bedarf den/die folgenden Parameter konfigurieren:

Parameter	Beschreibung
enable-ra	Aktivieren, um Router-Ankündigungen zu senden.
adv-interval-option	Beinhaltet eine Option "Advertisement Interval", die den Hosts die maximale Zeit in Millisekunden zwischen aufeinanderfolgenden unaufgeforderten Router-Ankündigungen anzeigt.
home-agent-config-flag	Stellt die Flag in der IPv6-Router-Ankündigung ein/aus, die den Hosts anzeigt, dass der Router als Home Agent fungiert und eine Home Agent-Option enthält.
home-agent-lifetime { home-agent-lifetime }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 0 und 65520 **Standard:** 1800 Der in der Home Agent-Option einzugebende Wert, sofern die Flag zur Konfiguration des Home Agent eingestellt ist, der die Lebensdauer des Home Agent zu den Hosts anzeigt. Ein Wert von "0" bedeutet, dass ein Lebensdauer-Wert des Routers einzugeben ist.
home-agent-preference { home-agent-preference }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 0 und 65535 **Standard:** 0 Der in der Home Agent-Option einzugebende Wert, sofern die Flag zur Konfiguration des Home Agent eingestellt ist, der die Einstellungen des Home Agent zu den Hosts anzeigt.
managed-config-flag	Die Flag in IPv6-Router-Ankündigungen, die den Hosts anzeigt, dass sie das verwaltete (zustandsorientierte) Protokoll für die Autokonfiguration von Adressen verwenden sollen, zusätzlich zu allen Adressen, die über Autokonfiguration für zustandslose Adressen konfiguriert wurden.
other-config-flag	Die Flag in IPv6-Router-Ankündigungen, die den Hosts anzeigt, dass sie das verwaltete (zustandsorientierte) Protokoll verwenden sollen, um andere Autokonfigurationsinformationen als Adressen zu erhalten.
ra-lifetime { ra-lifetime }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 0 und 9000 **Standard:** 1800 Der Wert (in Sekunden), der in das Feld "Router Lifetime" der von der Schnittstelle gesendeten Router-Ankündigungen einzugeben ist. Zeigt die Nützlichkeit des Routers als Standard-Router an dieser Schnittstelle an. Den Wert auf Null zu setzen, bedeutet, dass der Router nicht als Standard-Router an dieser Schnittstelle in Betracht kommt. Der Wert muss entweder Null sein oder zwischen dem Wert, der mit dem "IPv6 nd ra-interval" (oder Standardwert) festgelegt ist, und 9000 Sekunden liegen.

Parameter	Beschreibung
reachable-time-msec { reachable-time-msec }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 0 und 3600000 **Standard:** 0 Der Wert (in Millisekunden), der in das Feld "Reachable Time" in den vom Router gesendeten Router-Ankündigungen einzugeben ist. Die konfigurierte Zeit ermöglicht es dem Router, nicht verfügbare Nachbarn zu erkennen. Der Wert Null steht für unspezifiziert (durch diesen Router).

4. Konfigurieren Sie das Router-Advertisement-Intervall, indem Sie je nach Bedarf den/die folgenden Parameter konfigurieren:

Parameter	Beschreibung
value { value }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 3 und 1800 Der Intervallwert. **HINWEIS** *Der Wert kann nicht spezifiziert werden, wenn die Einheit nicht ebenfalls spezifiziert ist.*
unit { unit }	**Zusammenfassung:** { sec, msec } Die Intervalleinheit. **HINWEIS** *Die Einheit kann nicht spezifiziert werden, wenn der Wert nicht ebenfalls spezifiziert ist.*

5. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.1.6
IPv6-Netzwerkpräfixe verwalten

Eine IPv6-fähige Schnittstelle kann mit der Neighbor-Discovery-Funktion ihrem Nachbarn auf der gleichen Verbindung IPv6-Netzwerkpräfixe mitteilen.

INHALT

- Abschnitt 7.1.6.1, „Hinzufügen eines IPv6-Netzwerkpräfixes“
- Abschnitt 7.1.6.2, „Ein Ipv6-Netzwerkpräfix löschen“

Abschnitt 7.1.6.1
Hinzufügen eines IPv6-Netzwerkpräfixes

Um ein Netzwerkpräfix aus der Neighbor-Discovery-Konfiguration für eine IPv6-Adresse hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie das Netzwerkpräfix hinzu, indem Sie Folgendes eingeben:

```
ip interface ipv6 nd prefix prefix
```

Erläuterung:

- *interface* ist die Bezeichnung der Schnittstelle
- *prefix* ist die IPv6-Adresse und das Präfix

3. Konfigurieren Sie die Lifetime-Einstellungen mithilfe der folgenden Parameter:

Parameter	Beschreibung
valid { valid }	**Zusammenfassung:** { infinite } oder eine vorzeichenlose 32-Bit-Ganzzahl zwischen 0 und 4294967295 Die Zeitdauer in Sekunden, während der das Präfix für die Bestimmung des "on-link" gültig ist. **HINWEIS** *Die gültige Lebensdauer kann nicht konfiguriert werden, wenn die bevorzugte Lebensdauer nicht konfiguriert ist.*
preferred { preferred }	**Zusammenfassung:** { infinite } oder eine vorzeichenlose 32-Bit-Ganzzahl zwischen 0 und 4294967295 Die Zeitdauer in Sekunden, während der von dem Präfix generierte Adressen bevorzugt bleiben. **HINWEIS** *Die bevorzugte Lebensdauer kann nicht konfiguriert werden, wenn die gültige Lebensdauer nicht konfiguriert ist.*

4. Konfigurieren Sie die Präfix-Einstellungen mithilfe der folgenden Parameter:

Parameter	Beschreibung
off-link	Zeigt an, dass die Ankündigung keine Angabe über "on-link"- oder "off-link"-Eigenschaften des Präfixes macht.
no-autoconfig	Zeigt den Hosts auf der lokalen Verbindung an, dass das festgelegte Präfix nicht für die IPv6-Autokonfiguration verwendet werden kann.
router-address	Zeigt den Hosts auf der lokalen Verbindung an, dass das festgelegte Präfix bei Einstellung der R-Flag eine vollständige IP-Adresse enthält. **HINWEIS** *Die Router-Adresse kann nicht festgelegt werden, sofern nicht "off-link" oder "no-autoconfig" eingestellt sind.*

5. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.1.6.2

Ein Ipv6-Netzwerkpräfix löschen

Um ein Netzwerkpräfix aus der Neighbor Discovery-Konfiguration für eine IPv6-Adresse zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die Adresse, indem Sie Folgendes eingeben:

```
no ip interface ipv6 address address
```

Erläuterung:

- *interface* ist die Bezeichnung der Schnittstelle
- *address* ist die IPv6-Adresse

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.2

Verwalten des DHCP Relay Agent (IPv4)

Ein DHCP Relay Agent ist eine Komponente, die DHCP-Pakete zwischen Clients und Servern weiterleitet, wenn diese sich nicht auf demselben physischen LAN-Segment oder IP-Subnetz befinden. Diese Funktion wird aktiviert, wenn die IP-Adresse des DHCP-Servers und eine Reihe von Zugangsports konfiguriert werden.

Die DHCP-Option 82 bietet einen Mechanismus für die Zuweisung einer IP-Adresse in Abhängigkeit vom Standort des Client-Geräts im Netzwerk. Informationen über den Client-Standort können zusammen mit der DHCP-Anfrage an den Server gesendet werden. Anhand dieser Informationen trifft der DHCP-Server eine Entscheidung über die zuzuweisende IP-Adresse.

Der DHCP Relay Agent nimmt die übertragenen DHCP-Anfragen von den Clients, die am konfigurierten Zugangsport empfangen wurden, und fügt die Relay-Agent-Informationsoption (Option 82) in das Paket ein. Die Option 82 beinhaltet die VLAN-ID (2 Bytes) und die Portnummer des Zugangsports (2 Bytes: die Circuit-ID-Suboption) und die MAC-Adresse des Switch (die Remote-ID-Suboption). Diese Information definiert eindeutig die Position des Zugangsports im Netzwerk. Beispiel: Im RUGGEDCOM ROX II ist die Circuit-ID für VLAN 2 am Line-Modul (LM) 4 Port 15 `00:00:00:02:04:0F`.

Der DHCP-Server, der die Option 82 unterstützt, sendet eine Unicast-Antwort und gibt die Option 82 zurück. Der DHCP Relay Agent entfernt das Option 82-Feld und überträgt das Paket zum Port, von dem die ursprüngliche Anfrage empfangen wurde.

Der DHCP Relay Agent kommuniziert über eine Management-Schnittstelle mit dem Server. Die IP-Adresse des Agenten ist die für die Management-Schnittstelle konfigurierte Adresse.

Der RUGGEDCOM ROX II kann als DHCP Relay Agent konfiguriert werden, der DHCP- und BOOTP-Anfragen von Clients in einem Layer-2-Netzwerk an einen oder mehrere konfigurierte DHCP-Server in anderen Netzwerken weiterleitet. Dadurch wird eine Implementierung bestimmter Isolierungsmaßnahmen zwischen DHCP-Clients und -Servern ermöglicht.

Der DHCP Relay Agent ist so konfiguriert, dass er auf DHCP- und BOOTP-Anfragen an bestimmten Ethernet- und VLAN-Netzwerkschnittstellen hört und auf eine Liste von einem oder mehreren DHCP-Servern ausgerichtet ist. Wenn eine Anfrage von einem Client empfangen wird, leitet der RUGGEDCOM ROX II die Anfrage an jeden konfigurierten DHCP-Server weiter. Wenn eine Antwort von einem Server empfangen wird, leitet der RUGGEDCOM ROX II die Antwort an den ursprünglichen Client zurück.

HINWEIS
Obwohl DHCP-Relay- und DHCP-Server so konfiguriert werden können, dass sie simultan laufen, können sie jedoch nicht so konfiguriert werden, dass sie an derselben Netzwerkschnittstelle laufen.

INHALT

- Abschnitt 7.2.1, „Den DHCP Relay Agent (IPv4) konfigurieren“
- Abschnitt 7.2.2, „Eine Liste der DHCP-Client-Ports (IPv4) anzeigen“
- Abschnitt 7.2.3, „Einen DHCP-Client-Port (IPv4) hinzufügen“

- Abschnitt 7.2.4, „Einen DHCP-Client-Port (IPv4) löschen“

Abschnitt 7.2.1

Den DHCP Relay Agent (IPv4) konfigurieren

Um den DHCP Relay Agent zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
dhcp-server-address { dhcp-server-address }	**Zusammenfassung:** Eine Zeichenkette Die IP-Adresse des DHCP-Servers, an den die DHCP-Anfragen von diesem Relay-Agent weitergeleitet werden.

3. Fügen Sie Client-Ports hinzu. Weitere Informationen finden Sie unter Abschnitt 7.2.3, „Einen DHCP-Client-Port (IPv4) hinzufügen“.
4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.2.2

Eine Liste der DHCP-Client-Ports (IPv4) anzeigen

Um eine Liste der Client-Ports des DHCP Relay Agents anzusehen, geben Sie Folgendes ein:

```
show running-config switch dhcp-relay-agent dhcp-client-ports
```

Falls Client-Ports konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config switch dhcp-relay-agent dhcp-client-ports switch dhcp-relay-agent dhcp-client-ports swport 1 ! !
```

Falls keine Client-Ports konfiguriert wurden, fügen Sie je nach Bedarf Client-Ports hinzu. Weitere Informationen finden Sie unter Abschnitt 7.2.3, „Einen DHCP-Client-Port (IPv4) hinzufügen“.

Abschnitt 7.2.3

Einen DHCP-Client-Port (IPv4) hinzufügen

Um einen Client-Port für den DHCP-Relay-Agent hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den Client-Port hinzu, indem Sie Folgendes eingeben:

   ```
   switch dhcp-relay-agent  dhcp-client-ports slot port
   ```

   Erläuterung:

   - *`slot`* ist die Bezeichnung des Modul-Einbauorts.
   - *`port`* ist die Nummer des Ports (oder eine Liste von Ports, wenn sie in einem Port-Trunk gebündelt sind) für das Modul.

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.2.4
Einen DHCP-Client-Port (IPv4) löschen

Um einen Client-Port für den DHCP-Relay-Agent zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den Client-Port, indem Sie Folgendes eingeben:

   ```
   no switch dhcp-relay-agent  dhcp-client-ports slot port
   ```

   Erläuterung:

   - *`slot`* ist die Bezeichnung des Modul-Einbauorts.
   - *`port`* ist die Nummer des Ports (oder eine Liste von Ports, wenn sie in einem Port-Trunk gebündelt sind) für das Modul.
3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.3
Den DHCP-Server verwalten

Das DHCP (Dynamic Host Configuration Protocol) ermöglicht die zentrale, einheitliche Verwaltung von IP-Adressen und Einstellungen für Clients, wobei eine Vielzahl von Zuordnungsverfahren angeboten wird. IP-Adressen können anhand der Ethernet-MAC-Adresse eines Clients entweder fortlaufend oder mit Hilfe der von einem DHCP Relay Agent bereitgestellten Port-Identifikation zugewiesen werden.

Die den Adressen in DHCP zugewiesenen Informationen sind so organisiert, dass Clients auf Schnittstellen-, Subnetz-, Pool-, gemeinsame Netzwerk-, Host-Gruppen- und Host-Ebene bedient werden können.

RUGGEDCOM ROX II unterstützt sowohl IPv4- als auch IPv6-Adresszuordnungen.

INHALT

- Abschnitt 7.3.1, „Eine Liste der aktiven Leases anzeigen“
- Abschnitt 7.3.2, „Den DHCP-Server konfigurieren“
- Abschnitt 7.3.3, „Den DHCP-Server aktivieren/deaktivieren“
- Abschnitt 7.3.4, „Konfigurieren von Optionen für den DHCP-Server“
- Abschnitt 7.3.5, „DHCP-Client-Konfigurationsoptionen verwalten“
- Abschnitt 7.3.6, „Hörende DHCP-Schnittstellen verwalten“
- Abschnitt 7.3.7, „Gemeinsame Netzwerke verwalten“
- Abschnitt 7.3.8, „Subnetze verwalten“
- Abschnitt 7.3.9, „Host-Gruppen verwalten“
- Abschnitt 7.3.10, „DHCP-Hosts verwalten“
- Abschnitt 7.3.11, „Adressen-Pools (IPv4) verwalten“

- Abschnitt 7.3.12, „Adressen-Pools (IPv6) verwalten“
- Abschnitt 7.3.13, „IP-Bereiche verwalten (IPv4)“
- Abschnitt 7.3.14, „IP-Bereiche verwalten (IPv6)“
- Abschnitt 7.3.15, „IPv6-Präfixe verwalten“
- Abschnitt 7.3.16, „Temporäre Subnetze verwalten“
- Abschnitt 7.3.17, „IPv6-Subnetze verwalten“
- Abschnitt 7.3.18, „Option 82-Klassen für Adress-Pools (IPv4) verwalten“

Abschnitt 7.3.1

Eine Liste der aktiven Leases anzeigen

RUGGEDCOM ROX II kann eine Liste der aktiven Leases erstellen. Die Liste enthält die Anfangs- und Endzeiten, die Hardware-Ethernet-Adresse und den Hostnamen des Clients für jedes Lease.

Um eine Liste der aktiven Leases anzuzeigen, gehen Sie wie folgt vor:

Um eine Liste der aktiven Leases anzuzeigen, geben Sie Folgendes ein:

- **Für IPv4**

```
services dhcpserver show-active-leases
```

- **Für IPv6**

```
services dhcpserver6 show-active-leases
```

Wenn Zertifikate konfiguriert wurden, wird eine Tabelle oder Liste ähnlich der Folgenden angezeigt:

```
ruggedcom# services dhcpserver show-active-leases
dhcpActionResult
lease 192.168.0.9 {
  starts 2 2012/11/13 20:35:47;
  ends 2 2012/11/13 20:45:47;
  hardware Ethernet 00:01:c0:0c:8b:a4;
  client-hostname "ape2-PC";
}

lease 192.168.0.11 {
  starts 2 2012/11/13 20:38:37;
  ends 2 2012/11/13 20:48:37;
  hardware Ethernet 00:01:c0:0b:b7:70;
}

lease 192.168.0.8 {
  starts 2 2012/11/13 20:38:47;
  ends 2 2012/11/13 20:48:47;
  hardware Ethernet 00:01:c0:0c:8b:a3;
  client-hostname "ape2-PC";
}

lease 192.168.0.22 {
  starts 2 2012/11/13 20:36:14;
  ends 2 2012/11/13 20:46:14;
  hardware Ethernet 00:01:c0:0b:b7:71;
}
```

Abschnitt 7.3.2
Den DHCP-Server konfigurieren

Um den DHCP-Server zu konfigurieren, gehen Sie wie folgt vor:

1. Aktivieren Sie den DHCP-Server. Weitere Informationen finden Sie unter Abschnitt 7.3.3, „Den DHCP-Server aktivieren/deaktivieren“.
2. Fügen Sie hörende DHCP-Schnittstellen hinzu und konfigurieren Sie diese. Weitere Informationen finden Sie unter Abschnitt 7.3.6.2, „Eine hörende DHCP-Schnittstelle hinzufügen“.
3. Fügen Sie gemeinsame Netzwerke hinzu und konfigurieren Sie diese. Weitere Informationen finden Sie unter Abschnitt 7.3.7.2, „Ein gemeinsames Netzwerk hinzufügen“.

   HINWEIS
   Wenn zwei oder mehr Subnetze für die gleiche Schnittstelle konfiguriert sind, muss mindestens ein gemeinsames Netzwerk verfügbar sein.
4. Fügen Sie Subnetze hinzu und konfigurieren Sie diese. Weitere Informationen finden Sie unter Abschnitt 7.3.8.2, „Hinzufügen eines Subnetzes“.
5. Fügen Sie Hosts hinzu und konfigurieren Sie diese. Weitere Informationen finden Sie unter Abschnitt 7.3.10.2, „Einen Host hinzufügen“.
6. Fügen Sie Host-Gruppen hinzu und konfigurieren Sie diese. Weitere Informationen finden Sie unter Abschnitt 7.3.9.2, „Eine Hostgruppe hinzufügen“.

Abschnitt 7.3.3
Den DHCP-Server aktivieren/deaktivieren

Um den DHCP-Server zu aktivieren oder zu deaktivieren, geben Sie Folgendes ein:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Aktivieren oder deaktivieren Sie den DHCP-Server, indem Sie Folgendes eingeben:
   - **Zum Aktivieren für IPv4**
     ```
     services dhcpserver enabled
     ```
   - **Zum Deaktivieren für IPv4**
     ```
     no services dhcpserver enabled
     ```
   - **Zum Aktivieren für IPv6**
     ```
     services dhcpserver6 enabled
     ```
   - **Zum Deaktivieren für IPv6**
     ```
     no services dhcpserver6 enabled
     ```
3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.3.4
Konfigurieren von Optionen für den DHCP-Server

Um Optionen für den DHCP-Server zu konfigurieren, gehen Sie folgendermaßen vor:

HINWEIS
Für ein Subnetz eingestellte Optionen übersteuern die für den DHCP-Server eingestellten Optionen.

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu:
   - **Für IPv4**
     services » dhcpserver » options
   - **Für IPv6**
     services » dhcpserver6 » options
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

WICHTIG!
Nur für IPv4:

Wenn DHCP-Relais-Clients (bzw. Option 82-Clients) im selben Subnetz verwendet werden wie der DHCP-Server, versuchen einige Clients, den Lease sofort nach dem Empfang zu verlängern, indem sie direkt beim DHCP-Server eine Verlängerung anfordern. Weil der DHCP-Server standardmäßig so konfiguriert ist, dass der Lease nur über einen mit den aktuellen Option 82-Feldern konfigurierten Relais-Agenten bereitgestellt wird, sendet der Server dem Client eine NAK-Meldung (negative Quittierung) und gestattet den Lease nicht. Durch Aktivieren von Option 82 wird die NAK-Meldung deaktiviert, weshalb die vom DHCP-Relais-Agenten gesendete Verlängerungsanforderung (die der DHCP-Server annimmt, da die richtigen Option 82-Felder hinzugefügt wurden) die einzige Meldung ist, für die der Client eine Antwort empfängt.

Unterstützung für Option 82 darf nur aktiviert werden, wenn sich der DHCP-Server und die Clients im selben Subnetz befinden.

Die Bedeutung der meisten Option 82-Felder wird vom DHCP-Relais-Client festgelegt. Um zu ermitteln, welche Werte vom Client für besondere Optionen benötigt werden, ziehen Sie die Client-Dokumentation hinzu.

Unterstützung für DHCP-Relais kann auch in einzelnen Subnetzen aktiviert werden. Weitere Informationen finden Sie unter Abschnitt 7.3.8.3, „Optionen für Subnetze konfigurieren“.

Parameter	Beschreibung
unknown-client { unknown-client }	**Zusammenfassung:** { allow, deny, ignore } Maßnahmen für bisher nicht registrierte Clients
authorize-server	Aktiviert/deaktiviert die Autorisierung des Servers an diesem Client. Wenn diese Option aktiviert ist, sendet der Server "Deny"-Nachrichten an den Client, der versucht, den Lease zu erneuern, von dem der Server weiß, dass der Client ihn nicht hat.
option82	Aktiviert/deaktiviert das NAK von Option 82-Clients für dieses Subnetz.

4. [Optional] Konfigurieren Sie weitere Client-Konfigurationsoptionen. Weitere Informationen finden Sie in Abschnitt 7.3.5.1, „Konfigurieren von Standard-Konfigurationsoptionen (IPv4) für DHCP-Clients“ oder Abschnitt 7.3.5.2, „Konfigurieren von Standard-Konfigurationsoptionen (IPv6) für DHCP-Clients“.
5. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.3.5
DHCP-Client-Konfigurationsoptionen verwalten

Standard- und benutzerspezifische Optionen können global im DHCP-Server oder für bestimmte gemeinsame Netzwerke, Subnetze, Host-Gruppen oder Hosts konfiguriert werden. Optionen, die auf einer individuellen Ebene eingestellt sind, haben Vorrang vor global eingestellten Optionen.

INHALT

- Abschnitt 7.3.5.1, „Konfigurieren von Standard-Konfigurationsoptionen (IPv4) für DHCP-Clients“
- Abschnitt 7.3.5.2, „Konfigurieren von Standard-Konfigurationsoptionen (IPv6) für DHCP-Clients“
- Abschnitt 7.3.5.3, „Anzeigen einer Liste der kundenspezifischen Konfigurationsoptionen für DHCP-Clients“
- Abschnitt 7.3.5.4, „Hinzufügen einer kundenspezifischen Konfigurationsoption für DHCP-Clients“
- Abschnitt 7.3.5.5, „Löschen einer kundenspezifischen Konfigurationsoption für DHCP-Clients“

Abschnitt 7.3.5.1
Konfigurieren von Standard-Konfigurationsoptionen (IPv4) für DHCP-Clients

Konfigurationsoptionen für DHCP-Clients können global oder für ein einzelnes gemeinsames Netzwerk, Subnetz, eine Hostgruppe oder einen Host konfiguriert werden.

HINWEIS
Für ein einzelnes gemeinsames Netzwerk, Subnetz, eine Hostgruppe oder einen Host eingestellte Optionen übersteuern die auf globaler Ebene eingestellten Optionen.

Um Client-Optionen zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***services » dhcpserver » {path} » options***, wobei *path* der Pfad zum und die Bezeichnung des gewünschten gemeinsamen Netzwerks, Subnetzes, der Hostgruppe oder des Hosts ist. Um beispielsweise auf die Optionen für ein gemeinsames Netzwerk mit der Bezeichnung *Shared* zuzugreifen, navigieren Sie zu:

   services » dhcpserver » shared-network » Shared » options

   Um auf die globalen Optionen zuzugreifen, navigieren Sie zu:

   services » dhcpserver » options
3. Konfigurieren Sie je nach Bedarf die folgenden Parameter:

Parameter	Beschreibung
hostname { hostname }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 32 Zeichen Die eindeutige Bezeichnung, um den Host innerhalb einer DHCP-Konfiguration zu benennen.
subnetmask { subnetmask }	**Zusammenfassung:** Eine Zeichenkette mit 7 bis 15 Zeichen Subnetzmaske
default-route { default-route }	**Zusammenfassung:** Eine Zeichenkette mit 7 bis 15 Zeichen Die Standardroute, die der Server dem Client anbietet, wenn er dem Client den Lease ausgibt.
broadcast { broadcast }	**Zusammenfassung:** Eine Zeichenkette mit 7 bis 15 Zeichen

Parameter	Beschreibung
	Die Broadcast-Adresse, die der Server dem Client anbietet, wenn er dem Client den Lease ausgibt.
domain { domain }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 253 Zeichen Der Domain-Name, den der Server dem Client anbietet, wenn er dem Client den Lease ausgibt.
dns-server { dns-server }	**Zusammenfassung:** Eine Zeichenkette mit 7 bis 31 Zeichen Der Domain-Namenserver, den der Server dem Client anbietet, wenn er dem Client den Lease ausgibt.
static-route { static-route }	**Zusammenfassung:** Eine Zeichenkette mit 7 bis 15 Zeichen Die statische Route, die der DHCP-Server dem Client anbietet, wenn er dem Client den Lease ausgibt.

4. [Optional] Fügen Sie kundenspezifische Optionen hinzu. Weitere Informationen finden Sie unter Abschnitt 7.3.5.4, „Hinzufügen einer kundenspezifischen Konfigurationsoption für DHCP-Clients“.
5. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.3.5.2

Konfigurieren von Standard-Konfigurationsoptionen (IPv6) für DHCP-Clients

Konfigurationsoptionen für DHCP-Clients können global oder für ein einzelnes gemeinsames Netzwerk, Subnetz, eine Hostgruppe oder einen Host konfiguriert werden.

HINWEIS
Für ein einzelnes gemeinsames Netzwerk, Subnetz, eine Hostgruppe oder einen Host eingestellte Optionen übersteuern die auf globaler Ebene eingestellten Optionen.

Um Client-Optionen zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***services » dhcpserver6 » {path} » {name} » options***, wobei *path* der Pfad zum und die Bezeichnung des gewünschten gemeinsamen Netzwerks, Subnetzes6, der Hostgruppe oder des Hosts und *name* die vom Benutzer hinzugefügte Bezeichnung ist.

   Um beispielsweise auf die Optionen für ein gemeinsames Netzwerk mit der Bezeichnung *Shared* zuzugreifen, navigieren Sie zu:

   services » dhcpserver6 » shared-network » Shared » options

   Um auf die globalen Optionen zuzugreifen, navigieren Sie zu:

   services » dhcpserver6 » options
3. Konfigurieren Sie je nach Bedarf die folgenden Parameter:

Parameter	Beschreibung
domain { domain }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 253 Zeichen Der Domain-Name, den der Server dem Client anbietet, wenn er dem Client den Lease ausgibt.
dns-server { dns-server }	**Zusammenfassung:** Eine Zeichenkette mit 6 bis 87 Zeichen

Parameter	Beschreibung
	Der Domain-Namenserver, den der Server dem Client anbietet, wenn er dem Client den Lease ausgibt.
domain-search { domain-search }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 773 Zeichen Die Domain-Suchliste, die der Server dem Client anbietet, wenn er dem Client den Lease ausgibt.

4. [Optional] Fügen Sie kundenspezifische Optionen hinzu. Weitere Informationen finden Sie unter Abschnitt 7.3.5.4, „Hinzufügen einer kundenspezifischen Konfigurationsoption für DHCP-Clients“.
5. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.3.5.3
Anzeigen einer Liste der kundenspezifischen Konfigurationsoptionen für DHCP-Clients

Um eine Liste der kundenspezifischen Konfigurationsoptionen für DHCP-Clients auf globaler Ebene oder für ein bestimmtes gemeinsames Netzwerk anzuzeigen, geben Sie Folgendes ein:

- **Für IPv4**

```
show running-config services dhcpserver path options client custom
```

- **Für IPv6**

```
show running-config services dhcpserver6 options client custom
```

Erläuterung: *`path`* ist der Pfad zum und die Bezeichnung des gewünschten gemeinsamen Netzwerks, Subnetzes, der Hostgruppe oder des Hosts.

Falls kundenspezifische Konfigurationen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config services dhcpserver options client custom
services
 dhcpserver
  options
   client
    custom 120 500
    !
   !
  !
 !
!
```

Falls keine kundenspezifische Konfigurationen konfiguriert wurden, fügen Sie sie je nach Bedarf hinzu. Weitere Informationen finden Sie unter Abschnitt 7.3.5.4, „Hinzufügen einer kundenspezifischen Konfigurationsoption für DHCP-Clients“.

Abschnitt 7.3.5.4
Hinzufügen einer kundenspezifischen Konfigurationsoption für DHCP-Clients

Um eine kundenspezifische Client-Option hinzuzufügen, gehen Sie wie folgt vor:

HINWEIS
Die Nummer der Option (festgelegt von der Internet Assigned Numbers Authority bzw. IANA) und deren zulässiger Wert müssen bekannt sein, bevor eine kundenspezifische Option konfiguriert werden kann. Weitere Informationen über verfügbare DHCP-Optionen finden Sie in RFC 2132 [http://tools.ietf.org/html/rfc2132].

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu:
   - **Für IPv4**
     services » dhcpserver » {path} » options » client » custom
   - **Für IPv6**
     services » dhcpserver6 » options » client » custom

   wobei *path* der Pfad zum und die Bezeichnung des gewünschten gemeinsamen Netzwerks, Subnetzes, der Hostgruppe oder des Hosts ist.

   HINWEIS
   *Kundenspezifische Optionen sind auf **{path}**-Ebene nur für IPv4 verfügbar.*

   Um beispielsweise auf die kundenspezifischen IPv4-Optionen für ein gemeinsames Netzwerk mit der Bezeichnung *Shared* zuzugreifen, navigieren Sie zu:

   services » dhcpserver » shared-network » Shared » options » client » custom

   Um auf kundenspezifische IPv4-Optionen auf globaler Ebene zuzugreifen, navigieren Sie zu:

   services » dhcpserver » options » client » custom
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
{ number }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl
{ value }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl Der Wert der benutzerspezifischen Option.

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.3.5.5
Löschen einer kundenspezifischen Konfigurationsoption für DHCP-Clients

Um eine kundenspezifische Client-Option zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu:
   - **Für IPv4**
     services » dhcpserver » {path} » options » client » custom
   - **Für IPv6**
     services » dhcpserver6 » options » client » custom

   wobei *path* der Pfad zum und die Bezeichnung des gewünschten gemeinsamen Netzwerks, Subnetzes, der Hostgruppe oder des Hosts ist.

HINWEIS
*Kundenspezifische Optionen sind auf **{path}**-Ebene nur für IPv4 verfügbar.*

Um beispielsweise auf die kundenspezifischen IPv4-Optionen für ein gemeinsames Netzwerk mit der Bezeichnung *Shared* zuzugreifen, navigieren Sie zu:

services » dhcpserver » shared-network » Shared » options » client » custom

Um auf kundenspezifische IPv4-Optionen auf globaler Ebene zuzugreifen, navigieren Sie zu:

services » dhcpserver » options » client » custom

3. Löschen Sie die kundenspezifische Option, indem Sie Folgendes eingeben:
   - **Für IPv4**
     ```
     no services dhcpserver path options client custom number
     ```
   - **Für IPv6**
     ```
     no services dhcpserver6 options client custom number
     ```

   Erläuterung:
   - *path* ist der Pfad zum und die Bezeichnung des gewünschten gemeinsamen Netzwerks, Subnetzes, der Hostgruppe oder des Hosts.
   - *number* ist die Optionsnummer
4. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.3.6
Hörende DHCP-Schnittstellen verwalten

Hörende DHCP-Schnittstellen legen die IP-Schnittstelle fest, an die der Client eine Anforderung sendet.

INHALT

- Abschnitt 7.3.6.1, „Eine Liste der hörenden DHCP-Schnittstellen anzeigen“
- Abschnitt 7.3.6.2, „Eine hörende DHCP-Schnittstelle hinzufügen“
- Abschnitt 7.3.6.3, „Eine hörende DHCP-Schnittstelle löschen“

Abschnitt 7.3.6.1
Eine Liste der hörenden DHCP-Schnittstellen anzeigen

Um eine Liste der hörenden DHCP-Schnittstellen anzusehen, geben Sie Folgendes ein:

- **Für IPv4**
  ```
  show running-config services dhcpserver interface
  ```
- **Für IPv6**
  ```
  show running-config services dhcpserver6 interface
  ```

Falls hörende DHCP-Schnittstellen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config services dhcpserver interface | tab
NAME
-------------
switch.0001

 !
!
```

Falls keine hörenden DHCP-Schnittstellen konfiguriert wurden, fügen Sie je nach Bedarf Schnittstellen hinzu. Weitere Informationen finden Sie unter Abschnitt 7.3.6.2, „Eine hörende DHCP-Schnittstelle hinzufügen“.

Abschnitt 7.3.6.2
Eine hörende DHCP-Schnittstelle hinzufügen

Um eine hörende DHCP-Schnittstelle hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie die Schnittstelle hinzu, indem Sie Folgendes eingeben:
   - **Für IPv4**
     ```
     services dhcpserver interface name
     ```
   - **Für IPv6**
     ```
     services dhcpserver6 interface name
     ```

   Erläuterung:

   - *name* ist die Bezeichnung der Schnittstelle
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.3.6.3
Eine hörende DHCP-Schnittstelle löschen

Um eine hörende DHCP-Schnittstelle zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie das Interface, indem Sie Folgendes eingeben:
   - **Für IPv4**
     ```
     no services dhcpserver interface name
     ```
   - **Für IPv6**
     ```
     no services dhcpserver6 interface name
     ```

   Erläuterung:

   - *name* ist die Bezeichnung der Schnittstelle
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.3.7

Gemeinsame Netzwerke verwalten

Gemeinsame Netzwerke werden verwendet, wenn mehrere Subnetze durch einen einzelnen physikalischen Port bedient werden sollen. Dies ist der Fall, wenn ein mit dem Port verbundener DHCP Relay Agent mit zusätzlichen Subnetzen hinter dem Relay Agent verwendet wird, oder wenn mehrere virtuelle Netzwerke an einer physikalischen Schnittstelle vorhanden sind. Jedes Subnetz erhält dann seine eigene Subnetzdefinition im gemeinsamen Netzwerk statt auf der übergeordneten Ebene. Gemeinsame Netzwerke enthalten Subnetze, Gruppen und Hosts.

INHALT

- Abschnitt 7.3.7.1, „Eine Liste gemeinsamer Netzwerke anzeigen“
- Abschnitt 7.3.7.2, „Ein gemeinsames Netzwerk hinzufügen“
- Abschnitt 7.3.7.3, „Optionen für gemeinsame Netzwerke konfigurieren“
- Abschnitt 7.3.7.4, „Ein gemeinsames Netzwerk löschen“

Abschnitt 7.3.7.1

Eine Liste gemeinsamer Netzwerke anzeigen

Um eine Liste der gemeinsamen Netzwerke anzusehen, geben Sie Folgendes ein:

- **Für IPv4**

  ```
  show running-config services dhcpserver shared-network
  ```

- **Für IPv6**

  ```
  show running-config services dhcpserver6 shared-network
  ```

Falls gemeinsame Netzwerke konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config services dhcpserver shared-network
services
 dhcpserver
  shared-network Shared
   options client
    no hostname
    no subnetmask
    no default-route
    no broadcast
    no domain
    no dns-server
    no static-route
    no nis server
    no nis domain
   !
  !
 !
!
```

Falls keine gemeinsamen Netzwerke konfiguriert wurden, fügen Sie je nach Bedarf Netzwerke hinzu. Weitere Informationen finden Sie unter Abschnitt 7.3.7.2, „Ein gemeinsames Netzwerk hinzufügen“.

Abschnitt 7.3.7.2

Ein gemeinsames Netzwerk hinzufügen

Um einem DHCP-Server ein gemeinsames Netzwerk hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie das gemeinsame Netzwerk hinzu, indem Sie Folgendes eingeben:
   - **Für IPv4**
     ```
     services dhcpserver shared-network name
     ```
   - **Für IPv6**
     ```
     services dhcpserver6 shared-network name
     ```

   Erläuterung:
   - *name* ist die Bezeichnung des gemeinsamen Netzwerkes
3. Konfigurieren Sie Optionen für das gemeinsame Netzwerk. Für weitere Informationen siehe Abschnitt 7.3.7.3, „Optionen für gemeinsame Netzwerke konfigurieren“.
4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.3.7.3

Optionen für gemeinsame Netzwerke konfigurieren

Um Optionen für ein gemeinsames Netzwerk auf dem DHCP-Server zu konfigurieren, gehen Sie folgendermaßen vor:

HINWEIS
Für ein gemeinsames Netzwerk eingestellte Optionen übersteuern die für den DHCP-Server eingestellten Optionen.

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu:
   - **Für IPv4**
     ```
     services dhcpserver shared-network{gemeinsames Netzwerk} options
     ```
   - **Für IPv6**
     ```
     services dhcpserver6 shared-network{gemeinsames Netzwerk} options
     ```
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

WICHTIG!
Nur für IPv4:

Wenn DHCP-Relais-Clients (bzw. Option 82-Clients) im selben Subnetz verwendet werden wie der DHCP-Server, versuchen einige Clients, den Lease sofort nach dem Empfang zu verlängern, indem sie direkt beim DHCP-Server eine Verlängerung anfordern. Weil der DHCP-Server standardmäßig so konfiguriert ist, dass der Lease nur über einen mit den aktuellen Option 82-Feldern konfigurierten Relais-Agenten bereitgestellt wird, sendet der Server dem Client eine NAK-Nachricht (negative Quittierung) und gestattet den Lease nicht. Durch Aktivieren von Option 82 wird die NAK-Nachricht deaktiviert, weshalb die vom DHCP-Relais-Agenten gesendete

Verlängerungsanforderung (die der DHCP-Server annimmt, da die richtigen Option 82-Felder hinzugefügt wurden) die einzige Nachricht ist, für die der Client eine Antwort empfängt.

Unterstützung für Option 82 darf nur aktiviert werden, wenn sich der DHCP-Server und die Clients im selben Subnetz befinden.

Die Bedeutung der meisten Option 82-Felder wird vom DHCP-Relais-Client festgelegt. Um zu ermitteln, welche Werte vom Client für besondere Optionen benötigt werden, ziehen Sie die Client-Dokumentation hinzu.

Unterstützung für DHCP-Relais kann auch in einzelnen Subnetzen aktiviert werden. Weitere Informationen finden Sie unter Abschnitt 7.3.8.3, „Optionen für Subnetze konfigurieren“.

Parameter	Beschreibung
unknown-client { unknown-client }	**Zusammenfassung:** { allow, deny, ignore } Maßnahmen für bisher nicht registrierte Clients
authorize-server	Aktiviert/deaktiviert die Autorisierung des Servers an diesem Client. Wenn diese Option aktiviert ist, sendet der Server "Deny"-Nachrichten an den Client, der versucht, den Lease zu erneuern, von dem der Server weiß, dass der Client ihn nicht hat.
option82	Aktiviert/deaktiviert das NAK von Option 82-Clients für dieses Subnetz.

4. [Optional] Konfigurieren Sie die Konfigurationsoptionen für DHCP-Clients in freigegebenen Netzwerken. Weitere Informationen finden Sie in Abschnitt 7.3.5.1, „Konfigurieren von Standard-Konfigurationsoptionen (IPv4) für DHCP-Clients“ oder Abschnitt 7.3.5.2, „Konfigurieren von Standard-Konfigurationsoptionen (IPv6) für DHCP-Clients“.
5. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.3.7.4

Ein gemeinsames Netzwerk löschen

Um ein gemeinsames Netzwerk zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie das gemeinsame Netzwerk, indem Sie Folgendes eingeben:
   - **Für IPv4**
     ```
     no services dhcpserver shared-network name
     ```
   - **Für IPv6**
     ```
     no services dhcpserver6 shared-network name
     ```

   Erläuterung:
   - *`name`* ist die Bezeichnung des gemeinsamen Netzwerkes
3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.3.8

Subnetze verwalten

Subnetze steuern die Einstellungen jedes von DHCP bedienten Subnetzes. Ein Subnetz kann einen Bereich von IP-Adressen für Clients enthalten. Subnetze enthalten Gruppen, Pools und Hosts. Nur ein einziges Subnetz kann dynamische IP-Adressbereiche ohne Zugangsbeschränkungen für einen bestimmten physikalischen Port enthalten, da DHCP nicht weiß, zu welchem Subnetz ein Client gehören soll, wenn die Anforderung empfangen wird.

INHALT

- Abschnitt 7.3.8.1, „Eine Liste der Subnetze anzeigen“
- Abschnitt 7.3.8.2, „Hinzufügen eines Subnetzes“
- Abschnitt 7.3.8.3, „Optionen für Subnetze konfigurieren“
- Abschnitt 7.3.8.4, „Ein Subnetz löschen“

Abschnitt 7.3.8.1

Eine Liste der Subnetze anzeigen

Um eine Liste der Subnetze anzusehen, geben Sie Folgendes ein:

- **Für IPv4**

```
show running-config services dhcpserver subnet-name
```

- **Für IPv6**

```
show running-config services dhcpserver6 subnet6-name
```

Falls Subnetze konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config services dhcpserver subnet-name network-ip | tab
NAME  NETWORK IP
-----------------------
SUB1  192.168.0.0/27
SUB2  192.168.0.32/27

 !
!
```

Falls keine Subnetze konfiguriert wurden, fügen Sie je nach Bedarf Subnetze hinzu. Weitere Informationen finden Sie unter Abschnitt 7.3.8.2, „Hinzufügen eines Subnetzes“.

Abschnitt 7.3.8.2

Hinzufügen eines Subnetzes

Um ein Subnetz zu einem DHCP-Server hinzuzufügen, gehen Sie wie folgt vor:

HINWEIS
Wenn zwei oder mehr Subnetze für dieselbe Schnittstelle konfiguriert werden, dann muss mindestens ein gemeinsames Netzwerk verfügbar sein. Für Informationen über das Konfigurieren eines gemeinsamen Netzwerkes siehe Abschnitt 7.3.7.2, „Ein gemeinsames Netzwerk hinzufügen“.

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.

2. Fügen Sie das Subnetz hinzu, indem Sie Folgendes eingeben:
   - **Für IPv4**
     ```
     services dhcpserver subnet-name name
     ```
   - **Für IPv6**
     ```
     services dhcpserver6 subnet6-name name
     ```

   Erläuterung:
   - *name* ist die Bezeichnung des Subnetzes
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
network-ip { network-ip }	**Zusammenfassung:** Eine Zeichenkette mit 9 bis 18 Zeichen Die Netzwerk-IP-Adresse für dieses Subnetz. Dieser Parameter ist obligatorisch.
shared-network { shared-network }	**Zusammenfassung:** Eine Zeichenkette Das gemeinsame Netzwerk, zu dem der Host gehört.

Parameter	Beschreibung
network-ip { network-ip }	**Zusammenfassung:** Eine Zeichenkette mit 4 bis 43 Zeichen Die Netzwerk-IPv6-Adresse für dieses Subnetz. Dieser Parameter ist obligatorisch.
shared-network { shared-network }	**Zusammenfassung:** Eine Zeichenkette Das gemeinsame Netzwerk, zu dem der Host gehört.

4. Konfigurieren Sie die Optionen für das Subnetz. Weitere Informationen finden Sie unter Abschnitt 7.3.8.3, „Optionen für Subnetze konfigurieren“.
5. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.3.8.3
Optionen für Subnetze konfigurieren

Um Optionen für ein Subnetz zu konfigurieren, gehen Sie folgendermaßen vor:

HINWEIS
Für ein Subnetz eingestellte Optionen übersteuern die für den DHCP-Server eingestellten Optionen.

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu:
   - **Für IPv4**
     ```
     services dhcpserver subnet-name name options
     ```
   - **Für IPv6**
     ```
     services dhcpserver6 subnet6-name name options
     ```

   Erläuterung:

- *name* ist die Bezeichnung des Subnetzes

3. Konfigurieren Sie die Lease-Zeiteinstellungen mithilfe der folgenden Parameter:
   - **Für IPv4:**

Parameter	Beschreibung
default { default }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl **Standard:** 600 Die minimale Lease-Zeit in Sekunden, die der Server den Clients anbietet.
maximum { maximum }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl **Standard:** 7200 Die maximale Lease-Zeit in Sekunden, die der Server den Clients anbietet.

   - **Für IPv6:**

Parameter	Beschreibung
default { default }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl **Standard:** 600 Die minimale Lease-Zeit in Sekunden, die der Server den Clients anbietet.
maximum { maximum }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl **Standard:** 7200 Die maximale Lease-Zeit in Sekunden, die der Server den Clients anbietet.

4. Konfigurieren Sie die Client-Einstellungen mithilfe der folgenden Parameter:

WICHTIG!
Nur für IPv4:

Wenn DHCP-Relais-Clients (bzw. Option 82-Clients) im selben Subnetz verwendet werden wie der DHCP-Server, versuchen einige Clients, den Lease sofort nach dem Empfang zu verlängern, indem sie direkt beim DHCP-Server eine Verlängerung anfordern. Weil der DHCP-Server standardmäßig so konfiguriert ist, dass der Lease nur über einen mit den aktuellen Option 82-Feldern konfigurierten Relais-Agenten bereitgestellt wird, sendet der Server dem Client eine NAK-Nachricht (negative Quittierung) und gestattet den Lease nicht. Durch Aktivieren von Option 82 wird die NAK-Nachricht deaktiviert, weshalb die vom DHCP-Relais-Agenten gesendete Verlängerungsanforderung (die der DHCP-Server annimmt, da die richtigen Option 82-Felder hinzugefügt wurden) die einzige Nachricht ist, für die der Client eine Antwort empfängt.

Unterstützung für Option 82 darf nur aktiviert werden, wenn sich der DHCP-Server und die Clients im selben Subnetz befinden.

Die Bedeutung der meisten Option 82-Felder wird vom DHCP-Relais-Client festgelegt. Um zu ermitteln, welche Werte vom Client für besondere Optionen benötigt werden, ziehen Sie die Client-Dokumentation hinzu.

Unterstützung für DHCP-Relais kann auch in einzelnen Subnetzen aktiviert werden.

   - **Für IPv4**

Parameter	Beschreibung
unknown-client { unknown-client }	**Zusammenfassung:** { allow, deny, ignore } Maßnahmen für bisher nicht registrierte Clients
option82	Aktiviert/deaktiviert das NAK von Option 82-Clients für dieses Subnetz.

Parameter	Beschreibung
authorize-server	Aktiviert/deaktiviert die Autorisierung des Servers an diesem Client. Wenn diese Option aktiviert ist, sendet der Server "Deny"-Nachrichten an den Client, der versucht, den Lease zu erneuern, von dem der Server weiß, dass der Client ihn nicht hat.

- **Für IPv6**

Parameter	Beschreibung
unknown-client { unknown-client }	**Zusammenfassung:** { allow, deny, ignore } Maßnahmen für bisher nicht registrierte Clients
authorize-server	Aktiviert/deaktiviert die Autorisierung des Servers an diesem Client. Wenn diese Option aktiviert ist, sendet der Server "Deny"-Nachrichten an den Client, der versucht, den Lease zu erneuern, von dem der Server weiß, dass der Client ihn nicht hat.

5. [Optional] Konfigurieren Sie die Konfigurationsoptionen für DHCP-Clients im Subnetz. Weitere Informationen finden Sie in Abschnitt 7.3.5.1, „Konfigurieren von Standard-Konfigurationsoptionen (IPv4) für DHCP-Clients“ oder Abschnitt 7.3.5.2, „Konfigurieren von Standard-Konfigurationsoptionen (IPv6) für DHCP-Clients“.
6. Konfigurieren Sie einen oder mehrere Adress-Pools für das Subnetz. Weitere Informationen finden Sie unter Abschnitt 7.3.11.2, „Hinzufügen eines Adress-Pools (IPv4)“ oder Abschnitt 7.3.12.2, „Hinzufügen eines Adress-Pools (IPv6)“.
7. Konfigurieren Sie einen oder mehrere IP-Bereiche für das Subnetz. Weitere Informationen finden Sie unter Abschnitt 7.3.13.2, „Hinzufügen eines IP-Bereichs (IPv4)“ oder Abschnitt 7.3.14.2, „Hinzufügen eines IP-Bereichs (IPv6)“.
8. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.3.8.4

Ein Subnetz löschen

Um ein Subnetz zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie das Subnetz, indem Sie Folgendes eingeben:
   - **Für IPv4**
     ```
     no services dhcpserver subnet-name name
     ```
   - **Für IPv6**
     ```
     no services dhcpserver6 subnet6-name name
     ```

   Erläuterung:

   - *name* ist die Bezeichnung des Subnetzes
3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.3.9

Host-Gruppen verwalten

Mit Hilfe von Host-Gruppen können für mehrere Hosts einheitliche Einstellungen vorgenommen werden, was Änderungen an den Einstellungen für alle Hosts der Gruppe vereinfacht. Host-Gruppen enthalten Hosts.

INHALT

- Abschnitt 7.3.9.1, „Eine Liste der Host-Gruppen anzeigen“
- Abschnitt 7.3.9.2, „Eine Hostgruppe hinzufügen“
- Abschnitt 7.3.9.3, „Konfigurieren von Optionen für eine Hostgruppe“
- Abschnitt 7.3.9.4, „Eine Hostgruppe löschen“

Abschnitt 7.3.9.1

Eine Liste der Host-Gruppen anzeigen

Um eine Liste der Host-Gruppen anzusehen, geben Sie Folgendes ein:

- **Für IPv4**

```
show running-config services dhcpserver host-groups
```

- **Für IPv6**

```
show running-config services dhcpserver6 host-groups
```

Falls Host-Gruppen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config services dhcpserver host-groups
services
 dhcpserver
  host-groups "Local Group"
   options
    client
     no hostname
     no subnetmask
     no default-route
     no broadcast
     no domain
     no dns-server
     no static-route
     no nis server
     no nis domain
    !
   !
  !
 !
!
```

Falls keine Host-Gruppen konfiguriert wurden, fügen Sie je nach Bedarf Host-Gruppen hinzu. Weitere Informationen finden Sie unter Abschnitt 7.3.9.2, „Eine Hostgruppe hinzufügen“.

Abschnitt 7.3.9.2

Eine Hostgruppe hinzufügen

Um eine Hostgruppe zu einem DHCP-Server hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu:
   - **Für IPv4**
     ```
     services dhcpserver host-groups
     ```
   - **Für IPv6**
     ```
     services dhcpserver6 host-groups
     ```
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
{ name }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 32 Zeichen Die Beschreibung der Host-Gruppen.

4. Konfigurieren Sie die Optionen für die Hostgruppe. Für weitere Informationen siehe Abschnitt 7.3.9.3, „Konfigurieren von Optionen für eine Hostgruppe“.
5. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.3.9.3
Konfigurieren von Optionen für eine Hostgruppe

Um Optionen für eine Hostgruppe auf dem DHCP-Server zu konfigurieren, gehen Sie folgendermaßen vor:

> **HINWEIS**
> *Für eine Hostgruppe eingestellte Optionen übersteuern die für den DHCP-Server eingestellten Optionen.*

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Ändern Sie den Modus in **Edit Private** oder **Edit Exclusive**.
3. Navigieren Sie zu:
   - **Für IPv4**
     services » dhcpserver » host-groups » {host} » options
   - **Für IPv6**
     services » dhcpserver6 » host-groups » {host} » options

   Wobei *{host}* die Bezeichnung der Hostgruppe ist.
4. Konfigurieren Sie die Lease-Zeiteinstellungen mithilfe der folgenden Parameter:
   - **Für IPv4:**

Parameter	Beschreibung
default { default }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl **Standard:** 600 Die minimale Lease-Zeit in Sekunden, die der Server den Clients anbietet.
maximum { maximum }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl **Standard:** 7200 Die maximale Lease-Zeit in Sekunden, die der Server den Clients anbietet.

- **Für IPv6:**

Parameter	Beschreibung
default { default }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl **Standard:** 600 Die minimale Lease-Zeit in Sekunden, die der Server den Clients anbietet.
maximum { maximum }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl **Standard:** 7200 Die maximale Lease-Zeit in Sekunden, die der Server den Clients anbietet.

5. Konfigurieren Sie die Client-Einstellungen mithilfe der folgenden Parameter:
   - **Für IPv4**

Parameter	Beschreibung
unknown-client { unknown-client }	**Zusammenfassung:** { allow, deny, ignore } Maßnahmen für bisher nicht registrierte Clients
shared-network { shared-network }	**Zusammenfassung:** Eine Zeichenkette Das gemeinsame Netzwerk, zu dem der Host gehört.
subnet { subnet }	**Zusammenfassung:** Eine Zeichenkette Das Subnetz, zu dem der Host gehört.

   - **Für IPv6**

Parameter	Beschreibung
unknown-client { unknown-client }	**Zusammenfassung:** { allow, deny, ignore } Maßnahmen für bisher nicht registrierte Clients
shared-network { shared-network }	**Zusammenfassung:** Eine Zeichenkette Das gemeinsame Netzwerk, zu dem der Host gehört.
subnet6 { subnet6 }	**Zusammenfassung:** Eine Zeichenkette Das Subnetz, zu dem der Host gehört.

6. [Optional] Konfigurieren Sie die Konfigurationsoptionen für DHCP-Clients in der Hostgruppe. Weitere Informationen finden Sie in Abschnitt 7.3.5.1, „Konfigurieren von Standard-Konfigurationsoptionen (IPv4) für DHCP-Clients“ oder Abschnitt 7.3.5.2, „Konfigurieren von Standard-Konfigurationsoptionen (IPv6) für DHCP-Clients“.
7. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.3.9.4

Eine Hostgruppe löschen

Um eine Hostgruppe zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die Hostgruppe, indem Sie Folgendes eingeben:
   - **Für IPv4**

```
no services dhcpserver host-groups name
```

- **Für IPv6**

```
no services dhcpserver6 host-groups name
```

Erläuterung:

- *name* ist die Bezeichnung der Hostgruppe

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.3.10

DHCP-Hosts verwalten

Host-Einträge weisen einem bestimmten Client Einstellungen anhand seiner Ethernet-MAC-Adresse zu.

INHALT

- Abschnitt 7.3.10.1, „Eine Liste der Hosts anzeigen“
- Abschnitt 7.3.10.2, „Einen Host hinzufügen“
- Abschnitt 7.3.10.3, „Konfigurieren von Optionen für einen Host“
- Abschnitt 7.3.10.4, „Hosts löschen“

Abschnitt 7.3.10.1

Eine Liste der Hosts anzeigen

Um eine Liste der Hosts auf dem DHCP-Server anzuzeigen, geben Sie Folgendes ein:

- **Für IPv4**

```
show running-config services dhcpserver host
```

- **Für IPv6**

```
show running-config services dhcpserver6 host
```

Falls Hosts konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config services dhcpserver host APE-INT
services
 dhcpserver
  host APE-INT
   options
    hardware mac 00:01:C0:0B:B7:71
    fixed-ip       192.168.0.60
    unknown-client allow
    subnet         SUB2
    client
     hostname APE-INT
     no subnetmask
     no default-route
     no broadcast
     no domain
     no dns-server
     no static-route
     no nis server
     no nis domain
    !
```

```
    !
  !
 !
!
```

Falls keine Hosts konfiguriert wurden, fügen Sie je nach Bedarf Hosts hinzu. Weitere Informationen finden Sie unter Abschnitt 7.3.10.2, „Einen Host hinzufügen“.

Abschnitt 7.3.10.2
Einen Host hinzufügen

Um einen Host zu einem DHCP-Server hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den Host hinzu, indem Sie Folgendes eingeben:
   - **Für IPv4**
     ```
     services dhcpserver host name
     ```
   - **Für IPv6**
     ```
     services dhcpserver6 host name
     ```

   Erläuterung:

   - *name* ist die Bezeichnung des Hosts
3. Konfigurieren Sie die Optionen für den Host. Für weitere Informationen siehe Abschnitt 7.3.10.3, „Konfigurieren von Optionen für einen Host“.
4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.3.10.3
Konfigurieren von Optionen für einen Host

Um Optionen für einen Host auf dem DHCP-Server zu konfigurieren, gehen Sie folgendermaßen vor:

HINWEIS
Für einen Host eingestellte Optionen übersteuern die für den DHCP-Server eingestellten Optionen.

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu:
   - **Für IPv4**
     services » dhcpserver » hosts » {host} » options
   - **Für IPv6**
     services » dhcpserver6 » hosts » {host} » options

   Wobei *{host}* die Bezeichnung des Hosts ist.
3. Konfigurieren Sie die Hardware-Einstellungen mithilfe der folgenden Parameter:

Parameter	Beschreibung
type { type }	**Zusammenfassung:** { fddi, token-ring, ethernet } **Standard:** ethernet

Parameter	Beschreibung
	Der Typ der Netzwerk-Hardware, die vom Client verwendet wird und mit dem Host-Eintrag verbunden ist.
mac { mac }	**Zusammenfassung:** Eine Zeichenkette mit 17 Zeichen Die physische Netzwerkadresse des Clients. Beachten Sie, dass dies dem Hardwaretyp entspricht, z. B. der MAC-Adresse für das Ethernet. Dieser Parameter ist obligatorisch.

4. Konfigurieren Sie die Lease-Zeiteinstellungen mithilfe der folgenden Parameter:

Parameter	Beschreibung
default { default }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl **Standard:** 600 Die minimale Lease-Zeit in Sekunden, die der Server den Clients anbietet.
maximum { maximum }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl **Standard:** 7200 Die maximale Lease-Zeit in Sekunden, die der Server den Clients anbietet.

5. Konfigurieren Sie die Client-Einstellungen mithilfe der folgenden Parameter:

- **Für IPv4**

Parameter	Beschreibung
fixed-ip { fixed-ip }	**Zusammenfassung:** Eine Zeichenkette mit 7 bis 15 Zeichen Die IP-Adresse, die der Server dem passenden Client zuweist. Dieser Parameter ist obligatorisch.
unknown-client { unknown-client }	**Zusammenfassung:** { allow, deny, ignore } Maßnahmen für bisher nicht registrierte Clients
shared-network { shared-network }	**Zusammenfassung:** Eine Zeichenkette Das gemeinsame Netzwerk, zu dem der Host gehört.
subnet { subnet }	**Zusammenfassung:** Eine Zeichenkette Das Subnetz, zu dem der Host gehört.
host-groups { host-groups }	**Zusammenfassung:** Eine Zeichenkette Die Host-Gruppen, zu denen dieser Host gehört.

- **Für IPv6**

Parameter	Beschreibung
fixed-ip { fixed-ip }	**Zusammenfassung:** Eine Zeichenkette mit 6 bis 40 Zeichen Die IPv6-Adresse, die der Server dem passenden Client zuweist.
fixed-prefix6 { fixed-prefix6 }	**Zusammenfassung:** Eine Zeichenkette mit 4 bis 43 Zeichen Die IPv6-Präfix-Delegation, die der Server dem passenden Client zuweist.
unknown-client { unknown-client }	**Zusammenfassung:** { allow, deny, ignore } Maßnahmen für bisher nicht registrierte Clients
shared-network { shared-network }	**Zusammenfassung:** Eine Zeichenkette Das gemeinsame Netzwerk, zu dem der Host gehört.
subnet6 { subnet6 }	**Zusammenfassung:** Eine Zeichenkette

Parameter	Beschreibung
	Das Subnetz, zu dem der Host gehört.
host-groups { host-groups }	**Zusammenfassung:** Eine Zeichenkette Die Host-Gruppen, zu denen dieser Host gehört.

6. [Optional] Konfigurieren Sie die Konfigurationsoptionen für DHCP-Clients im Host. Weitere Informationen finden Sie in Abschnitt 7.3.5.1, „Konfigurieren von Standard-Konfigurationsoptionen (IPv4) für DHCP-Clients“ oder Abschnitt 7.3.5.2, „Konfigurieren von Standard-Konfigurationsoptionen (IPv6) für DHCP-Clients“.
7. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.3.10.4
Hosts löschen

Um einen Host zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den Host, indem Sie Folgendes eingeben:
   - **Für IPv4**
     ```
     no services dhcpserver host name
     ```
   - **Für IPv6**
     ```
     no services dhcpserver6 host name
     ```

   Erläuterung:
   - *`name`* ist die Bezeichnung des Hosts
3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.3.11
Adressen-Pools (IPv4) verwalten

Adressen-Pools legen einen Bereich von IP-Adressen fest, die DHCP-Clients im gleichen Subnetz zugeordnet werden können.

INHALT

- Abschnitt 7.3.11.1, „Eine Liste der Adress-Pools (IPv4) anzeigen“
- Abschnitt 7.3.11.2, „Hinzufügen eines Adress-Pools (IPv4)“
- Abschnitt 7.3.11.3, „Einen Adress-Pool (IPv4) löschen“

Abschnitt 7.3.11.1
Eine Liste der Adress-Pools (IPv4) anzeigen

Um eine Liste der für ein DHCP-Subnetz konfigurierten Adress-Pools anzuzeigen, geben Sie Folgendes ein:

```
show running-config services dhcpserver subnet-name name options ippool
```

Erläuterung:

- *name* ist die Bezeichnung des Subnetzes

Falls Pools konfiguriert wurden, wird eine Tabelle oder Liste ähnlich der Folgenden angezeigt:

```
ruggedcom# show running-config services dhcpserver subnet-name Local options ippool
services
 dhcpserver
  subnet Local
   options
    ippool pool1
     no unknown-client
     iprange 172.0.0.0
      end 172.0.0.1
     !
     option82 class1
      remote-id  00:00:00:01:03:01
      circuit-id 00:00:00:01:01:01
     !
    !
   !
  !
 !
!
```

Falls keine Pools konfiguriert wurden, fügen Sie je nach Bedarf Pools hinzu. Weitere Informationen finden Sie unter Abschnitt 7.3.11.2, „Hinzufügen eines Adress-Pools (IPv4)“.

Abschnitt 7.3.11.2

Hinzufügen eines Adress-Pools (IPv4)

Um einen Adress-Pool zum DHCP-Subnetz hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den Adress-Pool hinzu, indem Sie Folgendes eingeben:

   ```
   services dhcpserver subnet-name name options ippool description
   ```

   Erläuterung:

   - *name* ist die Bezeichnung des Subnetzes
   - *description* ist die Bezeichnung des IP-Pools
3. Konfigurieren Sie die Lease-Zeiteinstellungen mithilfe der folgenden Parameter:

Parameter	Beschreibung
default { default }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl **Standard:** 600 Die minimale Lease-Zeit in Sekunden, die der Server den Clients anbietet.
maximum { maximum }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl **Standard:** 7200 Die maximale Lease-Zeit in Sekunden, die der Server den Clients anbietet.

4. Konfigurieren Sie die Client- und Failover-Einstellungen mithilfe der folgenden Parameter:

Parameter	Beschreibung
unknown-client { unknown-client }	**Zusammenfassung:** { allow, deny, ignore } Maßnahmen für bisher nicht registrierte Clients
failover-peer { failover-peer }	**Zusammenfassung:** Eine Zeichenkette mit 7 bis 15 Zeichen Die IP-Adresse eines DHCP-Peer-Servers, falls ein Failover-Pool eingerichtet wurde.

5. Fügen Sie einen oder mehrere IP-Bereiche zum Pool hinzu. Weitere Informationen finden Sie unter Abschnitt 7.3.13.2, „Hinzufügen eines IP-Bereichs (IPv4)“.
6. Fügen Sie eine oder mehrere Option82-Klassen zum Pool hinzu. Weitere Informationen finden Sie unter Abschnitt 7.3.18.2, „Hinzufügen einer Option 82-Klasse zu einem Adress-Pool (IPv4)“.
7. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.3.11.3
Einen Adress-Pool (IPv4) löschen

Um einen Adress-Pool zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den Adress-Pool, indem Sie Folgendes eingeben:

```
no services dhcpserver subnet-name name options ippool description
```

   Erläuterung:

   - *`name`* ist die Bezeichnung des Subnetzes
   - *`description`* ist die Bezeichnung des IP-Pools
3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.3.12
Adressen-Pools (IPv6) verwalten

Adressen-Pools legen einen Bereich von IP-Adressen fest, die DHCP-Clients im gleichen Subnetz zugeordnet werden können.

INHALT

- Abschnitt 7.3.12.1, „Eine Liste der Adress-Pools (IPv6) anzeigen“
- Abschnitt 7.3.12.2, „Hinzufügen eines Adress-Pools (IPv6)“
- Abschnitt 7.3.12.3, „Einen Adress-Pool (IPv6) löschen“

Abschnitt 7.3.12.1
Eine Liste der Adress-Pools (IPv6) anzeigen

Um eine Liste der für ein DHCP-Subnetz konfigurierten Adress-Pools anzuzeigen, geben Sie Folgendes ein:

```
show running-config services dhcpserver6 subnet6-name name options ippool6
```

Erläuterung:

- *name* ist die Bezeichnung des Subnetzes

Falls Pools konfiguriert wurden, wird eine Tabelle oder Liste ähnlich der Folgenden angezeigt:

```
ruggedcom# show running-config services dhcpserver6 subnet6-name options ippool6
services
 dhcpserver6
  subnet6-name sub
   options
    ippool6 pool1
     iprange6 2001:db8:2728::2221
      end 2001:db8:2728::2230
     !
     agent class1
      remote-id     01:02:03:04:05:06
      subscriber-id 01:02:03:04
     !
    !
   !
  !
 !
!
!
```

Falls keine Pools konfiguriert wurden, fügen Sie je nach Bedarf Pools hinzu. Weitere Informationen finden Sie unter Abschnitt 7.3.12.2, „Hinzufügen eines Adress-Pools (IPv6)“.

Abschnitt 7.3.12.2
Hinzufügen eines Adress-Pools (IPv6)

Um einen Adress-Pool zum DHCP-Subnetz hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den Adress-Pool hinzu, indem Sie Folgendes eingeben:

   ```
   services dhcpserver6 subnet6-name name options ippool6 ippoolname
   ```

   Erläuterung:

   - *name* ist die Bezeichnung des Subnetzes
   - *ippoolname* ist die Bezeichnung des IPv6-Pools
3. Konfigurieren Sie die Lease-Zeiteinstellungen mithilfe der folgenden Parameter:

Parameter	Beschreibung
default { default }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl **Standard:** 600 Die minimale Lease-Zeit in Sekunden, die der Server den Clients anbietet.
maximum { maximum }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl **Standard:** 7200

Parameter	Beschreibung
	Die maximale Lease-Zeit in Sekunden, die der Server den Clients anbietet.

4. Konfigurieren Sie die Client- und Failover-Einstellungen mithilfe der folgenden Parameter:

Parameter	Beschreibung
unknown-client { unknown-client }	**Zusammenfassung:** { allow, deny, ignore } Maßnahmen für bisher nicht registrierte Clients

5. [Optional] Fügen Sie einen oder mehrere IP-Bereiche zum Pool hinzu. Weitere Informationen finden Sie unter Abschnitt 7.3.14.2, „Hinzufügen eines IP-Bereichs (IPv6)“.
6. [Optional] Fügen Sie ein oder mehrere Subnetze zum Pool hinzu. Weitere Informationen finden Sie unter Abschnitt 7.3.17.2, „Ein IPv6-Subnetz hinzufügen“.
7. [Optional] Fügen Sie ein oder mehrere temporäre Subnetze zum Pool hinzu. Weitere Informationen finden Sie unter Abschnitt 7.3.16.2, „Ein temporäres Subnetz hinzufügen“.
8. [Optional] Fügen Sie ein oder mehrere Präfixe zum Pool hinzu. Weitere Informationen finden Sie unter Abschnitt 7.3.15.2, „Ein IPv6-Präfix hinzufügen“.
9. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.3.12.3
Einen Adress-Pool (IPv6) löschen

Um einen Adress-Pool zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den Adress-Pool, indem Sie Folgendes eingeben:

```
no services dhcpserver subnet6-name name options ippool6 ippoolname
```

   Erläuterung:

   - *`name`* ist die Bezeichnung des Subnetzes
   - *`ippoolname`* ist die Bezeichnung des IPv6-Subnetzes

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.3.13
IP-Bereiche verwalten (IPv4)

Ein IP-Bereich stellt einen Bereich von IP-Adressen dar, die der DHCP-Server den Clients zuweisen kann. IP-Adressen außerhalb des eingestellten Bereichs sind für statisch adressierte Clients vorbehalten.

Ein IP-Bereich kann für ein DHCP-Subnetz und/oder seine(n) zugehörige(n) Adressen-Pool(s) konfiguriert werden.

INHALT

- Abschnitt 7.3.13.1, „Eine Liste der IP-Bereiche (IPv4) anzeigen“

- Abschnitt 7.3.13.2, „Hinzufügen eines IP-Bereichs (IPv4)“
- Abschnitt 7.3.13.3, „Löschen eines IP-Bereichs (IPv4)“

Abschnitt 7.3.13.1
Eine Liste der IP-Bereiche (IPv4) anzeigen

Um eine Liste der IP-Bereiche, die für ein DHCP-Subnetz konfiguriert sind, anzuzeigen, geben Sie Folgendes ein:

- **Bei einem DHCP-Subnetz**

```
show running-config services dhcpserver subnet-name name options iprange
```

- **Bei einem Adress-Pool**

```
show running-config services dhcpserver subnet-name name options ippool description iprange
```

Erläuterung:

- *name* ist die Bezeichnung des Subnetzes
- *description* (sofern zutreffend) ist die Bezeichnung des Adress-Pools

Falls Bereiche konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config services dhcpserver subnet-name Local options iprange
services
 dhcpserver
  subnet Local
   options
    iprange 172.30.144.251
     end 172.30.144.254
    !
   !
  !
 !
!
```

Falls keine IP-Bereiche konfiguriert wurden, fügen Sie je nach Bedarf Bereiche hinzu. Weitere Informationen finden Sie unter Abschnitt 7.3.13.2, „Hinzufügen eines IP-Bereichs (IPv4)“ oder Abschnitt 7.3.14.2, „Hinzufügen eines IP-Bereichs (IPv6)“.

Abschnitt 7.3.13.2
Hinzufügen eines IP-Bereichs (IPv4)

Um einen IP-Bereich zum DHCP-Subnetz oder zu einen seiner zugehörigen Adress-Pools hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den IP-Bereich hinzu, indem Sie Folgendes eingeben:
   - **Für ein DHCP-Subnetz**

```
services dhcpserver subnet-name name options iprange start end end
```

   - **Für einen Adress-Pool**

```
services dhcpserver subnet-name name options ippool description iprange start end end
```

   Erläuterung:

   - *name* ist die Bezeichnung des Subnetzes

- *description* (sofern zutreffend) ist die Bezeichnung des Adress-Pools
- *start* ist der Start-IP-Adress-Pool, den der Server dem Client anbietet
- *end* ist der End-IP-Adress-Pool, den der Server dem Client anbietet

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.3.13.3
Löschen eines IP-Bereichs (IPv4)

Um einen IP-Bereich aus dem DHCP-Subnetz oder aus einem seiner zugehörigen Adress-Pools zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den IP-Bereich, indem Sie Folgendes eingeben:
   - **Für ein DHCP-Subnetz**
     ```
     no dhcpserver subnet-name name options iprange start end end
     ```
   - **Für einen Adress-Pool**
     ```
     no services dhcpserver subnet-name name options ippool description iprange start end end
     ```

   Erläuterung:
   - *name* ist die Bezeichnung des Subnetzes
   - *description* (sofern zutreffend) ist die Bezeichnung des Adress-Pools
   - *start* ist der Start-IP-Adress-Pool, den der Server dem Client anbietet
   - *end* ist der End-IP-Adress-Pool, den der Server dem Client anbietet
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.3.14
IP-Bereiche verwalten (IPv6)

Ein IP-Bereich stellt einen Bereich von IP-Adressen dar, die der DHCP-Server den Clients zuweisen kann. IP-Adressen außerhalb des eingestellten Bereichs sind für statisch adressierte Clients vorbehalten.

Ein IP-Bereich kann für ein DHCP-Subnetz und/oder seine(n) zugehörige(n) Adressen-Pool(s) konfiguriert werden.

INHALT

- Abschnitt 7.3.14.1, „Eine Liste der IP-Bereiche (IPv6) anzeigen“
- Abschnitt 7.3.14.2, „Hinzufügen eines IP-Bereichs (IPv6)“
- Abschnitt 7.3.14.3, „Löschen eines IP-Bereichs (IPv6)“

Abschnitt 7.3.14.1
Eine Liste der IP-Bereiche (IPv6) anzeigen

Um eine Liste der IP-Bereiche, die für ein DHCP-Subnetz konfiguriert sind, anzuzeigen, geben Sie Folgendes ein:

- **Bei einem DHCP-IPv6-Subnetz**

  ```
  show running-config services dhcpserver6 subnet6-name name options iprange6
  ```

- **Bei einem IPv6-Adress-Pool**

  ```
  show running-config services dhcpserver6 subnet6-name name options ippool6 description iprange6
  ```

Erläuterung:

- *name* ist die Bezeichnung des Subnetzes
- *description* (sofern zutreffend) ist die Bezeichnung des Adress-Pools

Falls Bereiche konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config services dhcpserver6 subnet6-name sub options iprange6
services
 dhcpserver6
  subnet6-name sub
   options
    iprange6 2001:db8:2728::2200
     end 2001:db8:2728::2220
    !
   !
  !
 !
!
!
```

Falls keine IP-Bereiche konfiguriert wurden, fügen Sie je nach Bedarf Bereiche hinzu. Weitere Informationen finden Sie unter Abschnitt 7.3.14.2, „Hinzufügen eines IP-Bereichs (IPv6)“.

Abschnitt 7.3.14.2
Hinzufügen eines IP-Bereichs (IPv6)

Um einen IP-Bereich zum DHCP-Subnetz oder zu einen seiner zugehörigen Adress-Pools hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den IP-Bereich hinzu, indem Sie Folgendes eingeben:
   - **Für ein DHCP IPv6-Subnetz**

     ```
     services dhcpserver6 subnet6-name name options iprange6 start end end
     ```

   - **Für einen IPv6-Adress-Pool**

     ```
     services dhcpserver6 subnet6-name name options ippool6 description iprange6 start end end
     ```

   Erläuterung:

   - *name* ist die Bezeichnung des Subnetzes
   - *description* (sofern zutreffend) ist die Bezeichnung des Adress-Pools
   - *start* ist der Start-IP-Adress-Pool, den der Server dem Client anbietet
   - *end* ist der End-IP-Adress-Pool, den der Server dem Client anbietet

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.3.14.3
Löschen eines IP-Bereichs (IPv6)

Um einen IP-Bereich aus dem DHCP-Subnetz oder aus einem seiner zugehörigen Adress-Pools zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den IP-Bereich, indem Sie Folgendes eingeben:
   - **Für ein DHCP IPv6-Subnetz**
     ```
     no dhcpserver6 subnet6-name name options iprange6 start end end
     ```
   - **Für einen IPv6-Adress-Pool**
     ```
     no services dhcpserver6 subnet6-name name options ippool6 description iprange6 start end end
     ```

   Erläuterung:
   - *`name`* ist die Bezeichnung des Subnetzes
   - *`description`* (sofern zutreffend) ist die Bezeichnung des Adress-Pools
   - *`start`* ist der Start-IP-Adress-Pool, den der Server dem Client anbietet
   - *`end`* ist der End-IP-Adress-Pool, den der Server dem Client anbietet
3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.3.15
IPv6-Präfixe verwalten

Es können ein oder mehrere optionale IPv6-Präfixe festgelegt werden, die der Server dem Client anbieten kann.

Eine *prefix6*-Delegation enthält das IPv6-Subnetzwerk und die Präfix-Länge in Bits. Der verwendete Wert für das Subnetzwerk sollte innerhalb des Wertebereichs der umschließenden subnet6-Deklaration liegen.

INHALT

- Abschnitt 7.3.15.1, „Eine Liste der IPv6-Präfixe anzeigen“
- Abschnitt 7.3.15.2, „Ein IPv6-Präfix hinzufügen“
- Abschnitt 7.3.15.3, „Ein IPv6-Präfix löschen“

Abschnitt 7.3.15.1
Eine Liste der IPv6-Präfixe anzeigen

Um eine Liste der IP-Bereiche, die für ein DHCP-Subnetz konfiguriert sind, anzusehen, geben Sie Folgendes ein:

Für DHCP-IPv6-Subnetze

```
show running-config services dhcpserver6 subnet6-name name options prefix6
```

Erläuterung:

- *name* ist die Bezeichnung des Subnetzes

Falls Präfixe konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config services dhcpserver6 subnet6-name sub2 options prefix6
services
 dhcpserver6
  subnet6-name sub2
   options
    prefix6 2001:db8:28d2:f0::
     end  2001:db8:28d2:f0::
     bits 60
    !
   !
  !
 !
!
```

Falls keine Präfixe konfiguriert wurden, fügen Sie je nach Bedarf Bereiche hinzu. Weitere Informationen finden Sie unter Abschnitt 7.3.15.2, „Ein IPv6-Präfix hinzufügen“.

Abschnitt 7.3.15.2

Ein IPv6-Präfix hinzufügen

Um ein Präfix hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie das Präfix hinzu, indem Sie Folgendes eingeben:

   ```
   services dhcpserver6 subnet6-name name options prefix6 prefix
   ```

   Erläuterung:

   - *name* ist die Bezeichnung des Subnetzes
   - *prefix* ist die beginnende IPv6-Präfix-Delegation
3. Projektieren Sie die Konfiguration des IPv6-Bereichs, indem Sie nach Bedarf die folgenden Parameter konfigurieren:

Parameter	Beschreibung
end { end }	**Zusammenfassung:** Eine Zeichenkette mit 6 bis 40 Zeichen Die endende IPv6-Präfix-Delegation, die der Server zum Anbieten an den Client verwendet. Dieser Parameter ist obligatorisch.
bits { bits }	**Zusammenfassung:** Eine vorzeichenlose 8-Bit-Ganzzahl zwischen 1 und 64 Präfix-Delegationen der Bitlänge, die dem Client angeboten werden. Dieser Parameter ist obligatorisch.

4. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.3.15.3
Ein IPv6-Präfix löschen

Um ein Präfix zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie das Präfix, indem Sie Folgendes eingeben:

   ```
   no services dhcpserver6 subnet6-name name options prefix6 prefix
   ```

   Erläuterung:

   - *name* ist die Bezeichnung des Subnetzes
   - *prefix* ist das Präfix
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.3.16
Temporäre Subnetze verwalten

Es können ein oder mehrere optionale IPv6-Subnetze mit temporären Adressen festgelegt werden, die der Server dem Client anbieten kann.

INHALT

- Abschnitt 7.3.16.1, „Eine Liste temporärer Subnetze anzeigen“
- Abschnitt 7.3.16.2, „Ein temporäres Subnetz hinzufügen“
- Abschnitt 7.3.16.3, „Ein temporäres Subnetz löschen“

Abschnitt 7.3.16.1
Eine Liste temporärer Subnetze anzeigen

Um eine Liste der temporären Subnetze anzusehen, geben Sie Folgendes ein:

Für DHCP-IPv6-Subnetze

```
show running-config services dhcpserver6 subnet6-name name options temporarysubnet6
```

Erläuterung:

- *name* ist die Bezeichnung des Subnetzes

Falls temporäre Subnetze konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config services dhcpserver6 subnet6-name sub2 options temporarysubnet6
services
 dhcpserver6
  subnet6-name sub2
   options
    temporarysubnet6 2001:db8:28d2::/112
    !
   !
  !
 !
```

```
!
!
```

Falls keine Präfixe konfiguriert wurden, fügen Sie je nach Bedarf Bereiche hinzu. Weitere Informationen finden Sie unter Abschnitt 7.3.15.2, „Ein IPv6-Präfix hinzufügen“.

Abschnitt 7.3.16.2
Ein temporäres Subnetz hinzufügen

Um ein temporäres Subnetz hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie das Präfix hinzu, indem Sie Folgendes eingeben:

   ```
   services dhcpserver6 subnet6-name name options temporarysubnet6 temporaryname
   ```

   Erläuterung:

   - *name* ist die Bezeichnung des Subnetzes
   - *temporaryname* ist die Bezeichnung des temporären Subnetzes
3. Projektieren Sie die Konfiguration des IPv6-Bereichs, indem Sie nach Bedarf die folgenden Parameter konfigurieren:

Parameter	Beschreibung
{ subnet-number }	**Zusammenfassung:** Eine Zeichenkette mit 4 bis 43 Zeichen Das IPv6-Subnetz mit temporären Adressen, das der Server zum Anbieten an den Client verwendet. Dieser Parameter ist obligatorisch.

4. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.3.16.3
Ein temporäres Subnetz löschen

Um ein Präfix zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie das Präfix, indem Sie Folgendes eingeben:

   ```
   no services dhcpserver6 subnet6-name name options temporarysubnet6 temporaryname
   ```

   Erläuterung:

   - *name* ist die Bezeichnung des Subnetzes
   - *temporaryname* ist das temporäre Subnetz
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.3.17

IPv6-Subnetze verwalten

Es können ein oder mehrere optionale IPv6-Subnetze festgelegt werden, die der Server dem Client anbieten kann.

INHALT

- Abschnitt 7.3.17.1, „Eine Liste der IPv6-Subnetze anzeigen“
- Abschnitt 7.3.17.2, „Ein IPv6-Subnetz hinzufügen“
- Abschnitt 7.3.17.3, „Ein IPv6-Subnetz löschen“

Abschnitt 7.3.17.1

Eine Liste der IPv6-Subnetze anzeigen

Um eine Liste der IPv6-Subnetze anzusehen, geben Sie Folgendes ein:

```
show running-config services dhcpserver6 subnet6-name name options subnet6
```

Erläuterung:

- *name* ist die Bezeichnung des Subnetzes

Falls IPv6-Subnetze konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config services dhcpserver6 subnet6-name sub2 options subnet6
services
 dhcpserver6
  subnet6-name sub2
   options
    subnet6 2001:db8:28d2::/64
    !
   !
  !
 !
!
```

Falls keine Präfixe konfiguriert wurden, fügen Sie je nach Bedarf Bereiche hinzu. Weitere Informationen finden Sie unter Abschnitt 7.3.15.2, „Ein IPv6-Präfix hinzufügen“.

Abschnitt 7.3.17.2

Ein IPv6-Subnetz hinzufügen

Um ein IPv6-Subnetz hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie das Ipv6-Subnetz hinzu, indem Sie Folgendes eingeben:

   ```
   services dhcpserver6 subnet6-name name options subnet6 subnet6name
   ```

   Erläuterung:

   - *name* ist die Bezeichnung des Subnetzes
   - *subnet6name* ist die Bezeichnung des IPv6-Subnetzes
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
{ subnet-number }	**Zusammenfassung:** Eine Zeichenkette mit 4 bis 43 Zeichen Das IPv6-Subnetz, das der Server zum Anbieten an den Client verwendet. Dieser Parameter ist obligatorisch.

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.3.17.3
Ein IPv6-Subnetz löschen

Um ein IPv6-Subnetz zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie das Präfix, indem Sie Folgendes eingeben:

```
no services dhcpserver6 subnet6-name name options subnet6 subnet6name
```

Erläuterung:

- *`name`* ist die Bezeichnung des Subnetzes
- *`subnet6name`* ist die Bezeichnung des IPv6-Subnetzes

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.3.18
Option 82-Klassen für Adress-Pools (IPv4) verwalten

Option 82 oder die Informationsoption des DHCP-Relais-Agenten schützt den DHCP-Server vor IP-Adressen-Spoofing und DHCP IP Starvation Attacks, indem Informationen über die Netzwerkquelle von IP-Adressanforderungen bereitgestellt werden. Wenn ein DHCP-Client eine IP-Adressanforderung ausgibt, fügt ein DHCP-Relais-Agent die Option 82-Informationen zum Paketkopf der Anforderung hinzu. Der Relais-Agent leitet die Anforderung dann an den DHCP-Server weiter. Wenn der DHCP-Server feststellt, dass die Anforderung aus einer nicht vertrauenswürdigen Quelle stammt, wird sie abgewiesen.

Der DHCP-Server muss so konfiguriert sein, dass er Option 82-Informationen akzeptiert, wenn er die Vertrauenswürdigkeit der von einem DHCP-Client verwendeten Netzwerkschnittstelle feststellen soll. Dies kann global oder für einzelne Subnetze erfolgen.

WICHTIG!
Für weitere Informationen, wie Sie den DHCP-Server aktivieren, damit er Option 82-Informationen annimmt, siehe Abschnitt 7.3.4, „Konfigurieren von Optionen für den DHCP-Server“ oder Abschnitt 7.3.8.3, „Optionen für Subnetze konfigurieren“.

Sobald Option 82 aktiviert ist, müssen Komponenten (oder Klassen) für Unteroptionen für jeden Adress-Pool definiert werden, der DHCP-Clients enthält, die Option 82-Informationen senden. Dieser Abschnitt beschreibt, wie Komponenten der Unteroptionen für Adress-Pools verwaltet werden.

INHALT

- Abschnitt 7.3.18.1, „Eine Liste von Option 82-Klassen für Adress-Pools (IPv4) anzeigen“
- Abschnitt 7.3.18.2, „Hinzufügen einer Option 82-Klasse zu einem Adress-Pool (IPv4)“
- Abschnitt 7.3.18.3, „Eine Option 82-Klasse aus einem Adress-Pool (IPv4) löschen“

Abschnitt 7.3.18.1

Eine Liste von Option 82-Klassen für Adress-Pools (IPv4) anzeigen

Um eine Liste von Option 82-Klassen, die für einen Adress-Pool konfiguriert sind, anzuzeigen, geben Sie Folgendes ein:

```
show running-config services dhcpserver subnet-name name options ippool description option82
```

Erläuterung:

- *name* ist die Bezeichnung des Subnetzes
- *description* ist die Bezeichnung des Adress-Pools

Falls Klassen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config services dhcpserver subnet Local options ippool pool1 option82
services
 dhcpserver
  subnet Local
   options
    ippool pool1
     option82 class1
      remote-id  00:00:00:01:03:01
      circuit-id 00:00:00:01:01:01
     !
    !
   !
  !
 !
!
```

Falls keine Option 82-Klassen konfiguriert wurde, fügen Sie je nach Bedarf Klassen hinzu. Weitere Informationen finden Sie unter Abschnitt 7.3.18.2, „Hinzufügen einer Option 82-Klasse zu einem Adress-Pool (IPv4)“.

Abschnitt 7.3.18.2

Hinzufügen einer Option 82-Klasse zu einem Adress-Pool (IPv4)

Um eine Option 82-Klasse einem Adress-Pool hinzuzufügen, gehen Sie wie folgt vor:

HINWEIS
Das Format des Werts `circuit-id` *ist* ***00:00:00:{vlan}:{slot}:{port}****. Wenn der entfernte Host mit LM3/1 im VLAN 1 verschaltet ist, dann wäre die ID 00:00:00:01:03:01.*

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.

2. Fügen Sie den Pool hinzu, indem Sie Folgendes eingeben:

```
services dhcpserver subnet-name name options ippool description option82 class
```

Erläuterung:

- *name* ist die Bezeichnung des Subnetzes
- *description* ist die Bezeichnung des Adress-Pools
- *class* ist die Bezeichnung der Option82-Klasse

3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
remote-id { remote-id }	**Zusammenfassung:** Eine Zeichenkette mit 17 Zeichen Gibt die Informationen zum entfernten Host-Ende des Netzwerks an. Dieser Parameter ist obligatorisch.
circuit-id { circuit-id }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 17 Zeichen Gibt die lokalen Informationen an, auf welches Netzwerk die Anforderung eingetroffen ist (d. h. 00:02:03:02) Dieser Parameter ist obligatorisch.

4. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.3.18.3
Eine Option 82-Klasse aus einem Adress-Pool (IPv4) löschen

Um eine Option 82-Klasse aus einem Adress-Pool zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die Klasse, indem Sie Folgendes eingeben:

```
no services dhcpserver subnet-name name options ippool description option82 class
```

Erläuterung:

- *name* ist die Bezeichnung des Subnetzes
- *description* ist die Bezeichnung des Adress-Pools
- *class* ist die Bezeichnung der Option 82-Klasse

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.4
Statische DNS verwalten

Dieser Abschnitt beschreibt, wie sie eine statische oder feste IP-Adresse für das Gerät reservieren können. Obwohl normalerweise eine zufällige Adresse von einem *dynamischen* DNS-Server zugeteilt wird, kann die Anforderung

einer festen Adresse von einem statischen DNS-Server für die Verbindung mit virtuellen privaten Netzwerken (VPN) oder anderen entfernten Adressdiensten, die nur bestimmten IP-Adressen vertrauen, erforderlich sein.

INHALT

- Abschnitt 7.4.1, „Domainnamen verwalten“
- Abschnitt 7.4.2, „Domain-Name-Server verwalten“

Abschnitt 7.4.1

Domainnamen verwalten

Der DNS-Dienst kann so konfiguriert werden, dass er einen oder mehrere Domainnamen bei der Abfrage eines Domain-Name-Servers verwendet. Die Liste der Domainnamen kann die Domain enthalten, zu der der Router gehört, sowie andere Domains, die für die Suche nach einem unqualifizierten Hostnamen verwendet werden können (als wäre es ein lokaler Host).

INHALT

- Abschnitt 7.4.1.1, „Eine Liste der Domain-Namen anzeigen“
- Abschnitt 7.4.1.2, „Einen Domain-Namen hinzufügen“
- Abschnitt 7.4.1.3, „Einen Domain-Namen löschen“

Abschnitt 7.4.1.1

Eine Liste der Domain-Namen anzeigen

Um eine Liste der Domain-Namen anzusehen, geben Sie Folgendes ein:

```
show running-config dns search
```

Falls Domain-Namen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config admin dns search
admin
 dns
  search ruggedcom.com
  !
 !
!
```

Falls keine Domain-Namen konfiguriert wurden, fügen Sie je nach Bedarf Namen hinzu. Weitere Informationen finden Sie unter Abschnitt 7.4.1.2, „Einen Domain-Namen hinzufügen“.

Abschnitt 7.4.1.2

Einen Domain-Namen hinzufügen

Um einen Domain-Namen hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den Domain-Namen durch die folgende Eingabe hinzu:

```
admin dns search name
```

Erläuterung:

- *name* ist die Bezeichnung der Domain

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.4.1.3
Einen Domain-Namen löschen

Um einen Domain-Namen zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den Domain-Namen durch Eingabe von:

```
no admin dns search name
```

Erläuterung:

- *name* ist die Bezeichnung der Domain

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.4.2
Domain-Name-Server verwalten

Für den DNS-Dienst kann eine hierarchische Liste der Domain-Name-Server konfiguriert werden. RUGGEDCOM ROX II nimmt die Verbindung zu jedem Server in der Reihenfolge dieser Liste auf, wenn Domainnamen aufgelöst werden müssen.

INHALT

- Abschnitt 7.4.2.1, „Eine Liste der Domain-Name-Server anzeigen“
- Abschnitt 7.4.2.2, „Einen Domain-Name-Server hinzufügen“
- Abschnitt 7.4.2.3, „Einen Domain-Name-Server löschen“

Abschnitt 7.4.2.1
Eine Liste der Domain-Name-Server anzeigen

Um eine Liste der Domain-Name-Server anzusehen, geben Sie Folgendes ein:

```
show running-config dns server
```

Falls Domain-Name-Server konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config admin dns server
admin
 dns
  server 10.1.1.1
```

```
  !
 !
!
```

Falls keine Domain-Name-Server konfiguriert wurden, fügen Sie je nach Bedarf Server hinzu. Weitere Informationen finden Sie unter Abschnitt 7.4.2.2, „Einen Domain-Name-Server hinzufügen“.

Abschnitt 7.4.2.2
Einen Domain-Name-Server hinzufügen

Um einen Domain-Name-Server hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den Domain-Name-Server durch die folgende Eingabe hinzu:

   ```
   admin dns server address
   ```

   Erläuterung:

   - *address* ist die IP-Adresse des Domain-Name-Servers.
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.4.2.3
Einen Domain-Name-Server löschen

Um einen Domain-Name-Server zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den Domain-Name-Server durch Eingabe von:

   ```
   no admin dns server address
   ```

   Erläuterung:

   - *address* ist die IP-Adresse des Domain-Name-Servers.
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.5
Dynamic DNS (DDNS) verwalten

Aktivieren Sie den Service Dynamic Domain Name Server (DDNS) in RUGGEDCOM ROX II, damit entfernte Hosts über einen festen Hostnamen eine Verbindung mit der Standardschnittstelle des Geräts herstellen können. Der Service Dynamic DNS meldet sich über einen DNS-Client bei einem DNS-Dienstanbieter an und registriert den/die zugewiesenen Hostnamen, mit dem/denen über das Internet auf das Gerät zugegriffen werden kann.

Ein Konto bei einem der unterstützten DDNS-Serviceanbieter ist erforderlich:

- noip.com [http://www.noip.com]
- dyn.com [http://www.dyn.com]

Die Antworten von jedem Dynamic DNS-Serviceanbieter werden vom Dynamic DNS-Client validiert. Wenn eine Antwort als ungültig erkannt wird, wird ein *DDNS Bad Response* -Alarm ausgelöst und der Service vorübergehend deaktiviert. Der Service kann erst wieder aufgenommen werden, wenn der Alarm gelöscht wurde. Informationen zum Konfigurieren dieses Alarms finden Sie unter Abschnitt 5.6.4, „Konfigurieren eines Alarms“.

INHALT

- Abschnitt 7.5.1, „Aktivieren und Konfigurieren von Dynamic DNS“
- Abschnitt 7.5.2, „Dynamische DNS-Server verwalten“
- Abschnitt 7.5.3, „Hostnamen für dynamische DNS-Server verwalten“

Abschnitt 7.5.1

Aktivieren und Konfigurieren von Dynamic DNS

Um Dynamic DNS zu aktivieren und zu konfigurieren, gehen Sie wie folgt vor:

WICHTIG!
Aktualisierungsanfragen werden über den gewählten Serviceanbieter über HTTPS gesendet. Vor der Aktivierung von Dynamic DNS muss der Trusted Certificate Store aktiviert werden. Weitere Informationen finden Sie unter Abschnitt 6.6.2.2, „Den Speicher für vertrauenswürdige Zertifikate aktivieren/deaktivieren“.

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Aktivieren Sie den dynamischen DNS-Client, indem Sie Folgendes eingeben:

```
services ddns enabled true
```

3. Geben Sie **`options`** ein und konfigurieren Sie anschließend je nach Bedarf die folgenden Parameter:

Parameter	Beschreibung
ip-check-interval { ip-check-interval }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 600 und 864000 **Standard:** 1800 Intervall (in Sekunden) zum Prüfen von Änderungen der IP-Adresse
force-update-interval { force-update-interval }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 600 und 2592000 **Standard:** 86400 Intervall (in Sekunden) zum Senden von Updates zum DDNS-Server, selbst wenn er unverändert ist

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.5.2

Dynamische DNS-Server verwalten

Dieser Abschnitt beschreibt, wie Sie eine Verbindung mit einem oder mehreren unterstützten dynamischen DNS-Service-Providern herstellen können.

INHALT

- Abschnitt 7.5.2.1, „Eine Liste der dynamischen DNS-Server anzeigen“
- Abschnitt 7.5.2.2, „Den Status eines DDNS-Servers anzeigen“
- Abschnitt 7.5.2.3, „Einen DDNS-Server hinzufügen“
- Abschnitt 7.5.2.4, „Einen dynamischen DNS-Server löschen“

Abschnitt 7.5.2.1

Eine Liste der dynamischen DNS-Server anzeigen

Um eine Liste der dynamischen DNS-Server anzusehen, geben Sie Folgendes ein:

```
show running-config services ddns servers
```

```
ruggedcom# show running-config services ddns servers | tab
SERVER  ENABLED  USERNAME  PASSWORD                      HOSTNAME
-------------------------------------------------------------------
dyndns  true     admin     $4$wIo7Yd068FRwhYYI0d4IDw==
                                                        host1
noip    true     admin     $4$wIo7Yd068FRwhYYI0d4IDw==
                                                        host2

 !
!
```

Falls keine dynamischen DNS-Server konfiguriert wurden, fügen Sie je nach Bedarf Server hinzu. Weitere Informationen finden Sie unter Abschnitt 7.5.2.3, „Einen DDNS-Server hinzufügen“.

Abschnitt 7.5.2.2

Den Status eines DDNS-Servers anzeigen

Um den Status eines dynamischen DNS-Servers anzuzeigen, geben Sie Folgendes ein:

```
show services ddns servers [ noip | dyndns ] status
```

Wenn der gewählte DDNS-Server aktiviert ist, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show services ddns servers dyndns status
status
 ddns state Enabled
 details
  ddns last success        "Wed Jan 25 11:18:39 2017"
  ddns last ip address     205.206.34.228
  ddns last failure        "Not available"
  ddns last failure reason "Not available"
```

Die Tabelle/Liste liefert die folgenden Informationen:

Parameter	Beschreibung
ddns-state	**Zusammenfassung:** Eine Zeichenkette Zeigt den DDNS-Zustand an

Abschnitt 7.5.2.3
Einen DDNS-Server hinzufügen

Um einen DDNS-Server hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den DDNS-Server hinzu, indem Sie Folgendes eingeben:

```
services ddns servers [ dyndns | noip ]
```

3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
enabled	**Zusammenfassung:** { true, false } **Standard:** false Aktiviert/deaktiviert DDNS-Updates für den Server **HINWEIS** *Es sollte mindestens ein Hostname für den DDNS-Server konfiguriert sein*
username { username }	**Zusammenfassung:** Eine Zeichenkette mit 2 bis 24 Zeichen Der Benutzername des DNS-Servers Dieser Parameter ist obligatorisch.
password { password }	**Zusammenfassung:** Eine Zeichenkette Das Passwort des DNS-Servers Dieser Parameter ist obligatorisch.

4. Legen Sie einen oder mehrere Hostnamen für den Server fest. Weitere Informationen finden Sie in Abschnitt 7.5.3.2, „Einen Hostnamen hinzufügen“.
5. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.5.2.4
Einen dynamischen DNS-Server löschen

Um einen dynamischen DNS-Server zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den dynamischen DNS-Server durch Eingabe von:

```
no services ddns servers [ dyndns | noip ]
```

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.5.3

Hostnamen für dynamische DNS-Server verwalten

Dieser Abschnitt beschreibt, wie Sie Hostnamen für die konfigurierten dynamischen DNS-Server verwalten können.

WICHTIG!
Für jeden konfigurierten dynamischen DNS-Server ist mindestens ein Hostname erforderlich.

INHALT

- Abschnitt 7.5.3.1, „Eine Liste der Host-Namen anzeigen“
- Abschnitt 7.5.3.2, „Einen Hostnamen hinzufügen“
- Abschnitt 7.5.3.3, „Einen Hostnamen löschen“

Abschnitt 7.5.3.1

Eine Liste der Host-Namen anzeigen

Um eine Liste der dynamischen DNS-Server anzusehen, geben Sie Folgendes ein:

```
show running-config services ddns servers [ dyndns | noip ] hostnames
```

Falls Host-Namen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config services ddns servers noip hostnames
services
 ddns
  servers noip
   hostnames host1
   !
  !
 !
!
```

Falls keine Host-Namen konfiguriert wurden, fügen Sie je nach Bedarf Hosts hinzu. Weitere Informationen finden Sie unter Abschnitt 7.5.3.2, „Einen Hostnamen hinzufügen“.

Abschnitt 7.5.3.2

Einen Hostnamen hinzufügen

Um für einen DDNS-Server einen Hostnamen hinzuzufügen, gehen Sie wie folgt vor:

WICHTIG!
Für jeden konfigurierten DDNS-Server ist mindestens ein Hostname erforderlich.

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den Hostnamen hinzu, indem Sie Folgendes eingeben:

   ```
   services ddns servers [ dyndns | noip ] hostnames name
   ```

   Erläuterung: *name* ist der Hostname der vom DDNS-Server aktualisiert werden muss.

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 7.5.3.3
Einen Hostnamen löschen

Um einen Hostnamen zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den DDNS-Server, indem Sie Folgendes eingeben:

   ```
   no services ddns servers [ dyndns | noip ] hostnames name
   ```

   Erläuterung: *`name`* ist der gewünschte Hostname.
3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

8 Layer 2

Dieses Kapitel beschreibt die Layer-2- oder Data-Link-Layer (DLL)-Merkmale von RUGGEDCOM ROX II.

INHALT

- Abschnitt 8.1, „Switched-Ethernet-Ports verwalten“
- Abschnitt 8.2, „Ethernet-Trunk-Schnittstellen verwalten“
- Abschnitt 8.3, „MAC-Adressen verwalten“
- Abschnitt 8.4, „Multicast-Filterung verwalten“
- Abschnitt 8.5, „VLANs verwalten“
- Abschnitt 8.6, „Spanning Tree Protocol (STP) verwalten“

Abschnitt 8.1

Switched-Ethernet-Ports verwalten

Dieser Abschnitt beschreibt, wie Sie Switched-Ethernet-Ports konfigurieren und verwalten können.

INHALT

- Abschnitt 8.1.1, „Eine Liste der Switched-Ethernet-Ports anzeigen“
- Abschnitt 8.1.2, „Einen Switched-Ethernet-Port konfigurieren“
- Abschnitt 8.1.3, „Statistiken der Switched-Ethernet-Ports anzeigen“
- Abschnitt 8.1.4, „Anzeigen der RMON-Portstatistik“
- Abschnitt 8.1.5, „Switched-Ethernet-Port-Statistiken löschen“
- Abschnitt 8.1.6, „Einen Switched-Ethernet-Port zurücksetzen“
- Abschnitt 8.1.7, „Kabel für Switched-Ethernet-Ports testen“

Abschnitt 8.1.1

Eine Liste der Switched-Ethernet-Ports anzeigen

Um eine Liste der Switched-Ethernet-Ports, die auf einem Gerät konfiguriert sind, anzuzeigen, geben Sie Folgendes ein:

```
show running-config interface switch
```

Falls Switched-Ethernet-Ports konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config interface switch
interface
 switch swport 1
  auton      on
  speed      auto
  duplex     auto
  switchport
  no flow-control
  no alias
  rate-limiting
   no ingress-limit
   no egress-limit
  !
  port-security
   no shutdown-time
   no admin-shutdown
   dot1x
    no reauth-enable
   !
  !
  lldp
   no notify
  !
  mcast-filtering
   no gmrp
  !
  cos
   no inspect-tos
  !
  vlan
   pvid 1
   no gvrp-mode
  !
  spanning-tree
   no restricted-role
   no restricted-tcn
  !
 !
.
.
.
```

Abschnitt 8.1.2

Einen Switched-Ethernet-Port konfigurieren

Um einen Switched-Ethernet-Port zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***interface » switch » swport » {port}***, dabei ist *{port}* der Switched-Ethernet-Port.
3. Konfigurieren Sie mit dem/den folgenden Parameter(n) die Porteinstellungen je nach Bedarf:

ACHTUNG!
Sicherheitsgefahr – Risiko eines unberechtigten Zugriffs und/oder einer unberechtigten Nutzung Switched-Ethernet-Ports sind standardmäßig aktiviert. Es ist empfehlenswert, nicht verwendete Ports zu deaktivieren. Freie Ports könnten, sofern sie nicht ordnungsgemäß konfiguriert sind, verwendet werden, um Zugriff auf das Netzwerk hinter dem Gerät zu erlangen.

ACHTUNG!
Konfigurationsgefahr - Gefahr der Datenbeschädigung. Durch Versetzen eines Switched-Ethernet-Ports vom Switchport-Modus in den dedizierten Routingmodus werden automatisch alle von dem Port abhängigen Konfigurationselemente geändert und möglicherweise Teile der Gerätekonfiguration ungültig gemacht. Handelt es sich beispielsweise bei einem Switched-Ethernet-Port um einen Hauptleitungsport wird der Port beim Wechsel in den dedizierten Routingmodus automatisch von der Hauptleitung entfernt und somit die Hauptleitung ungültig gemacht. Eine Hauptleitung muss aus zwei Hauptleitungsports bestehen.

HINWEIS
Switched-Ethernet-Ports im dedizierten Routingmodus können keine Hauptleitungsports sein.

HINWEIS
Die Konfiguration für einen Switched-Ethernet-Port im Switchport-Modus kann bei Entfernen des Ports von einer Hauptleitung wiederhergestellt werden. Die Konfiguration kann jedoch nicht wiederhergestellt werden, wenn sich der Port im dedizierten Routingmodus befindet.

Parameter	Beschreibung
{ slot }	**Zusammenfassung:** Eine Zeichenkette Die Bezeichnung des Modul-Einbauorts gemäß Siebdruck auf der Geräteoberseite.
{ port }	**Zusammenfassung:** Eine Zeichenkette Die Portnummer, wie auf der Frontscheibe des Switch aufgedruckt (oder eine Liste von Ports, wenn sie in einem Port-Trunk gebündelt sind).
enabled	**Zusammenfassung:** { true, false } **Standard:** true Bietet die Option, diese Schnittstelle zu aktivieren oder zu deaktivieren. Wenn die Option nicht markiert ist (d. h. deaktiviert), verhindert die Schnittstelle, dass Frames an dieser Schnittstelle gesendet oder empfangen werden.
auton { auton }	**Zusammenfassung:** Eine Zeichenkette Aktiviert oder deaktiviert die IEEE 802.3 Auto-Negotiation. Die Aktivierung von Auto-Negotiation führt dazu, dass Geschwindigkeit und Duplex bei Link-Erkennung verhandelt werden; beide Endgeräte müssen für bestmögliche Ergebnisse mit Auto-Negotiation kompatibel sein. Dieser Parameter ist obligatorisch.
speed { speed }	**Zusammenfassung:** Eine Zeichenkette Geschwindigkeit (in "megabits-per-second" oder "gigabits-per-second"). Ist Auto-Negotiation aktiviert, ist dies das Geschwindigkeitspotential, das vom Auto-Negotiations-Verfahren angekündigt wird. Ist Auto-Negotiation deaktiviert, wird der Port explizit zu diesem Geschwindigkeitsmodus gezwungen. AUTO bedeutet das Ankündigen aller unterstützten Geschwindigkeitsmodi. Dieser Parameter ist obligatorisch.
duplex { duplex }	**Zusammenfassung:** Eine Zeichenkette Ist Auto-Negotiation aktiviert, ist dies die Duplexkapazität, die vom Auto-Negotiations-Verfahren angekündigt wird. Ist Auto-Negotiation deaktiviert, wird der Port explizit zu diesem Duplexmodus gezwungen. AUTO bedeutet das Ankündigen aller unterstützten Duplexmodi. Dieser Parameter ist obligatorisch.
link-alarms	**Zusammenfassung:** { true, false } **Standard:** true

Parameter	Beschreibung
	Das Deaktivieren von Link-Alarmen („link-alarms") verhindert, dass Alarme und "LinkUp"- und "LinkDown"-SNMP-Traps für diese Schnittstelle versendet werden. Link-Alarme können für das gesamte System auch unter "admin / alarm-cfg" verwaltet werden.
switchport	**Zusammenfassung:** { true, false } Versetzt den physikalischen Port entweder in Switched-Modus oder in einen bestimmten Routing-Modus.
flow-control	Während starkem Netzwerkverkehr ist die Flusskontrolle hilfreich, um den Verlust von Frames zu verhindern.
on-demand	Diese Schnittstelle wird nur on-Demand angesprochen
lfi	Linkfehler-Anzeige (LFI) ist spezifisch für FX-Schnittstellen.
ip-address-src { ip-address-src }	**Zusammenfassung:** { static, dynamic } **Standard:** static Zeigt an, ob die IP-Adresse statisch oder dynamisch über DHCP oder BOOTP zugewiesen ist. Die Option DYNAMIC wird gewöhnlich für eine dynamisch zugewiesene IP-Adresse eingesetzt. Sie schaltet zwischen BOOTP und DHCP, bis sie die Antwort vom entsprechenden Server erhält. Bei nicht verwalteten Schnittstellen muss dies statisch sein.
ipv6-address-src { ipv6-address-src }	**Zusammenfassung:** { static, dynamic } **Standard:** static Zeigt an, ob die IPv6-Adresse statisch oder dynamisch über DHCPv6 zugewiesen ist. Die Option DYNAMIC wird gewöhnlich für eine dynamisch zugewiesene IPv6-Adresse eingesetzt. Bei nicht verwalteten Schnittstellen muss dies statisch sein.
proxyarp	Aktiviert/deaktiviert, dass das VLAN auf ARP-Anfragen für andere Hosts als sich selbst antwortet
mtu { mtu }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 68 und 9216 **Standard:** 1500 Maximale Übertragungseinheit (größte zulässige Paketgröße für diese Schnittstelle).
alias { alias }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 64 Zeichen Der SNMP-Aliasname der Schnittstelle.
operating-mode { operating-mode }	**Zusammenfassung:** { PRP Redbox } **Standard:** PRP Redbox Aktuelle Betriebsart für diesen RNA-Port.
life-check-interval { life-check-interval }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 0 und 300 **Standard:** 2 Intervall zwischen gesendeten PRP_Supervision-Frames, in einer Dauer von Sekunden.
node-forget-time	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl **Standard:** 60 Wählt die Dauer aus, nach der ein Knoteneintrag aus der Knoten-Tabelle gelöscht wird.
proxy-node-forget-time	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl **Standard:** 60 Wählt die Dauer aus, nach der ein Knoteneintrag aus der Proxy-Knoten-Tabelle gelöscht wird.
entry-forget-time	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl **Standard:** 40 Wählt die Dauer aus, nach der ein Eintrag aus der Tabelle für die Duplikatsentfernung gelöscht wird.
proxy-node-max-entries	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl

Parameter	Beschreibung
	Standard: 128 Maximale Anzahl an Proxy-Knoten, die vom Gerät verarbeitet werden können
ingress-limit { ingress-limit }	**Zusammenfassung:** { disabled } oder eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 62 und 256000 **Standard:** 1000 Die Datenrate in Kbaud, bei der der Switch beginnt, empfangene Frames (der Art, wie sie von den Parametern für eingehende Frames beschrieben sind) zu verwerfen. Der gültige Bereich entspricht 62 bis 256000 Kbaud. Der Standardwert ist 1000 Kbaud. Wenn nichts eingestellt (gelöscht), ist diese Funktion deaktiviert.
ingress-frames { ingress-frames }	**Zusammenfassung:** { broadcast, multicast, mcast-flood-ucast, all } **Standard:** broadcast Dieser Parameter spezifiziert die Art der Frames zur Begrenzung der Datenrate an diesem Port. Dies gilt nur für empfangene Frames: • BROADCAST : Es werden nur Broadcast-Frames begrenzt. • MULTICAST : Alle Multicast-Frames (einschließlich Broadcast) werden begrenzt. • MCAST-FLOOD-UCAST : Alle Multicast-Frames (einschließlich Broadcast) werden begrenzt. Unicast wird nicht begrenzt. • ALL : Alle Frames (Multicast wie Unicast) werden begrenzt.
egress-limit { egress-limit }	**Zusammenfassung:** { disabled } oder eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 62 und 256000 **Standard:** disabled Die maximale Datenrate in Kbaud, bei der der Switch Frames (Multicast, Broadcast und Unicast) an diesem Port überträgt. Der Switch wird Frames verwerfen, um bei Bedarf diese Rate zu erreichen. Der gültige Bereich entspricht 62 bis 256000 Kbaud. Wenn nichts eingestellt ist, ist diese Funktion deaktiviert.
admin-status { admin-status }	**Zusammenfassung:** { tx-only, rx-only, rx-tx, no-lldp } **Standard:** rx-tx • no-lldp : Der lokale LLDP Agent kann weder LLDP-Frames übertragen noch empfangen. • rxTx : Der lokale LLDP Agent kann LLDP-Frames über den Port sowohl übertragen als auch empfangen. • txOnly : Der lokale LLDP Agent kann LLDP-Frames nur übertragen. • rxOnly : Der lokale LLDP Agent kann LLDP-Frames nur empfangen.
notify	Das Deaktivieren von Benachrichtigungen verhindert, dass vom LLDP Agent für eine bestimmte Schnittstelle Benachrichtigungen gesendet und Alarme erzeugt werden.
gmrp { gmrp }	**Zusammenfassung:** { advertise_only, learn_advertise } GMRP (GARP Multicast Registration Protocol)-Betrieb am Port. Es gibt mehrere GMRP-Betriebsarten: • DISABLED : Der Port ist zu keiner GMRP-Verarbeitung fähig. • ADVERTISE ONLY : Der Port erkennt alle im Switch vorhandenen MCAST-Adressen (konfiguriert oder gelernt), lernt aber keine MCAST-Adressen. • ADVERTISE and LEARN : Der Port erkennt alle im Switch vorhandenen MCAST-Adressen (konfiguriert oder gelernt) und kann dynamisch MCAST-Adressen lernen.
default-priority { default-priority }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 0 und 7 **Standard:** 0 Die Priorität von Frames, die an diesem Port empfangen werden und nicht aufgrund des Frame-Inhalts priorisiert sind (z. B. Prioritätsfeld im VLAN-Tag, DiffServ-Feld im IP-Header, priorisierte MAC-Adresse).
inspect-tos	Aktiviert oder deaktiviert das Parsen des Feldes Type-of-Service (ToS) im IP-Header der empfangenen Frames, um festzulegen, welcher Berechtigungsklasse (CoS, en: Class of Service) sie zugewiesen werden sollen. Ist das ToS-Parsen aktiviert, verwendet der Switch die differenzierten Dienste-Bits im Feld TOS.
pvid { pvid }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 1 und 4094

Parameter	Beschreibung
	Die VLAN-Kennung des Ports gibt die VLAN-ID an, die nicht markierten (und als 802.1p Priorität markierten) Frames zugeordnet ist, die auf diesem Port empfangen werden. Frames, die mit einer VLAN-ID ungleich Null markiert sind, sind stets der VLAN-ID zugeordnet, die vom Frame-Tag abgerufen wurde.
type { type }	**Zusammenfassung:** { edge, trunk, pvlanedge } **Standard:** edge So bestimmt der Port seine Mitgliedschaft in VLANs. Es gibt verschiedene Port-Typen: • EDGE : Der Port ist nur Mitglied eines VLAN (sein natives, vom Parameter 'PVID' festgelegtes VLAN). • PVLAN Edge : Der Port leitet im selben VLAN keinen Verkehr an andere PVLAN Edge-Ports weiter. • TRUNK : Der Port ist automatisch Mitglied aller konfigurierten VLANs. Frames, die von einem Trunk-Port an alle VLANs, außer dem nativen VLAN des Ports, ausgesendet werden, sind immer getaggt. Er kann auch so konfiguriert sein, dass er GVRP für automatische VLAN-Konfiguration verwendet.
format { format }	**Zusammenfassung:** { untagged, tagged } **Standard:** untagged Zeigt an, ob Frames, die über den Port auf seinem nativen VLAN (angegeben durch den Parameter 'PVID') übertragen werden, getaggt oder nicht getaggt sind.
gvrp-mode { gvrp-mode }	**Zusammenfassung:** { advertise_only, learn_advertise } GVRP (Generic VLAN Registration Protocol)-Betrieb am Port. Es gibt mehrere GVRP-Betriebsarten: • DISABLED : Der Port ist zu keiner GVRP-Verarbeitung fähig. • ADVERTISE ONLY : Der Port erkennt alle im Switch vorhandenen VLANs (konfiguriert oder gelernt), lernt aber keine VLANs. • ADVERTISE and LEARN : Der Port erkennt alle im Switch vorhandenen VLANs (konfiguriert oder gelernt) und kann dynamisch VLANs lernen.

4. Konfigurieren Sie mit dem/den folgenden Parameter(n) die Einstellungen für "Rate Limiting" je nach Bedarf:

Parameter	Beschreibung
ingress-limit { ingress-limit }	**Zusammenfassung:** { disabled } oder eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 62 und 256000 **Standard:** 1000 Die Datenrate in Kbaud, bei der der Switch beginnt, empfangene Frames (der Art, wie sie von den Parametern für eingehende Frames beschrieben sind) zu verwerfen. Der gültige Bereich entspricht 62 bis 256000 Kbaud. Der Standardwert ist 1000 Kbaud. Wenn nichts eingestellt (gelöscht), ist diese Funktion deaktiviert.
ingress-frames { ingress-frames }	**Zusammenfassung:** { broadcast, multicast, mcast-flood-ucast, all } **Standard:** broadcast Dieser Parameter spezifiziert die Art der Frames zur Begrenzung der Datenrate an diesem Port. Dies gilt nur für empfangene Frames: • BROADCAST : Es werden nur Broadcast-Frames begrenzt. • MULTICAST : Alle Multicast-Frames (einschließlich Broadcast) werden begrenzt. • MCAST-FLOOD-UCAST : Alle Multicast-Frames (einschließlich Broadcast) werden begrenzt. Unicast wird nicht begrenzt. • ALL : Alle Frames (Multicast wie Unicast) werden begrenzt.
egress-limit { egress-limit }	**Zusammenfassung:** { disabled } oder eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 62 und 256000 **Standard:** disabled Die maximale Datenrate in Kbaud, bei der der Switch Frames (Multicast, Broadcast und Unicast) an diesem Port überträgt. Der Switch wird Frames verwerfen, um bei Bedarf

Parameter	Beschreibung
	diese Rate zu erreichen. Der gültige Bereich entspricht 62 bis 256000 Kbaud. Wenn nichts eingestellt ist, ist diese Funktion deaktiviert.

5. Konfigurieren Sie mit dem/den folgenden Parameter(n) die LLDP-Einstellungen je nach Bedarf:

Parameter	Beschreibung
admin-status { admin-status }	**Zusammenfassung:** { tx-only, rx-only, rx-tx, no-lldp } **Standard:** rx-tx • no-lldp : Der lokale LLDP Agent kann weder LLDP-Frames übertragen noch empfangen. • rxTx : Der lokale LLDP Agent kann LLDP-Frames über den Port sowohl übertragen als auch empfangen. • txOnly : Der lokale LLDP Agent kann LLDP-Frames nur übertragen. • rxOnly : Der lokale LLDP Agent kann LLDP-Frames nur empfangen.
notify	Das Deaktivieren von Benachrichtigungen verhindert, dass vom LLDP Agent für eine bestimmte Schnittstelle Benachrichtigungen gesendet und Alarme erzeugt werden.

HINWEIS
Die Parameter Multicast Filtering, CoS und VLAN sind nur verfügbar, wenn sich der Port im Switchport-Modus befindet.

6. Konfigurieren Sie mit dem/den folgenden Parameter(n) die Einstellungen für "Multicast Filtering" je nach Bedarf:

Parameter	Beschreibung
gmrp { gmrp }	**Zusammenfassung:** { advertise_only, learn_advertise } GMRP (GARP Multicast Registration Protocol)-Betrieb am Port. Es gibt mehrere GMRP-Betriebsarten: • DISABLED : Der Port ist zu keiner GMRP-Verarbeitung fähig. • ADVERTISE ONLY : Der Port erkennt alle im Switch vorhandenen MCAST-Adressen (konfiguriert oder gelernt), lernt aber keine MCAST-Adressen. • ADVERTISE and LEARN : Der Port erkennt alle im Switch vorhandenen MCAST-Adressen (konfiguriert oder gelernt) und kann dynamisch MCAST-Adressen lernen.

7. Konfigurieren Sie mit dem/den folgenden Parameter(n) die CoS-Einstellungen je nach Bedarf:

Parameter	Beschreibung
default-priority { default-priority }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 0 und 7 **Standard:** 0 Die Priorität von Frames, die an diesem Port empfangen werden und nicht aufgrund des Frame-Inhalts priorisiert sind (z. B. Prioritätsfeld im VLAN-Tag, DiffServ-Feld im IP-Header, priorisierte MAC-Adresse).
inspect-tos	Aktiviert oder deaktiviert das Parsen des Feldes Type-of-Service (ToS) im IP-Header der empfangenen Frames, um festzulegen, welcher Berechtigungsklasse (CoS, en: Class of Service) sie zugewiesen werden sollen. Ist das ToS-Parsen aktiviert, verwendet der Switch die differenzierten Dienste-Bits im Feld TOS.

8. Konfigurieren Sie mit dem/den folgenden Parameter(n) die VLAN-Einstellungen je nach Bedarf:

Parameter	Beschreibung
pvid { pvid }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 1 und 4094 Die VLAN-Kennung des Ports gibt die VLAN-ID an, die nicht markierten (und als 802.1p Priorität markierten) Frames zugeordnet ist, die auf diesem Port empfangen werden.

Parameter	Beschreibung
	Frames, die mit einer VLAN-ID ungleich Null markiert sind, sind stets der VLAN-ID zugeordnet, die vom Frame-Tag abgerufen wurde.
type { type }	**Zusammenfassung:** { edge, trunk, pvlanedge } **Standard:** edge So bestimmt der Port seine Mitgliedschaft in VLANs. Es gibt verschiedene Port-Typen: • EDGE : Der Port ist nur Mitglied eines VLAN (sein natives, vom Parameter 'PVID' festgelegtes VLAN). • PVLAN Edge : Der Port leitet im selben VLAN keinen Verkehr an andere PVLAN Edge-Ports weiter. • TRUNK : Der Port ist automatisch Mitglied aller konfigurierten VLANs. Frames, die von einem Trunk-Port an alle VLANs, außer dem nativen VLAN des Ports, ausgesendet werden, sind immer getaggt. Er kann auch so konfiguriert sein, dass er GVRP für automatische VLAN-Konfiguration verwendet.
format { format }	**Zusammenfassung:** { untagged, tagged } **Standard:** untagged Zeigt an, ob Frames, die über den Port auf seinem nativen VLAN (angegeben durch den Parameter 'PVID') übertragen werden, getaggt oder nicht getaggt sind.
gvrp-mode { gvrp-mode }	**Zusammenfassung:** { advertise_only, learn_advertise } GVRP (Generic VLAN Registration Protocol)-Betrieb am Port. Es gibt mehrere GVRP-Betriebsarten: • DISABLED : Der Port ist zu keiner GVRP-Verarbeitung fähig. • ADVERTISE ONLY : Der Port erkennt alle im Switch vorhandenen VLANs (konfiguriert oder gelernt), lernt aber keine VLANs. • ADVERTISE and LEARN : Der Port erkennt alle im Switch vorhandenen VLANs (konfiguriert oder gelernt) und kann dynamisch VLANs lernen.

HINWEIS
*Sobald einem Switched-Ethernet-Port eine VLAN-ID zugeordnet wurde, wird ein VLAN angelegt und kann unter **switch » vlans » all-vlans** konfiguriert werden.*

9. Wenn sich der Port im Switchport-Modus befindet, konfigurieren Sie das VLAN für den Port. Weitere Informationen finden Sie unter Abschnitt 8.5.4.2, „VLANs für Switched-Ethernet-Ports konfigurieren“.
10. Konfigurieren Sie die Sicherheitseinstellungen des Ports. Weitere Informationen finden Sie unter Abschnitt 6.4.2, „Konfigurieren der Port-Sicherheit“.
11. Konfigurieren Sie die Einstellungen für den Spanning Tree. Weitere Informationen finden Sie unter Abschnitt 8.6.5, „Konfigurieren des STP für Switched-Ethernet-Ports und Ethernet-Trunk-Schnittstellen“.
12. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 8.1.3
Statistiken der Switched-Ethernet-Ports anzeigen

Um die Statistiken anzuzeigen, die für einen bestimmten Switched-Ethernet-Port erfasst werden, geben Sie Folgendes ein:

```
show interfaces switch swport port port-stats
```

Erläuterung:

- *port* ist die Nummer des Ports (oder eine Liste von Ports, wenn sie in einem Port-Trunk gebündelt sind) für das Modul.

Eine Tabelle oder Liste ähnlich dem folgenden Beispiel wird angezeigt:

```
ruggedcom# show interfaces switch swport 1 port-stats
port-stats
 in octets  6820
 out octets 3086
 in pkts    33
 out pkts   18
 error pkts 0
```

Diese Tabelle oder Liste liefert die folgenden Informationen:

Parameter	Beschreibung
in-octets	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl Oktette in guten Paketen, die empfangen werden. (Unicast+Multicast+Broadcast) und verworfene Pakete. Dieser Parameter ist obligatorisch.
out-octets	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl Oktette in guten Paketen, die übertragen werden. Dieser Parameter ist obligatorisch.
in-pkts	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl guter Pakete (Unicast+Multicast+Broadcast) und verworfener Pakete, die empfangen werden. Dieser Parameter ist obligatorisch.
out-pkts	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl guter Pakete, die übertragen werden. Dieser Parameter ist obligatorisch.
error-pkts	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl jeglicher Art von fehlerhaften Paketen. Dieser Parameter ist obligatorisch.

Abschnitt 8.1.4

Anzeigen der RMON-Portstatistik

Um die für einen bestimmten Switched-Ethernet-Port erhobene Remote-Network-Monitoring-(RMON)-Statistik anzuzeigen, geben Sie Folgendes ein:

```
show interfaces switch swport port rmon-stats
```

Erläuterung:

- *port* ist die Nummer des Ports (oder eine Liste von Ports, wenn sie in einem Port-Trunk gebündelt sind) für das Modul.

Eine Tabelle oder Liste ähnlich dem folgenden Beispiel wird angezeigt:

```
ruggedcom# show interfaces switch swport 1 rmon-stats | tab
rmon-stats
 in octets              10107903
 in pkts                53903
 in bcast pkts          607
```

```
in mcast pkts          42103
total in octets        10107903
total in pkts          53903
out octets             4974162
out pkts               14356
drop events            0
out bcast pkts         0
out mcast pkts         405
crc align errors       0
undersize pkts         0
oversize pkts          0
fragments              0
jabbers                0
collisions             0
late collisions        0
pkts 64 octets         10978
pkts 65to127 octets    24792
pkts 128to255 octets   19970
pkts 256to511 octets   2469
pkts 512to1023 octets  8410
pkts 1024to1518 octets 1640
```

Diese Tabelle oder Liste liefert die folgenden Informationen:

Parameter	Beschreibung
in-octets	**Zusammenfassung:** Eine vorzeichenlose 64-Bit-Ganzzahl Anzahl Oktette in guten Paketen (Unicast+Multicast+Broadcast) und verworfenen Paketen, die empfangen werden. Dieser Parameter ist obligatorisch.
in-pkts	**Zusammenfassung:** Eine vorzeichenlose 64-Bit-Ganzzahl Die Anzahl guter Pakete (Unicast+Multicast+Broadcast) und verworfener Pakete, die empfangen werden. Dieser Parameter ist obligatorisch.
in-bcast-pkts	**Zusammenfassung:** Eine vorzeichenlose 64-Bit-Ganzzahl Die Anzahl der guten empfangenen Broadcast-Pakete. Dieser Parameter ist obligatorisch.
in-mcast-pkts	**Zusammenfassung:** Eine vorzeichenlose 64-Bit-Ganzzahl Die Anzahl der guten empfangenen Multicast-Pakete. Dieser Parameter ist obligatorisch.
total-in-octets	**Zusammenfassung:** Eine vorzeichenlose 64-Bit-Ganzzahl Die Gesamtzahl Oktette aller empfangener Pakete. Dazu zählen Datenoktetts abgewiesener und lokaler Pakete, die nicht zur Übertragung an den Vermittlungskern weitergeleitet werden. Sie sollte alle auf der Leitung empfangenen Datenoktetts berücksichtigen. Dieser Parameter ist obligatorisch.
total-in-pkts	**Zusammenfassung:** Eine vorzeichenlose 64-Bit-Ganzzahl Die Anzahl der empfangenen Pakete. Dazu zählen abgewiesene, verworfene und lokale Pakete sowie Pakete, die nicht zur Übertragung an den Vermittlungskern weitergeleitet werden. Sie sollte alle auf der Leitung empfangenen Pakete berücksichtigen. Dieser Parameter ist obligatorisch.
out-octets	**Zusammenfassung:** Eine vorzeichenlose 64-Bit-Ganzzahl Die Anzahl Oktette in guten Paketen, die übertragen werden. Dieser Parameter ist obligatorisch.
out-pkts	**Zusammenfassung:** Eine vorzeichenlose 64-Bit-Ganzzahl Die Anzahl guter Pakete, die übertragen werden.

Parameter	Beschreibung
	Dieser Parameter ist obligatorisch.
drop-events	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl der empfangenen Pakete, die aufgrund fehlender Empfangspuffer verworfen werden. Dieser Parameter ist obligatorisch.
out-bcast-pkts	**Zusammenfassung:** Eine vorzeichenlose 64-Bit-Ganzzahl Die Anzahl der übertragenen Broadcast-Pakete. Dieser Parameter ist obligatorisch.
out-mcast-pkts	**Zusammenfassung:** Eine vorzeichenlose 64-Bit-Ganzzahl Die Anzahl der übertragenen Multicast-Pakete. Darin sind nicht Broadcast-Pakete eingeschlossen. Dieser Parameter ist obligatorisch.
crc-align-errors	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl der empfangenen Pakete, die sämtliche der folgenden Bedingungen erfüllen: 1. Die Paketdatenlänge beträgt zwischen 64 und 1536 Oktette einschließlich. 2. Die CRC des Pakets ist ungültig. 3. Es wurde kein Collision-Ereignis erkannt. 4. Es wurde kein Late Collision-Ereignis erkannt. Dieser Parameter ist obligatorisch.
undersize-pkts	**Zusammenfassung:** Eine vorzeichenlose 64-Bit-Ganzzahl Die Anzahl der empfangenen Pakete, die sämtliche der folgenden Bedingungen erfüllen: 1. Die Paketdatenlänge beträgt weniger als 64 Oktette. 2. Es wurde kein Collision-Ereignis erkannt. 3. Es wurde kein Late Collision-Ereignis erkannt. 4. Die CRC des Pakets ist gültig. Dieser Parameter ist obligatorisch.
oversize-pkts	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl der empfangenen Pakete mit einer Datenlänge von über 1536 Oktette und gültiger CRC. Dieser Parameter ist obligatorisch.
fragments	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl der empfangenen Pakete, die sämtliche der folgenden Bedingungen erfüllen: 1. Die Paketdatenlänge beträgt weniger als 64 Oktette oder es handelt sich um ein Paket ohne SFD, das weniger als 64 Oktette lang ist. 2. Es wurde kein Collision-Ereignis erkannt. 3. Es wurde kein Late Collision-Ereignis erkannt. 4. Die CRC des Pakets ist ungültig. Dieser Parameter ist obligatorisch.
jabbers	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl der Pakete, die sämtliche der folgenden Bedingungen erfüllen: 1. Die Paketdatenlänge beträgt mehr als 1536 Oktette. 2. Die CRC des Pakets ist ungültig. Dieser Parameter ist obligatorisch.
collisions	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl der empfangenen Pakete, bei denen ein Collision-Ereignis erkannt wurde. Dieser Parameter ist obligatorisch.
late-collisions	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl der empfangenen Pakete, bei denen ein Late Collision-Ereignis erkannt wurde. Dieser Parameter ist obligatorisch.
pkts-64-octets	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl empfangener und übertragener Pakete mit einer Größe von 64 Oktette. Dazu zählen empfangene und übertragene Pakete sowie verworfene und lokale empfangene Pakete. Darin sind nicht abgewiesene empfangene Pakete eingeschlossen.

Parameter	Beschreibung
	Dieser Parameter ist obligatorisch.
pkts-65to127-octets	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl empfangener und übertragener Pakete mit einer Größe von 65 bis 127 Oktette. Dazu zählen empfangene und übertragene Pakete sowie verworfene und lokale empfangene Pakete. Darin sind nicht abgewiesene empfangene Pakete eingeschlossen. Dieser Parameter ist obligatorisch.
pkts-128to255-octets	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl empfangener und übertragener Pakete mit einer Größe von 128 bis 257 Oktette. Dazu zählen empfangene und übertragene Pakete sowie verworfene und lokale empfangene Pakete. Darin sind nicht abgewiesene empfangene Pakete eingeschlossen. Dieser Parameter ist obligatorisch.
pkts-256to511-octets	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl empfangener und übertragener Pakete mit einer Größe von 256 bis 511 Oktette. Dazu zählen empfangene und übertragene Pakete sowie verworfene und lokale empfangene Pakete. Darin sind nicht abgewiesene empfangene Pakete eingeschlossen. Dieser Parameter ist obligatorisch.
pkts-512to1023-octets	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl empfangener und übertragener Pakete mit einer Größe von 512 bis 1023 Oktette. Dazu zählen empfangene und übertragene Pakete sowie verworfene und lokale empfangene Pakete. Darin sind nicht abgewiesene empfangene Pakete eingeschlossen. Dieser Parameter ist obligatorisch.
pkts-1024to1518-octets	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl empfangener und übertragener Pakete mit einer Größe von 1024 bis 1536 Oktette. Dazu zählen empfangene und übertragene Pakete sowie verworfene und lokale empfangene Pakete. Darin sind nicht abgewiesene empfangene Pakete eingeschlossen. Dieser Parameter ist obligatorisch.

Abschnitt 8.1.5

Switched-Ethernet-Port-Statistiken löschen

Um die Statistiken für einen bestimmten Switched-Ethernet-Port zu löschen, geben Sie Folgendes ein:

```
interfaces switch swport port clear-port-stats
```

Erläuterung:

- *port* ist die Nummer des Ports (oder eine Liste von Ports, wenn sie in einem Port-Trunk gebündelt sind) für das Modul

Abschnitt 8.1.6

Einen Switched-Ethernet-Port zurücksetzen

Um einen Switched-Ethernet-Port zurückzusetzen, geben Sie Folgendes ein:

```
interfaces switch swport port reset-port
```

Erläuterung:

- *port* ist die Nummer des Ports (oder eine Liste von Ports, wenn sie in einem Port-Trunk gebündelt sind) für das Modul

Abschnitt 8.1.7

Kabel für Switched-Ethernet-Ports testen

Kabel für Switched-Ethernet-Ports können durch Diagnosen auf ihre Qualität überprüft werden.

INHALT

- Abschnitt 8.1.7.1, „Ausführen eines Kabeldiagnosetests“
- Abschnitt 8.1.7.2, „Anzeigen der Kabeldiagnosestatistik“
- Abschnitt 8.1.7.3, „Löschen der Kabeldiagnosestatistik“

Abschnitt 8.1.7.1

Ausführen eines Kabeldiagnosetests

Um einen Kabeldiagnosetest an einem bestimmten Port auszuführen, geben Sie Folgendes ein:

WICHTIG!
Wenn die Kabeldiagnose an einem Port ausgeführt wird, werden hergestellte Netzwerkverbindungen am Port verworfen und der normale Netzwerkverkehr kann weder den getesteten Port (PUT) noch den Partnerport passieren. Wenn der Kabeldiagnosetest abgeschlossen ist, werden die ursprünglichen Netzwerkporteinstellungen sowohl für den PUT- als auch den Partner-Port zusammen mit hergestellten Verbindungen wiederhergestellt.

```
interfaces switch swport port diagnostics start-cable-test run runs calibration calibration
```

Erläuterung:

- *port* ist die Nummer des Ports (oder eine Liste von Ports, wenn sie in einem Port-Trunk gebündelt sind) für das Modul.
- *runs* ist die Gesamtanzahl, wie oft die Kabeldiagnose am ausgewählten Port ausgeführt werden soll. Wenn auf "0" gesetzt, wird die Kabeldiagnose kontinuierlich am ausgewählten Port ausgeführt.
- *calibration* ist der Wert, der zum Anpassen oder Kalibrieren der geschätzten Entfernung zum Fehler herangezogen wird. Um die geschätzte Entfernung zum Fehler zu kalibrieren, gehen Sie wie folgt vor:
  1. Schließen Sie ein Ethernet-Kabel mit einer bekannten Länge (z. B. 50 m) an den zu kalibrierenden Port an. Verbinden Sie das andere Ende des Kabels nicht mit einem Verbindungspartner.
  2. Führen Sie den Kabeldiagnosetest mehrmals am Port aus. Ein "OPEN"-Fehler sollte erkannt werden.
  3. Ermitteln Sie die mittlere Entfernung zum im Protokoll erfassten "OPEN"-Fehler und vergleichen Sie diese mit der bekannten Länge des Kabels. Die Differenz kann als Kalibrierungswert herangezogen werden.
  4. Geben Sie den Kalibrierungswert ein und führen Sie den Kabeldiagnosetest erneut mehrmals aus. Die Entfernung zum "OPEN"-Fehler sollte nun der Kabellänge entsprechen. Verwenden Sie den Entfernungswert zum Ermitteln des Kalibrierungswerts.

Informationen über das Anzeigen von Testergebnissen finden Sie unter Abschnitt 8.1.7.2, „Anzeigen der Kabeldiagnosestatistik“.

Abschnitt 8.1.7.2
Anzeigen der Kabeldiagnosestatistik

Um die für einen Switched-Ethernet-Port nach einem Kabeldiagnosetest erhobene Statistik anzuzeigen, geben Sie Folgendes ein:

```
show interfaces switch swport port diagnostics cable-diagnostic-results
```

- *port* ist die Nummer des Ports (oder eine Liste von Ports, wenn sie in einem Port-Trunk gebündelt sind) für das Modul.

Eine Liste ähnlich dem folgenden Beispiel wird angezeigt:

```
ruggedcom# show interfaces switch swport 1 diagnostics cable-diagnostic-results
diagnostics cable-diagnostic-results
 running         false
 good            20
 open            0
 short           20
 imped           0
 pass fail total "   10/    0/   10  "
 run count       0
 pass count      0
 fail count      0
```

Diese Liste liefert die folgenden Informationen:

Parameter	Beschreibung
running	**Zusammenfassung:** { true, false } Zeigt an, ob gerade eine Kabelprüfung an diesem Port durchgeführt wird. Dieser Parameter ist obligatorisch.
good	**Zusammenfassung:** Eine vorzeichenlose 16-Bit-Ganzzahl Die Anzahl der Ergebnisse mit GOOD TERMINATION (kein Fehler) an den Kabelpaaren des ausgewählten Ports. Dieser Parameter ist obligatorisch.
open	**Zusammenfassung:** Eine vorzeichenlose 16-Bit-Ganzzahl Die Anzahl der Ergebnisse mit OPEN an den Kabelpaaren des ausgewählten Ports. Dieser Parameter ist obligatorisch.
short	**Zusammenfassung:** Eine vorzeichenlose 16-Bit-Ganzzahl Die Anzahl der Ergebnisse mit SHORT an den Kabelpaaren des ausgewählten Ports. Dieser Parameter ist obligatorisch.
imped	**Zusammenfassung:** Eine vorzeichenlose 16-Bit-Ganzzahl Die Anzahl der Ergebnisse mit IMPEDANCE MISMATCH an den Kabelpaaren des ausgewählten Ports. Dieser Parameter ist obligatorisch.
pass-fail-total	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 19 Zeichen Dieses Feld fasst die Ergebnisse der bisher durchgeführten Kabeldiagnose zusammen. • Pass : die Anzahl der erfolgreichen Kabeldiagnosen an dem ausgewählten Port. • Fail : die Anzahl der fehlgeschlagenen Kabeldiagnosen an dem ausgewählten Port. • Total : die Gesamtanzahl der Versuche einer Kabeldiagnose an dem ausgewählten Port. Dieser Parameter ist obligatorisch.
run-count	**Zusammenfassung:** Eine vorzeichenlose 16-Bit-Ganzzahl Run Count : Die Gesamtzahl der Durchläufe

Parameter	Beschreibung
	Dieser Parameter ist obligatorisch.
pass-count	**Zusammenfassung:** Eine vorzeichenlose 16-Bit-Ganzzahl Pass Count Dieser Parameter ist obligatorisch.
fail-count	**Zusammenfassung:** Eine vorzeichenlose 16-Bit-Ganzzahl Failure Count Dieser Parameter ist obligatorisch.

Abschnitt 8.1.7.3
Löschen der Kabeldiagnosestatistik

Im Folgenden wird beschrieben, wie die bei Kabeldiagnosetests erhobene Statistik gelöscht wird. Sie können alle Statistiken oder nur die Statistiken für einen bestimmten Switchport löschen.

» Löschen aller Kabeldiagnosestatistiken

Um die Statistiken zu löschen, geben Sie Folgendes ein:

```
switch clear-cable-stats-all
```

» Löschen der Kabeldiagnosestatistik für einen bestimmten Switchport

Um nur die Statistiken für einen bestimmten Switchport zu löschen, geben Sie Folgendes ein:

Erläuterung:

- *port* ist die Nummer des Ports (oder eine Liste von Ports, wenn sie in einem Port-Trunk gebündelt sind) für das Modul.

Abschnitt 8.2
Ethernet-Trunk-Schnittstellen verwalten

Dieser Abschnitt beschreibt, wie Sie Ethernet-Trunk-Schnittstellen konfigurieren und verwalten können.

INHALT

- Abschnitt 8.2.1, „Eine Liste der Ethernet-Trunk-Schnittstellen anzeigen“
- Abschnitt 8.2.2, „Hinzufügen einer Ethernet-Trunk-Schnittstelle“
- Abschnitt 8.2.3, „Eine Ethernet-Trunk-Schnittstelle löschen“
- Abschnitt 8.2.4, „Ethernet-Trunk-Ports verwalten“

Abschnitt 8.2.1
Eine Liste der Ethernet-Trunk-Schnittstellen anzeigen

Um eine Liste der Ethernet-Trunk-Ports anzuzeigen, geben Sie Folgendes ein:

```
show running-config interface trunk
```

Falls Trunks konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config interface trunks
interface
 trunks 1
  switchport
  no alias
  no mcast-filtering gmrp
  no cos inspect-tos
  vlan pvid 1
  no vlan gvrp-mode
  trunk-ports swport 1
  !
  trunk-ports swport 2
  !
  no spanning-tree restricted-role
  no spanning-tree restricted-tcn
 !
!
```

Falls keine Ethernet-Trunk-Schnittstellen konfiguriert wurden, fügen Sie je nach Bedarf Trunks hinzu. Weitere Informationen finden Sie unter Abschnitt 8.2.2, „Hinzufügen einer Ethernet-Trunk-Schnittstelle“.

Abschnitt 8.2.2
Hinzufügen einer Ethernet-Trunk-Schnittstelle

Um eine Ethernet-Trunk-Schnittstelle hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie die Schnittstelle hinzu, indem Sie Folgendes eingeben:

   ```
   interface trunks id
   ```

   Erläuterung:

   - *id* ist die ID für den Trunk
3. Konfigurieren Sie die Schnittstelle, indem Sie Folgendes eingeben:

Parameter	Beschreibung
switchport	**Zusammenfassung:** { true, false } Physischer Port entweder im Switched-Modus oder in einem bestimmten Routing-Modus.
on-demand	Diese Schnittstelle wird nur on-Demand angesprochen
ip-address-src { ip-address-src }	**Zusammenfassung:** { static, dynamic } Zeigt an, ob die IP-Adresse statisch oder dynamisch über DHCP oder BOOTP zugewiesen ist. Die Option DYNAMIC wird gewöhnlich für eine dynamisch zugewiesene IP-Adresse eingesetzt. Sie schaltet zwischen BOOTP und DHCP, bis sie die Antwort vom entsprechenden Server erhält. Bei nicht verwalteten Schnittstellen muss dies statisch sein.
ipv6-address-src { ipv6-address-src }	**Zusammenfassung:** { static, dynamic }

Parameter	Beschreibung
	Standard: static Zeigt an, ob die IP-Adresse statisch oder dynamisch über DHCP zugewiesen ist. Die Option DYNAMIC wird gewöhnlich für eine dynamisch zugewiesene IP-Adresse eingesetzt. Bei nicht verwalteten Schnittstellen muss dies statisch sein.
proxyarp	Aktiviert/deaktiviert, dass das VLAN auf ARP-Anfragen für andere Hosts als sich selbst antwortet
mtu { mtu }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 68 und 9216 **Standard:** 1500 Maximale Übertragungseinheit (größte zulässige Paketgröße für diese Schnittstelle).
alias { alias }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 64 Zeichen Der SNMP-Aliasname der Schnittstelle.

4. Konfigurieren Sie die Multicast-Filtering-Einstellungen, indem Sie die folgenden Befehle eingeben:

Parameter	Beschreibung
gmrp { gmrp }	**Zusammenfassung:** { advertise_only, learn_advertise } GMRP (GARP Multicast Registration Protocol)-Betrieb am Port. Es gibt mehrere GMRP-Betriebsarten: • DISABLED : Der Port ist zu keiner GMRP-Verarbeitung fähig. • ADVERTISE ONLY : Der Port erkennt alle im Switch vorhandenen MCAST-Adressen (konfiguriert oder gelernt), lernt aber keine MCAST-Adressen. • ADVERTISE and LEARN : Der Port erkennt alle im Switch vorhandenen MCAST-Adressen (konfiguriert oder gelernt) und kann dynamisch MCAST-Adressen lernen.

5. Konfigurieren Sie die CoS-Einstellungen, indem Sie die folgenden Befehle eingeben:

Parameter	Beschreibung
default-priority { default-priority }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 0 und 7 **Standard:** 0 Die Priorität von Frames, die an diesem Port empfangen werden und nicht aufgrund des Frame-Inhalts priorisiert sind (z. B. Prioritätsfeld im VLAN-Tag, DiffServ-Feld im IP-Header, priorisierte MAC-Adresse).
inspect-tos	Aktiviert oder deaktiviert das Parsen des Feldes Type-of-Service (ToS) im IP-Header der empfangenen Frames, um festzulegen, welcher Berechtigungsklasse sie zugewiesen werden sollen. Ist das ToS-Parsen aktiviert, verwendet der Switch die differenzierten Dienste-Bits im Feld TOS.

6. Konfigurieren Sie die VLAN-Einstellungen, indem Sie die folgenden Befehle eingeben:

Parameter	Beschreibung
pvid { pvid }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 1 und 4094 Die VLAN-Kennung des Ports gibt die VLAN-ID an, die nicht markierten (und als 802.1p Priorität markierten) Frames zugeordnet ist, die auf diesem Port empfangen werden. Frames, die mit einer VLAN-ID ungleich Null markiert sind, sind stets der VLAN-ID zugeordnet, die vom Frame-Tag abgerufen wurde.
type { type }	**Zusammenfassung:** { edge, trunk, pvlanedge } **Standard:** edge So bestimmt der Port seine Mitgliedschaft in VLANs. Es gibt die folgenden Port-Typen: • EDGE : Der Port ist nur Mitglied eines VLAN (sein natives, vom Parameter 'PVID' festgelegtes VLAN). • PVLAN Edge : Der Port leitet im selben VLAN keinen Verkehr an andere PVLAN Edge-Ports weiter.

Parameter	Beschreibung
	• TRUNK : Der Port ist automatisch Mitglied aller konfigurierten VLANs. Frames, die von einem Trunk-Port an alle VLANs, außer dem nativen VLAN des Ports, ausgesendet werden, sind immer getaggt. Er kann auch so konfiguriert sein, dass er GVRP für automatische VLAN-Konfiguration verwendet.
format { format }	**Zusammenfassung:** { untagged, tagged } **Standard:** untagged Zeigt an, ob Frames, die über den Port auf seinem nativen VLAN (angegeben durch den Parameter 'PVID') übertragen werden, getaggt oder nicht getaggt sind.
gvrp-mode { gvrp-mode }	**Zusammenfassung:** { advertise_only, learn_advertise } GVRP (Generic VLAN Registration Protocol)-Betrieb am Port. Es gibt mehrere GVRP-Betriebsarten: • DISABLED : Der Port ist zu keiner GVRP-Verarbeitung fähig. • ADVERTISE ONLY : Der Port erkennt alle im Switch vorhandenen VLANs (konfiguriert oder gelernt), lernt aber keine VLANs. • ADVERTISE and LEARN : Der Port erkennt alle im Switch vorhandenen VLANs (konfiguriert oder gelernt) und kann dynamisch VLANs lernen.

7. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 8.2.3
Eine Ethernet-Trunk-Schnittstelle löschen

Um eine Ethernet-Trunk-Schnittstelle zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die Schnittstelle durch Eingabe von:

```
no interface trunks id
```

Erläuterung:

- *`id`* ist die ID des Trunks

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 8.2.4
Ethernet-Trunk-Ports verwalten

Dieser Abschnitt beschreibt, wie Sie Ethernet-Trunk-Portzuordnungen verwalten können.

INHALT

- Abschnitt 8.2.4.1, „Eine Liste der Ethernet-Trunk-Ports anzeigen“
- Abschnitt 8.2.4.2, „Einen Ethernet-Trunk-Port hinzufügen“
- Abschnitt 8.2.4.3, „Einen Ethernet-Trunk-Port löschen“

Abschnitt 8.2.4.1
Eine Liste der Ethernet-Trunk-Ports anzeigen

Um eine Liste der Ethernet-Trunk-Ports anzuzeigen, geben Sie Folgendes ein:

```
show running-config interface trunks id trunk-ports
```

Erläuterung:

- *id* ist die ID für die Schnittstelle

Falls Trunk-Ports konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config interface trunks 1 trunk-ports
interface
 trunks 1
  trunk-ports swport 1
  !
  trunk-ports swport 2
  !
 !
!
```

Falls keine Ethernet-Trunk-Ports konfiguriert wurden, fügen Sie je nach Bedarf Ports hinzu. Weitere Informationen finden Sie unter Abschnitt 8.2.4.2, „Einen Ethernet-Trunk-Port hinzufügen“.

Abschnitt 8.2.4.2
Einen Ethernet-Trunk-Port hinzufügen

Um einen Ethernet-Trunk-Port hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den Port hinzu, indem Sie Folgendes eingeben:

   ```
   interface trunks id trunk-ports swport port
   ```

   Erläuterung:

   - *id* ist die ID für den Trunk
   - *port* ist die Nummer des Ports (oder eine Liste von Ports, wenn sie in einem Port-Trunk gebündelt sind) für das Modul.
3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 8.2.4.3
Einen Ethernet-Trunk-Port löschen

Um einen Ethernet-Trunk-Port zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den Port, indem Sie Folgendes eingeben:

   ```
   no interface trunks id trunk-ports swport port
   ```

   Erläuterung:

   - *id* ist die ID für den Trunk

- *port* ist die Nummer des Ports (oder eine Liste von Ports, wenn sie in einem Port-Trunk gebündelt sind) für das Modul.

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 8.3
MAC-Adressen verwalten

Im Rahmen der Layer-2-Funktionalität pflegt RUGGEDCOM ROX II eine MAC-(Media Access Control)-Adressentabelle; dies ist eine Liste einmaliger MAC-Adressen für Netzwerkschnittstellen, die mit dem Gerät auf der Sicherungsschicht kommunizieren können. Die MAC-Adressentabelle kann manuell durch Eingabe spezifischer MAC-Adressen und/oder dynamisch aufgefüllt werden. Wird sie dynamisch aufgefüllt, fügt RUGGEDCOM ROX II automatisch die MAC-Adressen der Netzwerkschnittstellen hinzu, die es im Netzwerk erkennt. Diese Adressen werden entfernt, wenn sie ungültig werden oder eine Störung der Datenverbindung eintritt.

INHALT

- Abschnitt 8.3.1, „Anzeigen der dynamischen Liste der MAC-Adressen“
- Abschnitt 8.3.2, „Die dynamische MAC-Adressliste leeren“
- Abschnitt 8.3.3, „Optionen für das MAC-Adressenlernen konfigurieren“
- Abschnitt 8.3.4, „Statische MAC-Adressen verwalten“

Abschnitt 8.3.1
Anzeigen der dynamischen Liste der MAC-Adressen

Um eine dynamische Liste der gelernten und statisch konfigurierten MAC-Adressen anzuzeigen, geben Sie Folgendes ein:

```
show switch mac-tables mac-table
```

Eine Tabelle oder Liste ähnlich dem folgenden Beispiel wird angezeigt:

```
ruggedcom# show switch mac-tables mac-table
MAC               VID  SLOT    PORT  TYPE     COS
-----------------------------------------------------
00:01:c0:0b:b6:58  4    swport  4     dynamic  N/A
00:04:5f:fb:62:36  4    swport  4     dynamic  N/A
00:04:5f:fb:63:8e  4    swport  4     dynamic  N/A
00:06:b5:64:92:75  4    swport  4     dynamic  N/A
00:0a:dc:02:4f:c0  4    swport  4     dynamic  N/A
00:0a:dc:2d:a6:e3  4    swport  4     dynamic  N/A
00:0a:dc:e5:86:ff  4    swport  4     dynamic  N/A
00:0a:dc:e5:a4:ff  4    swport  4     dynamic  N/A
```

Diese Tabelleoder Liste liefert die folgenden Informationen:

Parameter	Beschreibung
mac	**Zusammenfassung:** Eine Zeichenkette mit 17 Zeichen Die vom Switch gelernte MAC-Adresse.
vid	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl

Parameter	Beschreibung
	Die VLAN-Kennung für das VLAN, über das die statische MAC-Adresse arbeitet. Dieser Parameter ist obligatorisch.
slot	**Zusammenfassung:** { sm, lm1, lm2, lm3, lm4, lm5, lm6, swport, eth, serport, celport, wlanport } Der Steckplatz, der Modul mit Port enthält. Dieser Parameter ist obligatorisch.
port	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 1 und 16 Der Port, an dem die MAC-Adresse gelernt wurde. Dieser Parameter ist obligatorisch.
type	**Zusammenfassung:** { static, dynamic } Legt fest, wie die MAC-Adresse vom Switch gelernt wurde: • STATIC: Die Adresse wurde anhand der Konfiguration in der Tabelle der statischen MAC-Adressen oder durch einen anderen Verwaltungsvorgang erlernt und kann nicht automatisch vom Switch abgelernt oder umgelernt werden. • DYNAMIC: Die Adresse wurde automatisch vom Switch gelernt und kann automatisch umgelernt werden. Dieser Parameter ist obligatorisch.
cos	**Zusammenfassung:** { N/A, normal, medium, high, crit } Die Berechtigungsklasse (CoS, Class of Service), die Frames zugeordnet ist, die die Adresse als Quell- oder Zieladresse führen. Dieser Parameter ist obligatorisch.

Wenn keine MAC-Adresse aufgeführt ist, gehen Sie wie folgt vor:

- Konfigurieren Sie die MAC-Adressenlernoptionen für die dynamische Erkennung der MAC-Adressen anderer Geräte im Netzwerk. Weitere Informationen finden Sie unter Abschnitt 8.3.3, „Optionen für das MAC-Adressenlernen konfigurieren“.
- Konfigurieren Sie die Adresse auf dem Gerät als statische MAC-Adresse. Weitere Informationen finden Sie unter Abschnitt 8.3.4.2, „Hinzufügen einer statischen MAC-Adresse“.

Abschnitt 8.3.2

Die dynamische MAC-Adressliste leeren

Um alle Einträge in der dynamischen MAC-Adressliste zu löschen, geben Sie Folgendes ein:

```
switch mac-tables purge-mac-table
```

Sobald die Tabelle leer ist, wird die folgende Meldung angezeigt:

```
purge-mac-table-string Success
```

Abschnitt 8.3.3

Optionen für das MAC-Adressenlernen konfigurieren

Die Optionen für das MAC-Adressenlernen steuern, wie und wann MAC-Adressen automatisch aus der Tabelle der MAC-Adressen gelöscht werden. Einzeladressen werden gelöscht, sobald der Alterungs-Timer überschritten ist. Adressen können zudem gelöscht werden, wenn ein Link ausfällt oder sich eine Topologie ändert.

Um die Optionen für das MAC-Adressenlernen zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***switch » mac-tables*** und konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
mac-aging-time { mac-aging-time }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 15 und 800 **Standard:** 300 Die Dauer, für die eine gelernte MAC-Adresse gehalten wird, bevor sie veraltet.
mac-age-on-loss	**Zusammenfassung:** { true, false } **Standard:** true Wenn ein Link-Ausfall (und möglicherweise eine Topologieänderung) auftritt, kann der Switch einige MAC-Adressen haben, die zuvor am ausgefallenen Port gelernt wurden. Solange diese Adressen nicht veraltet sind, leitet der Switch den Verkehr an diesen Port weiter und verhindert so, dass dieser Verkehr sein Ziel über die neue Netzwerktopologie erreicht. Mit diesem Parameter können alle MAC-Adressen, die an einem ausgefallenen Port gelernt wurden, sofort nach dem Erkennen eines Verbindungsfehlers veralten.

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 8.3.4
Statische MAC-Adressen verwalten

Statische MAC-Adressen müssen konfiguriert werden, wenn die Zielgeräte nur Frames empfangen, aber nicht senden können. Sie müssen manchmal auch konfiguriert werden, wenn die Port-Sicherheit (sofern unterstützt) verstärkt werden muss.

Priorisierte MAC-Adressen werden konfiguriert, wenn der Verkehr zu oder von einem bestimmten Gerät in einem LAN-Segment eine höhere CoS-Priorität als andere Geräte auf diesem Segment erhalten soll.

INHALT

- Abschnitt 8.3.4.1, „Eine Liste der statischen MAC-Adressen anzeigen“
- Abschnitt 8.3.4.2, „Hinzufügen einer statischen MAC-Adresse“
- Abschnitt 8.3.4.3, „Eine statische MAC-Adresse löschen“

Abschnitt 8.3.4.1
Eine Liste der statischen MAC-Adressen anzeigen

Um eine Liste der statischen MAC-Adressen, die auf einem Gerät konfiguriert sind, anzuzeigen, geben Sie Folgendes ein:

```
show running-config switch mac-tables static-mac-table
```

Falls statische MAC-Adressen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config switch mac-tables static-mac-table | tab MAC VID LEARNED SLOT PORT COS
 ------------------------------------------------------ 00:0a:dc:f6:8b:ff 4085 - swport 2 normal
 00:10:94:00:24:01 4084 - swport 1 normal 00:10:94:00:30:01 1 - swport 2 normal 00:10:94:00:40:01 4086
 - swport 2 normal !
```

Falls keine statischen MAC-Adressen konfiguriert wurden, fügen Sie je nach Bedarf Adressen hinzu. Weitere Informationen finden Sie unter Abschnitt 8.3.4.2, „Hinzufügen einer statischen MAC-Adresse“.

Abschnitt 8.3.4.2
Hinzufügen einer statischen MAC-Adresse

Um eine statische MAC-Adresse hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie die statische MAC-Adresse hinzu, indem Sie Folgendes eingeben:

   HINWEIS
   Die Buchstaben in MAC-Adressen müssen Kleinbuchstaben sein.

   ```
   switch mac-tables static-mac-table static-mac address vlan
   ```

   Erläuterung:

   - *address* ist die Unicast-MAC-Adresse, die statisch konfiguriert werden soll. Es können bis zu 6 Platzhalterzeichen '*' von rechts fortlaufend verwendet werden.
   - *vlan* ist die ID für das VLAN, über das die MAC-Adresse arbeitet.
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
learned	Ist sie eingestellt, lernt das System eigenständig den Port, auf dem sich das Gerät mit dieser Adresse befindet.
slot { slot }	**Zusammenfassung:** Eine Zeichenkette Die Bezeichnung des Modul-Einbauorts gemäß Siebdruck auf der Geräteoberseite.
port { port }	**Zusammenfassung:** Eine Zeichenkette Die ausgewählten Ports am Modul, die am angegebenen Steckplatz installiert sind.
cos { cos }	**Zusammenfassung:** { N/A, normal, medium, high, crit } **Standard:** normal Die Priorität des Verkehrs für eine bestimmte Adresse.

4. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 8.3.4.3
Eine statische MAC-Adresse löschen

Um eine statische MAC-Adresse zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die statische MAC-Adresse, indem Sie Folgendes eingeben:

   ```
   no switch mac-tables static-mac-table static-mac address vlan
   ```

   Erläuterung:

- *address* ist die Unicast-MAC-Adresse, die statisch konfiguriert werden soll. Es können bis zu 6 '*' Platzhalterzeichen von rechts fortlaufend verwendet werden.
- *vlan* ist die ID für das VLAN, über das die MAC-Adresse arbeitet

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 8.4
Multicast-Filterung verwalten

Multicast-Verkehr kann entweder mit statischen Multicast-Gruppen, IGMP (Internet Group Management Protocol) Snooping oder GMRP (GARP Multicast Registration Protocol) gefiltert werden.

INHALT

- Abschnitt 8.4.1, „Multicast-Filterkonzepte“
- Abschnitt 8.4.2, „GMRP aktivieren und konfigurieren“
- Abschnitt 8.4.3, „IGMP Snooping verwalten“
- Abschnitt 8.4.4, „Die statische Multicast-Gruppen-Tabelle verwalten“
- Abschnitt 8.4.5, „Ausgehende (egress) Ports für Multicast-Gruppen verwalten“
- Abschnitt 8.4.6, „Ein Übersicht der Multicast-Gruppen anzeigen“
- Abschnitt 8.4.7, „Eine Liste der IP-Multicast-Gruppen anzeigen“

Abschnitt 8.4.1
Multicast-Filterkonzepte

Dieser Abschnitt beschreibt einige wesentliche Konzepte für die Implementierung der Multicast-Filterung in RUGGEDCOM ROX II.

INHALT

- Abschnitt 8.4.1.1, „IGMP“
- Abschnitt 8.4.1.2, „GMRP (GARP Multicast Registration Protocol)“

Abschnitt 8.4.1.1
IGMP

IGMP wird von IP-Hosts verwendet, um Multicast-Routern ihre Gruppenmitgliedschaften zu melden. So wie die Hosts bestimmten Multicast-Gruppen beitreten und sie wieder verlassen, werden die Datenverkehrsströme an die Hosts weitergeleitet oder von ihnen ferngehalten.

Das IGMP-Protokoll agiert zwischen Multicast-Routern und IP-Hosts. Wenn ein Unmanaged Switch zwischen Multicast-Routern und ihren Hosts angeordnet wird, werden die Multicast-Streams an alle Ports verteilt. Dies kann an einigen Ports für erheblichen Datenverkehr sorgen, den diese Ports nicht benötigen und daraus keinen Nutzen ziehen.

IGMP-Snooping wirkt sich, sofern aktiviert, auf vom Router und vom Host gesendete IGMP-Nachrichten aus und beschränkt die Traffic-Streams auf die entsprechenden LAN-Segmente.

Beispiel: IGMP im Betrieb

Die folgenden Netzwerkpläne zeigen ein einfaches Beispiel für den Einsatz von IGMP.

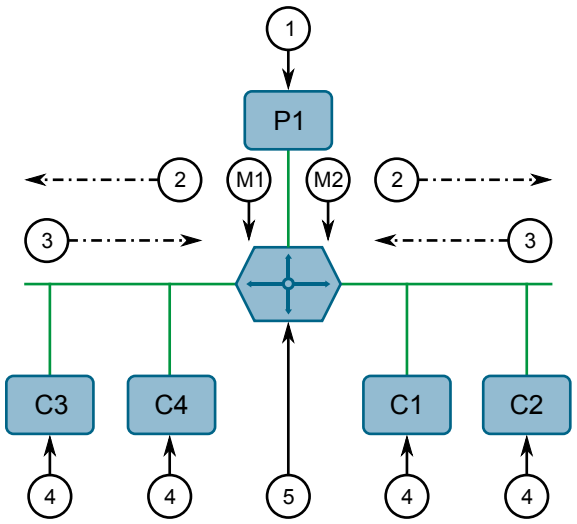


Abbildung 5: Beispiel – IGMP im Betrieb

1. Producer **2.** Mitgliedschaftsabfragen **3.** Mitgliedschaftsberichte **4.** Host **5.** Multicast-Router

Ein IP-Host als *Producer* (P1) generiert zwei IP-Multicast-Streams, M1 und M2. Für diese Streams gibt es vier mögliche *Consumer*, C1 bis C4. Der Multicast-Router erkennt, welcher Host welchen Stream abonnieren möchte, indem er jedem Segment Mitgliedschaftsabfragen sendet.

In diesem Beispiel wird die an das Segment C1-C2 gesendete allgemeine Mitgliedschaftsabfrage von einem Mitgliedschaftsbericht (bzw. *join*) beantwortet, womit der Wunsch übermittelt wird, den Stream M2 zu abonnieren. Der Router leitet den Stream M2 an das Segment C1-C2 weiter. Auf ähnliche Weise erkennt der Router, dass er Stream M1 an das Segment C3-C4 weiterleiten muss.

Ein *Consumer* kann einer beliebigen Anzahl Multicast-Gruppen beitreten und für jede Gruppe einen Mitgliedschaftsbericht ausgeben. Wenn ein Host einen Mitgliedschaftsbericht ausgibt, unterdrücken andere Hosts im selben Netzwerksegment, die ebenfalls die Mitgliedschaft für die gleiche Gruppe benötigen, ihre eigenen Anfragen, weil diese redundant wären. Auf diese Weise garantiert das IGMP-Protokoll, dass das Segment für jede Gruppe nur einen Mitgliedschaftsbericht ausgibt.

Der Router fragt regelmäßig jedes seiner Segmente ab, um zu ermitteln, ob mindestens noch ein Consumer einen bestimmten Stream abonniert. Wenn er innerhalb eines vorgegebenen Zeitraums (üblicherweise zwei Abfrageintervalle) keine Antworten empfängt, schneidet der Router den Multicast-Stream vom jeweiligen Segment zurück.

Eine häufiger vorkommende Pruning-Methode tritt auf, wenn Consumer ihr Abonnement aufheben möchten und eine IGMP-Nachricht *leave group* absetzen. Der Router gibt sofort eine gruppenspezifische Mitgliedschaftsabfrage aus, um zu ermitteln, ob in dem Segment noch Abonnenten der Gruppe übrig sind. Nachdem sich der letzte Consumer einer Gruppe abgemeldet hat, schneidet der Router den Multicast-Stream vom jeweiligen Segment zurück.

IGMP-Betrieb in Switches

Die IGMP-Snooping-Funktion bietet den Switches eines Möglichkeit zum Snooping (d.h. zum Beobachten) des Betriebs von Routern, zum Antworten mit join/leave-Nachrichten im Namen von Consumer-Ports und zum entsprechenden Pruning von Multicast-Streams. Für den Switch lassen sich zwei IGMP-Modi konfigurieren: aktiv und passiv.

- **Aktiver Modus**
  IGMP unterstützt eine Betriebsart *ohne Router*.

  Wenn ein solcher Switch ohne Multicast-Router verwendet wird, kann er so funktionieren, als ob er ein Multicast-Router wäre, der allgemeine IGMP-Abfragen sendet.
- **Passiver Modus**
  Wenn ein solcher Switch in einem Netzwerk mit einem Multicast-Router verwendet wird, kann er für die Ausführung des passiven IGMP konfiguriert werden. In dieser Betriebsart wird verhindert, dass der Switch die Abfragen sendet, die den Router verwirren können, sodass er keine IGMP-Abfragen mehr ausgibt.

HINWEIS
Ein Switch im passiven Modus erfordert das Vorhandensein eines Multicast-Routers, ansonsten kann er überhaupt keine Multicast-Streams mehr weiterleiten, wenn keine Multicast-Router vorhanden sind.

HINWEIS
Ohne einen Multicast-Router muss sich mindestens ein IGMP-Snooping-Switch im aktiven Modus befinden, damit IGMP funktionsfähig ist.

Regeln beim IGMP-Snooping

Beim IGMP-Snooping gelten die folgenden Regeln:

- Wenn eine Multicast-Quelle mit dem Multicasting beginnt, wird der Traffic-Stream an Segmenten, von deinen keine join-Nachrichten empfangen wurden, sofort gesperrt.
- Sofern nicht anders konfiguriert, leitet der Switch sämtlichen Multicast-Verkehr an die Ports weiter, an denen Multicast-Router angeschlossen sind.
- Pakete mit einer Ziel-IP-Multicast-Adresse im Bereich 224.0.0.X, bei denen es sich nicht um IGMP handelt, werden stets an alle Ports weitergeleitet. Dieses Verhalten basiert auf der Tatsache, dass viele Systeme für IP-Multicast-Adressen in diesem Bereich keine Mitgliedschaftsberichte senden, solange sie noch auf solche Pakete hören.
- Der Switch implementiert *proxy-reporting* (d.h. von downstream empfangene Mitgliedschaftsberichte werden zusammengefasst und vom Switch dazu verwendet, seine eigenen Berichte auszugeben).
- Der Switch sendet IGMP-Mitgliedschaftsberichte nur von denjenigen Ports, an denen Multicast-Router angeschlossen sind, da das Senden von Mitgliedschaftsberichten an Hosts dazu führen kann, dass ein Host unbeabsichtigt daran gehindert wird, einer spezifischen Gruppe beizutreten.
- Multicast-Router verwenden IGMP, um einen Master-Router als sogenannten *Querier* auszuwählen. Der *Querier* ist der Router mit der kleinsten IP-Adresse. Alle anderen Router werden Non-Querier und nehmen nur an der Weiterleitung von Multicast-Datenverkehr teil. Switches im aktiven Modus nehmen genauso wie Multicast-Router an der Querier-Wahl teil.
- Wenn die Querier-Wahl abgeschlossen ist, gibt der Switch vom Querier empfangene IGMP-Abfragen einfach weiter.
- Beim Senden von IGMP-Paketen verwendet der Switch seine eigene IP-Adresse, sofern er eine hat, für das VLAN, auf dem die Pakete gesendet werden, oder er verwendet die Adresse 0.0.0.0, sofern ihm keine IP-Adresse zugeordnet ist.

HINWEIS

IGMP-Snooping-Switches führen das Multicast-Pruning mithilfe der Ziel-MAC-Multicast-Adresse des Multicast-Frames durch, die von der IP-Multicast-Adresse der Gruppe abhängig ist. Die IP-Adresse W.X.Y.Z entspricht der MAC-Adresse 01-00-5E-XX-YY-ZZ. Dabei sind XX die niederen 7 Bits von X, und YY und ZZ sind einfach Y und Z in Hexadezimalcodierung.

Es ist zu beachten, dass IP-Multicast-Adressen wie 224.1.1.1 und 225.1.1.1 beide der gleichen MAC-Adresse 01-00-5E-01-01-01 zugeordnet werden. Dies ist ein Problem, für das die IETF Network Working Group derzeit keine Lösung anbietet. Die Benutzer sind angehalten, dieses Problem zu beachten und zu vermeiden.

IGMP und RSTP

Eine durch RSTP vorgenommene Topologieänderung kann bewirken, dass die für den Multicast-Datenverkehr ausgewählten Routen inkorrekt werden. Dies führt zu verlorenem Multicast-Traffic.

Wenn RSTP eine Änderung in der Netzwerktopologie erkennt, unternimmt IGMP einige Maßnahmen, um den Verlust von Multicast-Konnektivität zu verhindern und die Konvergenzzeit des Netzwerks zu reduzieren:

- Der Switch gibt sofort IGMP-Abfragen aus (sofern er sich im aktiven IGMP-Modus befindet), um mögliche Informationen über neue Gruppenmitgliedschaften abzurufen.
- Der Switch kann so konfiguriert werden, dass er temporär Multicast-Streams von allen Ports flutet, bei denen es sich nicht um RSTP-Edge-Ports handelt.

Kombinierter Router- und Switch-Betrieb mittels IGMP

Das folgende Beispiel zeigt die Herausforderungen bei mehreren Routern, VLAN-Unterstützung und Switching.

Producer P1 befindet sich in VLAN 2, während sich P2 in VLAN 3 befindet. Consumer C1 befindet sich in beiden VLANs, während sich C2 und C3 jeweils in VLAN 3 und 2 befinden. Router 2 befindet sich in VLAN 2, vermutlich, um Multicast-Datenverkehr an ein entferntes Netzwerk weiterzuleiten oder um selbst als Quelle für Multicast-Verkehr zu fungieren.

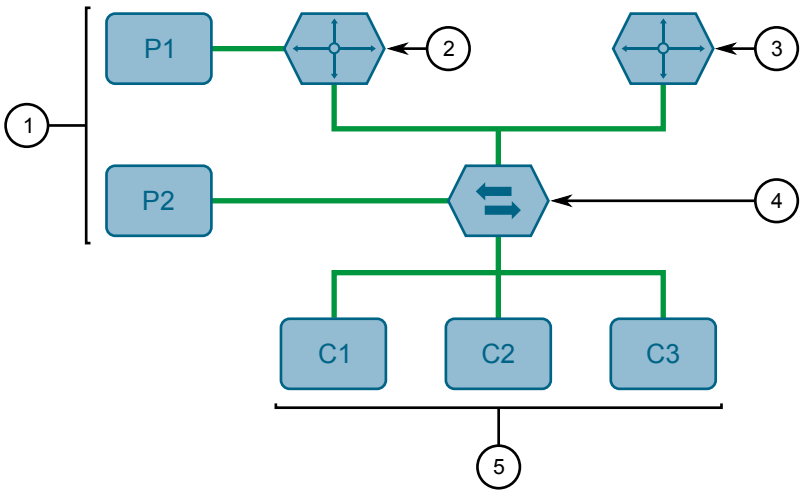


Abbildung 6: Beispiel – Kombinierter Router- und Switch-Betrieb mittels IGMP

1. Producer **2.** Multicast-Router 1 **3.** Multicast-Router 2 **4.** Switch **5.** Host

In diesem Beispiel:

- P1, Router 1, Router 2 und C3 befinden sich in VLAN 2
- P2 und C2 befinden sich in VLAN 3
- C1 befindet sich in VLAN 2 und 3

Vorausgesetzt, Router 1 ist der Querier für VLAN 2 und Router 2 ist einfach ein Non-Querier, empfängt der Switch regelmäßig Abfragen von Router 1 und speichert die Informationen, welcher Port eine Verbindung mit dem Multicast-Router herstellt. Der Switch-Port, der die Verbindung zu Router 2 herstellt, muss jedoch manuell als *Router-Port* konfiguriert werden. Andernfalls sendet der Switch weder Multicast-Streams noch join/leave-Nachrichten an Router 2.

Zu beachten ist, dass VLAN 3 über keinen externen Multicast-Router verfügt. Der Switch sollte für den Betrieb im Modus *ohne Router* konfiguriert werden und allgemeine Mitgliedschaftsabfragen ausgeben, als wäre er der Router.

- **Verarbeitung von Beitritten**
  Wenn Host C1 die Multicast-Streams von P1 und P2 abonnieren möchte, generiert er zwei Mitgliedschaftsberichte. Der Mitgliedschaftsbericht von C1 in VLAN 2 verursacht, dass der Switch sofort einen eigenen Mitgliedschaftsbericht an Multicast-Router 1 initiiert (und seinen eigenen Mitgliedschaftsbericht als Antwort auf Abfragen ausgibt).

  Der Mitgliedschaftsbericht von Host C1 für VLAN 3 verursacht, dass der Switch sofort damit beginnt, Multicast-Traffic von Producer P2 an Host C2 weiterzuleiten.
- **Verarbeitung von Austritten**
  Wenn Host C1 sich für den Austritt aus einer Multicast-Gruppe entscheidet, gibt er eine leave-Anforderung an den Switch aus. Der Switch fragt den Port ab, zu festzustellen, ob Host C1 das letzte Mitglied der Gruppe an dem Port ist. Ist Host C1 das letzte (oder einzige) Mitglied, wird die Gruppe sofort an dem Port zurückgeschnitten.

  Verlässt Host C1 die Multicast-Gruppe ohne eine leave group-Nachricht auszugeben und reagiert dann nicht auf eine allgemeine Mitgliedschaftsabfrage, stellt der Switch die Weiterleitung von Datenverkehr nach zwei Abfragen ein.

  Wenn der letzte Port in einer Multicast-Gruppe die Gruppe verlässt (oder durch Veralterung entfernt wird), gibt er Switch einen IGMP-Austrittsbericht an den Router aus.

Abschnitt 8.4.1.2
GMRP (GARP Multicast Registration Protocol)

Das GARP Multicast Registration Protocol (GMRP) ist eine Anwendung des Generic Attribute Registration Protocol (GARP) und bietet einen Layer-2-Mechanismus zum Verwalten von Multicast-Gruppenmitgliedschaften in einem überbrückten Layer-2-Netzwerk. Es ermöglicht Ethernet-Switches und Endgeräten, Mitgliedschaften in Multicast-Gruppen mit anderen Switches in einem LAN anzumelden bzw. abzumelden, woraufhin diese Informationen an alle Switches im LAN verteilt werden, die erweiterte Filterdienste unterstützen.

GMRP ist ein Standardprotokoll der Branche, das ursprünglich in IEEE 802.1D-1998 festgelegt und in IEEE 802.1Q-2005 erweitert wurde. GARP wurde in IEEE 802.1D-1998 festgelegt und in 802.1D-2004 aktualisiert.

HINWEIS
GMRP bietet ähnliche Funktionalität in Layer 2 wie IGMP in Layer 3.

Einer Multicast-Gruppe beitreten

Um einer Multicast-Gruppe beizutreten, sendet ein Endgerät eine GMRP-Nachricht vom Typ *join*. Der Switch, der die *join*-Nachricht empfängt, fügt den Port, über den die Nachricht empfangen wurde, der in der Nachricht angegebenen Multicast-Gruppe hinzu. Dann propagiert er die *join*-Nachricht an alle anderen Hosts im VLAN, von denen einer die Multicast-Quelle sein soll.

Wenn ein Switch GMRP-Updates sendet (von GMRP-fähigen Ports), werden alle dem Switch bekannten Multicast-Gruppen, egal ob manuell konfiguriert oder dynamisch über GMRP gelernt, dem Rest des Netzwerks angekündigt.

Solange sich ein Host in dem Layer-2-Netzwerk für eine bestimmte Multicast-Gruppe angemeldet hat, wird der Datenverkehr von der entsprechenden Multicast-Quelle im Netzwerk übertragen. Multicast-Verkehr von der Quelle wird von jedem Switch im Netzwerk nur an jene Ports weitergeleitet, von denen der Switch join-Nachrichten für die Multicast-Gruppe erhalten hat.

Eine Multicast-Gruppe verlassen

Der Switch sendet regelmäßig GMRP-Abfragen in Form einer *leave all*-Nachricht. Wenn ein Host (entweder ein Switch oder ein Endgerät) in einer Multicast-Gruppe bleiben möchte, bestätigt er seine Gruppenmitgliedschaft durch Beantworten der Abfrage mit einer entsprechenden *join*-Anfrage. Andernfalls kann er mit einer *leave*-Nachricht antworten oder einfach gar nicht antworten. Wenn der Switch vom Host eine *leave*-Nachricht empfängt oder nach Ablauf eines Timeout-Zeitraums keine Antwort empfangen hat, entfernt der Switch den Host aus der Multicast-Gruppe.

Hinweise zu GMRP

Da GMRP eine Anwendung von GARP ist, erfolgen Transaktionen mit dem GARP-Protokoll. GMRP definiert die folgenden beiden Attributtypen:

- Den Attributtyp Group zur Identifikation der Werte von Gruppen-MAC-Adressen
- Den Attributtyp Service Requirement zur Identifikation von Serviceanforderungen für die Gruppe

Attribute für Serviceanforderungen dienen dazu, für das Multicast-Filterverhalten des empfangenden Ports eines der folgenden Verhalten festzulegen:

- Sämtlichen Multicast-Gruppenverkehr im VLAN weiterleiten oder
- Sämtlichen unbekannten Verkehr weiterleiten (Multicast-Gruppen), für den in einem VLAN in dem Gerät keine Mitglieder angemeldet sind

Wenn GMRP auf dem RUGGEDCOM RX1400 deaktiviert ist, werden empfangene GMRP-Pakete wie jeder andere Datenverkehr weitergeleitet. Ansonsten werden GMRP-Pakete vom RUGGEDCOM RX1400 verarbeitet und nicht weitergeleitet.

Beispiel: Mitgliedschaft mit GMRP einrichten

Im folgenden Beispiel wird dargestellt, wie ein Netzwerk aus Hosts und Switches mit GMRP dynamisch zwei Multicast-Gruppen beitreten kann.

Bei diesem Szenario gibt es zwei Multicast-Quellen, S1 und S2, die jeweils per Multicast an die Multicast-Gruppen 1 und 2 übertragen. Ein Netzwerk aus fünf Switches, einschließlich einem Core-Switch (B), verbindet die Quellen mit zwei Hosts, H1 und H2, die jeweils die Multicast-Streams von S1 und S2 empfangen.

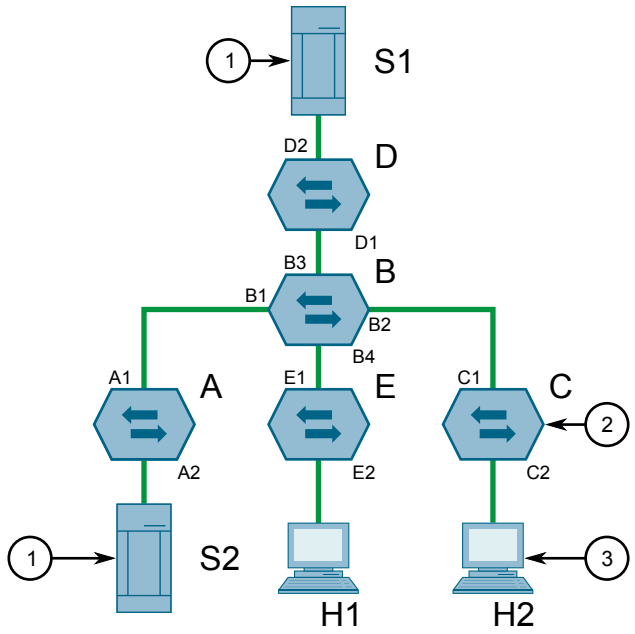


Abbildung 7: Beispiel – Mitgliedschaft mit GMRP einrichten

1. Multicast-Quelle **2.** Switch **3.** Multicast-Host

Die Hosts und Switches richten die Mitgliedschaft in den Multicast-Gruppen 1 und 2 wie folgt ein:

1. Host H1 ist nicht GMRP-fähig, muss jedoch den Datenverkehr für Multicast-Gruppe 1 sehen. Deshalb wird Port E2 an Switch E statisch so konfiguriert, dass er den Datenverkehr für Multicast-Gruppe 1 weiterleitet.
2. Switch E kündigt dem Netzwerk die Mitgliedschaft in Multicast-Gruppe 1 über Port E1 an und macht aus Port B4 an Switch B ein Mitglied in Multicast-Gruppe 1.
3. Switch B propagiert die *join*-Nachricht, wodurch die Ports A1, C1 und D1 zu Mitgliedern von Multicast-Gruppe 1 werden.
4. Host H2 ist GMRP-fähig und sendet eine *join*-Anfrage für Multicast-Gruppe 2 an Port C2, welcher dadurch zum Mitglied von Multicast-Gruppe 2 wird.
5. Switch C propagiert die *join*-Nachricht, wodurch die Ports A1, B2, D1 und E1 zu Mitgliedern von Multicast-Gruppe 2 werden.

Sobald die GMRP-basierte Anmeldung im Netzwerk propagiert wurde, kann der Multicast-Verkehr von S1 und S2 sein Ziel wie folgt erreichen:

- Quelle S1 sendet Multicast-Verkehr an Port D2, welcher über Port D1 weitergeleitet wird, der zuvor zu einem Mitglied von Multicast-Gruppe 1 wurde.
- Switch B leitet den Multicast von Gruppe 1 über Port B4 in Richtung Switch E weiter.
- Switch E leitet den Multicast von Gruppe 1 über Port E2 weiter, der statisch für die Mitgliedschaft in Multicast-Gruppe 1 konfiguriert wurde.
- Host H1 ist mit Port E2 verbunden und empfängt deshalb den Multicast von Gruppe 1.
- Quelle S2 sendet Multicast-Verkehr an Port A2, welcher dann über Port A1 weitergeleitet wird, der zuvor zu einem Mitglied von Multicast-Gruppe 2 wurde.
- Switch B leitet den Multicast von Gruppe 2 über Port B2 in Richtung Switch C weiter.

- Switch C leitet den Multicast von Gruppe 2 über Port C2 weiter, der zuvor zu einem Mitglied von Gruppe 2 wurde.
- Schließlich empfängt Host H2, der mit Port C2 verbunden ist, den Multicast von Gruppe 2.

Abschnitt 8.4.2
GMRP aktivieren und konfigurieren

Um das GMRP (GARP Multicast Registration Protocol) zu aktivieren und zu konfigurieren, gehen Sie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***switch » mcast-filtering*** und konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
enabled	**Zusammenfassung:** { true, false } **Standard:** false GMRP aktivieren
rstp-flooding	Bestimmt, ob Multicast-Streams bei Erkennung einer Topologieänderung aus allen Rapid Spanning Tree Protocol (RSTP)-Ports, die keine Edge-Ports sind, überflutet werden. Eine solche Überflutung ist dann von Vorteil, wenn die Multicast-Stream-Anlieferung ohne Unterbrechung gewährleistet sein muss.
leave-timer { leave-timer }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 600 und 300000 **Standard:** 4000 Die Zeit in Millisekunden, die nach dem Auslösen von "Leave" oder "LeaveAll" gewartet werden muss, bevor registrierte Multicast-Gruppen entfernt werden. Wenn Join-Nachrichten für bestimmte Adressen empfangen werden, bevor dieser Timer abläuft, bleiben die Adressen registriert.

3. Aktivieren Sie GMRP an einem oder mehreren Switched-Ethernet-Ports. Weitere Informationen finden Sie unter Abschnitt 8.1.2, „Einen Switched-Ethernet-Port konfigurieren“.
4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 8.4.3
IGMP Snooping verwalten

Dieser Abschnitt beschreibt, wie Sie IGMP Snooping konfigurieren, und Ports, die von diesem Dienst überwacht werden, verwalten können.

INHALT

- Abschnitt 8.4.3.1, „IGMP Snooping konfigurieren“
- Abschnitt 8.4.3.2, „Eine Liste der Router-Ports anzeigen“
- Abschnitt 8.4.3.3, „Einen Router-Port hinzufügen“
- Abschnitt 8.4.3.4, „Einen Router-Port löschen“

Abschnitt 8.4.3.1
IGMP Snooping konfigurieren

Um das IGMP Snooping zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***switch » mcast-filtering » igmp-snooping*** und konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
igmp-mode { igmp-mode }	**Zusammenfassung:** { active, passive } **Standard:** passive Legt den IGMP-Modus fest: • PASSIVE : Der Switch untersucht IGMP-Verkehr passiv und sendet niemals IGMP-Abfragen. • ACTIVE : Der Switch generiert IGMP-Abfragen, wenn für eine Weile keine Abfragen von einem besseren Kandidaten für den Querier erkannt werden.
igmp-query-interval { igmp-query-interval }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 10 und 3600 **Standard:** 60 Das Zeitintervall zwischen den vom Switch generierten IGMP-Abfragen. HINWEIS: Dieser Parameter wirkt sich auch auf das Intervall der Gruppenmitgliedschaft (d. h. die Alterungszeit der Gruppenteilnehmer) aus und ist daher auch im PASSIVE-Modus wirksam.
router-forwarding	**Zusammenfassung:** { true, false } **Standard:** true Bestimmt, ob Multicast-Streams immer an Multicast-Router weitergeleitet werden.
rstp-flooding	Bestimmt, ob Multicast-Streams bei Erkennung einer Topologieänderung aus allen Rapid Spanning Tree Protocol (RSTP)-Ports, die keine Edge-Ports sind, überflutet werden. Eine solche Überflutung ist dann von Vorteil, wenn die Multicast-Stream-Anlieferung ohne Unterbrechung gewährleistet sein muss.

3. Weisen Sie einen oder mehrere Ports für das IGMP zu, die verwendet werden, wenn Mitgliedschaftmeldungen gesendet werden. Für weitere Informationen siehe Abschnitt 8.4.3.3, „Einen Router-Port hinzufügen“.
4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 8.4.3.2
Eine Liste der Router-Ports anzeigen

Um eine Liste der für IGMP Snooping verwendeten Router-Ports anzusehen, geben Sie Folgendes ein:

```
show running-config switch mcast-filtering igmp-snooping router-ports
```

Falls Router-Ports konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config switch mcast-filtering igmp-snooping router-ports | tab SLOT PORT
 ------------ swport 1 ! !
```

Falls keine Router-Ports konfiguriert wurden, fügen Sie je nach Bedarf Ports hinzu. Weitere Informationen finden Sie unter Abschnitt 8.4.3.3, „Einen Router-Port hinzufügen“.

Abschnitt 8.4.3.3
Einen Router-Port hinzufügen

Um einen Router-Port für das IGMP Snooping hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den Router-Port hinzu, indem Sie Folgendes eingeben:

   ```
   switch mcast-filtering igmp-snooping router-ports swport port
   ```

   Erläuterung:

   - *port* ist die Nummer des Ports (oder eine Liste von Ports, wenn sie in einem Port-Trunk gebündelt sind) für das Modul.
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 8.4.3.4
Einen Router-Port löschen

Um einen Router-Port für das IGMP Snooping zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den Router-Port, indem Sie Folgendes eingeben:

   ```
   no switch mcast-filtering igmp-snooping router-ports swport port
   ```

   Erläuterung:

   - *slot* ist die Bezeichnung des Modul-Einbauorts
   - *port* ist die Nummer des Ports (oder eine Liste von Ports, wenn sie in einem Port-Trunk gebündelt sind) für das Modul.
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 8.4.4
Die statische Multicast-Gruppen-Tabelle verwalten

Dieser Abschnitt beschreibt, wie Sie Einträge in der statischen Multicast-Gruppen-Tabelle verwalten können.

INHALT

- Abschnitt 8.4.4.1, „Eine Liste statischer Multicast-Gruppeneinträge anzeigen“
- Abschnitt 8.4.4.2, „Einen Eintrag für eine statische Multicast-Gruppe hinzufügen“
- Abschnitt 8.4.4.3, „Einen Eintrag für eine statische Multicast-Gruppe löschen“

Abschnitt 8.4.4.1
Eine Liste statischer Multicast-Gruppeneinträge anzeigen

Um eine Liste mit Einträgen der bekannten statischen Multicast-Gruppen auf anderen Geräten anzusehen, geben Sie Folgendes ein:

```
show running-config switch mcast-filtering static-mcast-table
```

Falls Einträge erstellt wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config switch mcast-filtering static-mcast-table
switch mcast-filtering
 static-mcast-table 10 01:00:00:01:01:01
 !
!
```

Falls keine Einträge konfiguriert wurden, fügen Sie je nach Bedarf Einträge hinzu. Weitere Informationen finden Sie unter Abschnitt 8.4.4.2, „Einen Eintrag für eine statische Multicast-Gruppe hinzufügen“.

Abschnitt 8.4.4.2
Einen Eintrag für eine statische Multicast-Gruppe hinzufügen

Um eine statische Multicast-Gruppe von einem anderen Gerät in der Tabelle "Static Multicast Summary" aufzuführen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den Tabelleneintrag hinzu, indem Sie Folgendes eingeben:

   HINWEIS
   Die Buchstaben in MAC-Adressen müssen Kleinbuchstaben sein.

   ```
   switch mcast-filtering static-mcast-table id address
   ```

   Erläuterung:

   - *id* ist die ID für das VLAN, über das die statische Multicast-Gruppe arbeitet
   - *address* ist die MAC-Adresse für das Gerät in der Form 01:xx:xx:xx:xx:xx
3. Fügen Sie einen oder mehrere ausgehende (egress) Ports hinzu. Weitere Informationen finden Sie unter Abschnitt 8.4.5.2, „Hinzufügen eines ausgehenden (egress) Ports“.
4. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 8.4.4.3
Einen Eintrag für eine statische Multicast-Gruppe löschen

Um eine statische Multicast-Gruppe aus der Tabelle "Static Multicast Summary" zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den Tabelleneintrag, indem Sie Folgendes eingeben:

   ```
   no switch mcast-filtering static-mcast-table id address
   ```

Erläuterung:

- *id* ist die ID für das VLAN, über das die statische Multicast-Gruppe arbeitet
- *address* ist die MAC-Adresse für das Gerät in der Form 01:xx:xx:xx:xx:xx

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 8.4.5

Ausgehende (egress) Ports für Multicast-Gruppen verwalten

Dieser Abschnitt beschreibt, wie Sie ausgehende (egress) Ports für eine Multicast-Gruppe konfigurieren und verwalten können.

INHALT

- Abschnitt 8.4.5.1, „Eine Liste der ausgehenden (egress) Ports anzeigen“
- Abschnitt 8.4.5.2, „Hinzufügen eines ausgehenden (egress) Ports“
- Abschnitt 8.4.5.3, „Löschen eines ausgehenden (egress) Ports“

Abschnitt 8.4.5.1

Eine Liste der ausgehenden (egress) Ports anzeigen

Um eine Liste der ausgehenden (egress) Ports für eine statische Multicast-Gruppe anzuzeigen, die in der Tabelle "Static Multicast Group Summary" festgelegt ist, geben Sie Folgendes ein:

```
show switch mcast-filtering static-mcast-table id address egress-ports
```

Erläuterung:

- *id* ist die ID für das VLAN, über das die statische Multicast-Gruppe arbeitet
- *address* ist die MAC-Adresse für das Gerät in der Form 01:xx:xx:xx:xx:xx

Falls ausgehende (egress) Ports erstellt wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config switch mcast-filtering static-mcast-table 10 01:00:00:01:01:01 egress-
ports
switch mcast-filtering
 static-mcast-table 10 01:00:00:01:01:01
  egress-ports swport 1
  !
 !
!
```

Falls keine ausgehende (egress) Ports konfiguriert wurden, fügen Sie je nach Bedarf ausgehende Ports hinzu. Weitere Informationen finden Sie unter Abschnitt 8.4.5.2, „Hinzufügen eines ausgehenden (egress) Ports“.

Abschnitt 8.4.5.2
Hinzufügen eines ausgehenden (egress) Ports

Um einen ausgehenden (egress) Port zu einer statischen Multicast-Gruppe hinzuzufügen, die in der Tabelle Static Multicast Group Summary festgelegt ist, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den ausgehenden (egress) Port hinzu, indem Sie Folgendes eingeben:

   ```
   switch mcast-filtering static-mcast-table id address egress-ports swport port
   ```

   Erläuterung:

   - *id* ist die ID für das VLAN, über das die statische Multicast-Gruppe arbeitet
   - *address* ist die MAC-Adresse für das Gerät in der Form 01:xx:xx:xx:xx:xx
   - *port* ist die Nummer des Ports (oder eine Liste von Ports, wenn sie in einem Port-Trunk gebündelt sind) für das Modul.
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 8.4.5.3
Löschen eines ausgehenden (egress) Ports

Um einen ausgehenden (egress) Port für eine statische Multicast-Gruppe zu löschen, die in der Tabelle Static Multicast Group Summary festgelegt ist, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den Tabelleneintrag, indem Sie Folgendes eingeben:

   ```
   no switch mcast-filtering static-mcast-table id address egress-ports swport port
   ```

   Erläuterung:

   - *id* ist die ID für das VLAN, über das die statische Multicast-Gruppe arbeitet
   - *address* ist die MAC-Adresse für das Gerät in der Form 01:xx:xx:xx:xx:xx
   - *port* ist die Nummer des Ports (oder eine Liste von Ports, wenn sie in einem Port-Trunk gebündelt sind) für das Modul.
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 8.4.6
Ein Übersicht der Multicast-Gruppen anzeigen

Um eine Übersicht aller Multicast-Gruppen anzusehen, geben Sie Folgendes ein:

```
show switch mcast-filtering mcast-group-summary
```

Falls Multicast-Gruppen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show switch mcast-filtering mcast-group-summary
                        STATIC  STATIC  GMRP    GMRP
```

```
VID  MAC               SLOT    PORTS   SLOT    PORTS
-------------------------------------------------------
100  01:00:5e:00:01:01
                        swport  1
                                        swport  none
200  01:00:5e:00:01:02
                        swport  2
                                        swport  none
```

Diese Tabelle oder Liste liefert die folgenden Informationen:

Parameter	Beschreibung
vid	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl Die VLAN-Kennung für das VLAN, über das die statische Multicast-Gruppe arbeitet.
mac	**Zusammenfassung:** Eine Zeichenkette mit 17 Zeichen Die MAC-Adresse der Multicast-Gruppe.

Abschnitt 8.4.7

Eine Liste der IP-Multicast-Gruppen anzeigen

Um eine Liste aller IP-Multicast-Gruppen anzuzeigen, geben Sie Folgendes ein:

```
show switch mcast-filtering ip-mcast-groups
```

Falls IP-Multicast-Gruppen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show switch mcast-filtering ip-mcast-groups
     IP                            JOINED     JOINED  ROUTER     ROUTER
VID  ADDRESS    MAC                SLOT       PORTS   SLOT       PORTS
-------------------------------------------------------------------------
100  225.0.1.1  01:00:5e:00:01:01
                                   swport     3
                                              swport     1
200  225.0.1.2  01:00:5e:00:01:02
                                   swport     4
                                              swport     2
```

Diese Tabelle oder Liste liefert die folgenden Informationen:

Parameter	Beschreibung
vid	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl Die VLAN-Kennung für das VLAN, über das die statische Multicast-Gruppe arbeitet.
ip-address	**Zusammenfassung:** Eine Zeichenkette Die IP-Adresse der Multicast-Gruppe.
mac	**Zusammenfassung:** Eine Zeichenkette mit 17 Zeichen Die Multicast-MAC-Adresse entsprechend der IP-Adresse der Multicast-Gruppe. Dieser Parameter ist obligatorisch.
Joined Slot	Die Bezeichnung des Modul-Einbauorts gemäß Siebdruck auf der Geräteoberseite.
Joined Ports	Die ausgewählten Ports am Modul, die am angegebenen Steckplatz installiert sind.
Router Slot	Die Bezeichnung des Modul-Einbauorts gemäß Siebdruck auf der Geräteoberseite.

Parameter	Beschreibung
Router Ports	Die ausgewählten Ports am Modul, die am angegebenen Steckplatz installiert sind.

Abschnitt 8.5
VLANs verwalten

Ein Virtual Local Area Network (VLAN) ist eine Gruppe von Geräten an einem oder mehreren LAN-Segmenten, die so kommunizieren, als ob sie an dasselbe physische LAN-Segment angeschlossen wären. VLANs sind äußerst flexibel, da sie eher auf logischen als auf auf physikalischen Verbindungen beruhen.

Bei Einführung eines VLAN muss der gesamte Verkehr im Netzwerk zu dem einen oder anderen VLAN gehören. Der Verkehr auf einem VLAN kann nicht an ein anderes VLAN weitergeleitet werden, außer über einen Internetwork-Router oder Layer-3-Switch.

VLANs werden auf drei Arten erstellt:

- **Explizit**
  Statische VLANs können im Switch erstellt werden. Weitere Informationen über statische VLANs finden Sie unter Abschnitt 8.5.5, „Statische VLANs verwalten“.
- **Implizit**
  Wenn eine VLAN-ID (VID) für ein Port-VLAN (PVLAN), eine statische MAC-Adresse oder eine IP-Schnittstelle eingestellt ist, wird automatisch ein entsprechendes VLAN erstellt, sofern es noch nicht vorhanden ist.
- **Dynamisch**
  VLANs können über GVRP gelernt werden. Weitere Informationen über GVRP finden Sie unter Abschnitt 8.5.1.7, „GARP VLAN Registration-Protokoll (GVRP)“.

INHALT

- Abschnitt 8.5.1, „VLAN-Konzepte“
- Abschnitt 8.5.2, „Konfigurieren des internen VLAN-Bereichs“
- Abschnitt 8.5.3, „Eingangsfilterung aktivieren/deaktivieren“
- Abschnitt 8.5.4, „VLANs für Switched-Ethernet-Ports verwalten“
- Abschnitt 8.5.5, „Statische VLANs verwalten“
- Abschnitt 8.5.6, „Verbotene Ports verwalten“
- Abschnitt 8.5.7, „VLANs für Schnittstellen und Tunnel verwalten“

Abschnitt 8.5.1
VLAN-Konzepte

Dieser Abschnitt beschreibt einige wesentliche Konzepte für die Implementierung von VLANs in RUGGEDCOM ROX II.

INHALT

- Abschnitt 8.5.1.1, „Getaggte und ungetaggte Frames“
- Abschnitt 8.5.1.2, „Natives VLAN“

- Abschnitt 8.5.1.3, „Edge- und Trunk-Porttypen“
- Abschnitt 8.5.1.4, „Eingangsfilterung“
- Abschnitt 8.5.1.5, „Liste verbotener Ports“
- Abschnitt 8.5.1.6, „VLAN-fähige Betriebsart“
- Abschnitt 8.5.1.7, „GARP VLAN Registration-Protokoll (GVRP)“
- Abschnitt 8.5.1.8, „PVLAN Edge“
- Abschnitt 8.5.1.9, „Vorteile von VLANs“

Abschnitt 8.5.1.1

Getaggte und ungetaggte Frames

VLAN-Tags kennzeichnen Frames als Teile eines VLAN-Netzwerks. Wenn ein Switch einen Frame mit einem VLAN-Tag (oder 802.1Q-Tag) empfängt, wird der VLAN-Identifier (VID) ausgelesen und der Frame an andere Ports im gleichen VLAN weitergeleitet.

Enthält ein Frame kein VLAN-Tag oder enthält er ein 802.1p-Tag (Priorisierungstag), das nur prioritäre Informationen enthält, und einen VID 0, gilt er als ungetaggter Frame.

Abschnitt 8.5.1.2

Natives VLAN

Jedem Port ist eine native VLAN-Nummer, die Port-VLAN-ID (PVID), zugeordnet. Wenn ein ungetaggter Frame an einem Port eintrifft, wird er dem nativen VLAN des Ports zugeordnet.

Wenn ein Switch einen Frame über das native VLAN überträgt, sendet er den Frame standardmäßig ungetaggt. Der Switch kann jedoch so konfiguriert werden, dass er getaggte Frames im nativen VLAN überträgt.

Abschnitt 8.5.1.3

Edge- und Trunk-Porttypen

Jeder Port kann als Edge- oder Trunk-Port konfiguriert werden.

Ein Edge-Port verbindet sich mit einem einzelnen Endgerät wie beispielsweise einem PC oder einem IED-Gerät (Intelligent Electronic Device). Ein Edge-Port überträgt Verkehr im nativen VLAN.

Trunk-Ports sind Teil des Netzwerks und übertragen Verkehr für alle VLANs zwischen Switches. Trunk-Ports sind automatisch Mitglieder aller im Switch konfigurierten VLANs.

Der Switch kann Verkehr "weiterleiten", d.h. er leitet Frames weiter, die an einem Trunk-Port von einem anderen Trunk-Port empfangen wurden. Die Trunk-Ports müssen Mitglieder aller VLANs sein, von denen der "weitergeleitete" Verkehr ein Teil ist und zwar auch dann, wenn keines dieser VLANs an Edge-Ports verwendet wird.

Frames, die vom Port an allen VLANs (mit Ausnahme des nativen VLANs des Ports) übertragen werden, werden immer markiert (getaggt) gesendet.

HINWEIS
Es ist möglicherweise erwünscht, den Verkehr am Trunk-Port auf eine bestimmte Gruppe von VLANs einzuschränken. Beispiel: Wenn der Trunk-Port sich mit einem Gerät wie einem Layer-3-Router

verbindet, der eine Teilmenge der verfügbaren LANs unterstützt. Um zu vermeiden, dass der Trunk-Port ein Mitglied des VLANs ist, nehmen Sie diesen in die Liste der verbotenen Ports des VLANs auf.

Weitere Informationen über die Liste der verbotenen Ports finden Sie unter Abschnitt 8.5.1.5, „Liste verbotener Ports“.

Porttyp	Unterstützte VLANs	PVID-Format	Verwendung
Edge	1 (nativ) konfiguriert	Nicht markiert (ungetaggt)	*Nicht-VLAN-fähige Netzwerke*: Alle Frames werden gesendet und empfangen, ohne dass dafür VLAN-Tags erforderlich sind.
		Markiert (getaggt)	*VLAN-fähige Netzwerke*: VLAN-Verkehr-Domains werden an einem einzelnen VLAN forciert.
Trunk-Port	Alle konfiguriert	Markiert (getaggt) oder nicht markiert (ungetaggt)	*Switch-zu-Switch-Verbindungen*: VLANs müssen manuell erstellt und verwaltet werden bzw. können über GVRP dynamisch gelernt werden. *Multiple-VLAN-Endgeräte*: Implementieren Sie Verbindungen zu Endgeräten, die mehrere VLANs gleichzeitig unterstützen.

Abschnitt 8.5.1.4

Eingangsfilterung

Durch die Eingangsfilterung wird überprüft, ob eingehende Pakete in einem Netzwerk tatsächlich vom erwarteten Absender stammen, bevor ihr Zugang (oder Eingang) freigegeben wird.

Ist die Eingangsfilterung aktiviert, prüft der Switch jeden getaggten Frame, der an einem Port eingeht. Gehört der Port nicht zum VLAN, dem der Frame zugeordnet ist, wird der Frame abgelehnt. Ist die Eingangsfilterung deaktiviert, werden Frames von VLANs, die für den Switch konfiguriert sind, nicht abgelehnt. Weitere Informationen über die Aktivierung und Deaktivierung der Eingangsfilterung finden Sie unter Abschnitt 8.5.3, „Eingangsfilterung aktivieren/deaktivieren“.

Abschnitt 8.5.1.5

Liste verbotener Ports

Mit der Liste der verbotenen Ports kann jedes VLAN so konfiguriert werden, dass bestimmte Ports aus dem VLAN ausgeschlossen werden. Mehr Informationen über die Konfiguration einer Liste verbotener Ports enthält Abschnitt 8.5.6, „Verbotene Ports verwalten“.

Abschnitt 8.5.1.6

VLAN-fähige Betriebsart

Die systemeigene Betriebsart für einen IEEE 802.1Q-kompatiblen Switch ist VLAN-fähig. Selbst wenn eine bestimmte Netzwerkarchitektur keine VLANs verwendet, ermöglichen die standardmäßigen VLAN-Einstellungen von RUGGEDCOM ROX II, dass der Switch weiterhin in einem VLAN-fähigen Modus betrieben werden kann, während er gleichzeitig eine Funktionalität bietet, die für fast jede Netzwerkanwendung erforderlich ist. Der Standard IEEE 802.1Q legt jedoch Regeln fest, die von allen VLAN-fähigen Switches einzuhalten sind:

- Gültige VIDs liegen im Bereich zwischen 1 und 4094. VIDs mit einem Wert von 0 oder 4095 sind ungültig.
- Jedem Frame, der in einen VLAN-fähigen Switch eingeht, ist eine gültige VID zugeordnet.

- Jeder Frame, der einen VLAN-fähigen Switch verlässt, ist entweder nicht "getaggt" (markiert) oder mit einer gültigen VID markiert. Mit Priorität markierte Frames mit einer ungültigen VID werden von einem VLAN-fähigen Switch niemals gesendet.

HINWEIS
Die Anforderungen einiger Anwendungen stehen mit der Betriebsart von IEEE 802.Q im Widerspruch. Beispielsweise müssen bei einigen Anwendungen die Endgeräte explizit mit Priorität markierte Frames empfangen.

Abschnitt 8.5.1.7

GARP VLAN Registration-Protokoll (GVRP)

Das GARP VLAN Registration-Protokoll (GVRP) ist ein auf dem GARP (Generic Attribute Registration Protocol) aufbauendes Standardprotokoll zur automatischen Verteilung von VLAN-Konfigurationsinformationen in einem Netzwerk. Jeder Switch in einem Netzwerk braucht nur mit VLANs konfiguriert zu werden, die er lokal benötigt. An anderer Stelle im Netzwerk konfigurierte VLANs werden über GVRP gelernt. Eine für eine bestimmte VID konfigurierte GVRP-fähige Endstation (d.h. ein PC oder ein IEC-Gerät) kann mit einem Trunk-Port an einem GVRP-fähigen Switch verbunden und automatisch Teil des gewünschten VLANs werden.

Wenn ein Switch GVRP-Bridge-Protokolldaten-Units (BPDUs) von allen GVRP-aktivierten Ports sendet, kündigen die GVRP BPDUs alle diesem Switch bekannten VLANs (manuell konfiguriert oder dynamisch gelernt über GVRP) dem restlichen Netzwerk an.

Wenn ein GVRP-fähiger Switch eine GVRP BPDU empfängt, in der ein Satz VLANs angekündigt wird, wird der empfangende Port Mitglied dieser angekündigten VLANs und der Switch beginnt mit der Ankündigung dieser VLANs über alle GVRP-fähigen Ports (nicht der Port, an dem die VLANs gelernt wurden).

Zur Verbesserung der Netzwerksicherheit mithilfe von VLANs können GVRP-fähige Ports so konfiguriert werden, dass das Lernen neuer dynamischer VLANs verhindert wird und gleichzeitig wird das Ankündigen der am Switch konfigurierten VLANs zugelassen.

Nachstehend ein Beispiel für die Verwendung von GVRP:

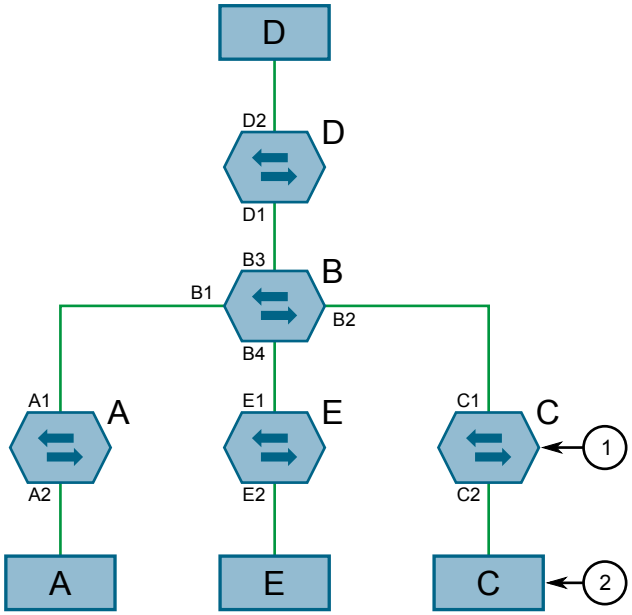


Abbildung 8: Verwenden von GVRP

1. Switch **2.** Endknoten

- Switch B ist der Core-Switch, alle anderen sind Edge-Switches
- Port A1, B1 bis B4, C1, D1, D2 und E1 sind GVRP-fähig
- Port B1 bis B4, D1 und D2 sind so eingestellt, dass sie ankündigen und lernen
- Port A1, C1 und E1 sind so eingestellt, dass sie nur ankündigen
- Port A2, C2 und E2 sind Edge-Ports
- Endknoten D ist GVRP-fähig
- Endknoten A, E und C sind nicht GVRP-fähig
- Port A2 und C2 sind konfiguriert mit PVID 7
- Port E2 ist konfiguriert mit PVID 20
- Endknoten D ist interessiert an VLAN 20, somit wird VLAN 20 durch den Knoten in Richtung Switch D angekündigt
- D2 wird Mitglied von VLAN 20
- Port A1 und C1 kündigen VID 7 an
- Port B1 und B2 werden Mitglieder von VLAN 7
- Port D1 und B1 kündigen VID 20 an
- Port B3, B4 und D1 werden Mitglieder von VLAN 20

Abschnitt 8.5.1.8

PVLAN Edge

Protected VLAN (PVLAN) Edge bezieht sich auf eine Funktion des Switch, die mehrere VLAN-Edge-Ports an einem einzelnen Gerät voneinander isoliert. Alle VLAN-Edge-Ports in einem Switch, die als *geschützt* konfiguriert sind, werden am Senden von Frames untereinander gehindert, ein Senden von Frames an andere, nicht-geschützte Ports innerhalb desselben VLANs ist jedoch zulässig. Dieser Schutzmechanismus erstreckt sich auf den gesamten Verkehr im VLAN, einschließlich Unicast-, Multicast- und Broadcast-Verkehr.

HINWEIS
Hierbei handelt es sich um eine ausschließlich lokale Funktion des Switch. PVLAN-Edge-Ports werden nicht an der Kommunikation mit Ports außerhalb des Switch gehindert, egal ob (dezentral) geschützt oder nicht.

Ports, die einer bestimmten PVID und einem VLAN-Typ eines PVLAN Edge angehören, sind Teil einer PVLAN-Edge-Gruppe. Eine PVLAN-Edge-Gruppe muss mindestens zwei Ports umfassen. Es können mehrere PVLAN-Edge-Gruppen an einem Switch existieren.

Abschnitt 8.5.1.9

Vorteile von VLANs

Im Folgenden werden einige der von VLANs gebotenen Vorteile erläutert.

» Traffic-Domain-Isolierung

VLANs werden am häufigsten für deren Fähigkeit genutzt, Verkehrsströme zwischen Gerätegruppen einzuschränken.

Unnötiger Broadcast-Verkehr kann so auf das VLAN beschränkt werden, das ihn benötigt. Broadcast-Stürme in einem VLAN müssen nicht zwangsläufig Benutzer in anderen VLANs beeinträchtigen.

Hosts in einem VLAN können daran gehindert werden, die IP-Adresse eines Hosts in einem anderen VLAN beabsichtigt oder unbeabsichtigt zu übernehmen.

Die Verwendung des Creative Bridge Filtering und mehrerer VLANs kann Unified-IP-Subnetze in mehrere Regionen unterteilen, die verschiedenen Sicherheits-/Zugriffsgrundregeln unterliegen.

Multi-VLAN-Hosts können verschiedenen VLANs unterschiedliche Verkehrstypen zuweisen.

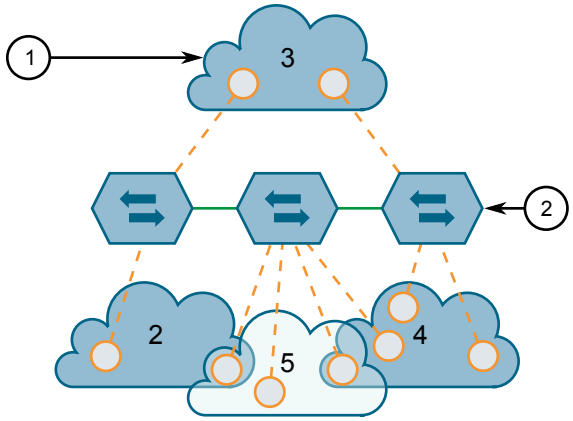


Abbildung 9: Multiple Overlapping VLANs

1. VLAN **2.** Switch

Verwaltungsvorteile

Durch die VLANs können Geräteumzüge mittels einer Neukonfiguration der Software anstelle von physischem Kabelmanagement erfolgen. Wenn der physische Standort eines Hosts geändert wird, wird häufig auch seine Verbindungsstelle geändert. Bei VLANs wird die VLAN-Zugehörigkeit und die Priorität des Hosts einfach in den neuen Port kopiert.

Reduzierte Hardware

Ohne VLANs setzt die Traffic-Domain-Isolierung den Einsatz separater Bridges für separate Netzwerke voraus. VLANs machen separate Bridges überflüssig.

Die Anzahl an Netzwerkhosts kann häufig reduziert werden. Oftmals wird ein Server zugewiesen, um Dienste für unabhängige Netzwerke zu erbringen. Diese Hosts können durch einen einzigen Multihomed-Host ersetzt werden, der jedes Netzwerk in seinem eigenen VLAN unterstützt. Dieser Host kann das Routing zwischen den VLANs ausführen.

Multi-VLAN-Hosts können verschiedenen VLANs unterschiedliche Verkehrstypen zuweisen.

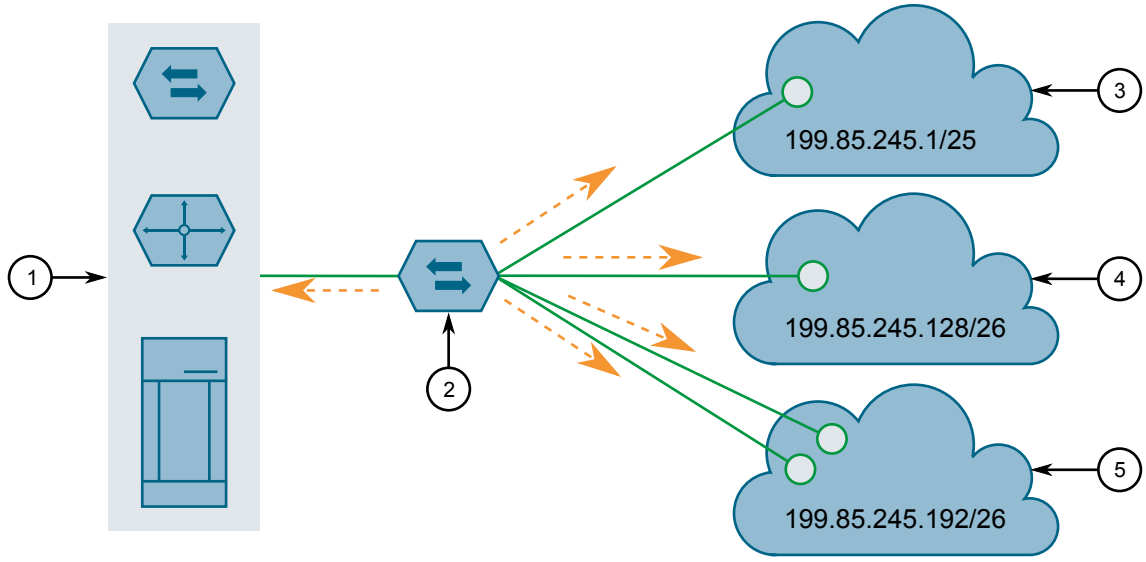


Abbildung 10: Inter-VLAN-Kommunikation

1. Server, Router oder Layer-3-Switch **2.** Switch **3.** VLAN 2 **4.** VLAN 3 **5.** VLAN 4

Abschnitt 8.5.2

Konfigurieren des internen VLAN-Bereichs

Der RUGGEDCOM ROX II erstellt und nutzt interne VLANs für interne Funktionen. Um dem RUGGEDCOM ROX II einen Pool an VLAN-IDs bereitzustellen, die für die Erstellung interner VLANs verwendet werden, muss ein VLAN-ID-Bereich reserviert werden.

ACHTUNG!
Konfigurationsgefahr – Risiko des Datenverlusts. Falls die Werte "range-start" oder "range-end" so geändert werden, dass konfigurierte interne VLANs ungültig werden, gehen die für die betroffenen VLANs definierten Konfigurationen bei der Neupositionierung verloren.

WICHTIG!
Für interne VLANs reservierte VLAN-IDs dürfen nicht vom Netzwerk verwendet werden.

HINWEIS
Durch die Änderung des Werts `range-end` *wird das übereinstimmende serielle VLAN neu positioniert. Das übereinstimmende serielle VLAN wird nicht beeinträchtigt, wenn der Wert* `range-start` *geändert wird.*

HINWEIS
Wenn bei der Konfiguration eines Switched-Ethernet- oder Trunk-Ports keine internen VLANs verfügbar sind, wird der Bereich automatisch vergrößert, sodass ein eindeutiger Wert zugewiesen werden kann.

HINWEIS
Routingfähige Ethernet-Ports und Trunks können nicht konfiguriert werden, wenn interne VLANs nicht aktiviert sind.

Um den internen VLAN-Bereich zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***admin » switch-config*** und konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

   HINWEIS
   Interne VLAN-Bereiche sind standardmäßig aktiviert.

Parameter	Beschreibung
enabled	**Zusammenfassung:** { true, false } **Standard:** false Aktiviert/Deaktiviert die Einstellungen zum Internen VLAN-Bereich. **HINWEIS** *Interne VLANs können nur deaktiviert werden, wenn alle gerouteten Ports in Switchports umgestellt wurden.*
range-start { range-start }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 2 und 4094 **Standard:** 4094 Definiert das untere Ende eines Bereichs von VLANs, die ausschließlich für das Gerät verwendet werden. VLAN ID 1 ist nicht zulässig. **HINWEIS** *range-start muss <= range-end sein*
range-end { range-end }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 2 und 4094 **Standard:** 4094 Definiert das obere Ende eines Bereichs von VLANs, die ausschließlich für das Gerät verwendet werden. VLAN ID 1 ist nicht zulässig. **HINWEIS** *range-end muss >= range-start sein*

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 8.5.3
Eingangsfilterung aktivieren/deaktivieren

Wenn die Eingangsfilterung aktiviert ist, wird jedes markierte Paket, das an einem Port ankommt, der kein Mitglied eines VLANs ist, dem dieses Paket zugeordnet ist, verworfen. Wenn deaktiviert, werden Pakete nicht verworfen.

Um eine Eingangsfilterung zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Aktivieren oder deaktivieren Sie die Eingangsfilterung, indem Sie Folgendes eingeben:

Zum Aktivieren der Eingangsfilterung

```
switch vlans ingress-filtering enabled
```

Zum Deaktivieren der Eingangsfilterung

```
no switch vlans ingress-filtering enabled
```

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 8.5.4

VLANs für Switched-Ethernet-Ports verwalten

Dieser Abschnitt beschreibt, wie Sie VLANS für Switched-Ethernet-Ports konfigurieren und verwalten können.

INHALT

- Abschnitt 8.5.4.1, „VLAN-Zuweisungen für Switched-Ethernet-Ports anzeigen“
- Abschnitt 8.5.4.2, „VLANs für Switched-Ethernet-Ports konfigurieren“

Abschnitt 8.5.4.1

VLAN-Zuweisungen für Switched-Ethernet-Ports anzeigen

Um zu bestimmen, welche VLANs jedem Switched-Ethernet-Port zugewiesen sind, geben Sie Folgendes ein:

```
show switch vlans vlan-summary
```

Eine Tabelle ähnlich dem folgenden Beispiel wird angezeigt:

```
ruggedcom# show switch vlans vlan-summary | tab
      IGMP            UNTAGD  UNTAGD  TAGGED  TAGGED
VID   SNOOPING  MSTI  SLOT    PORTS   SLOT    PORTS   QOS  INGRESS  MARK
-------------------------------------------------------------------------
1     false     0
                      swport  1,5,6
                                      swport  none
                                                      0    0
                                                      1    0
                                                      2    0
                                                      3    0
                                                      4    0
                                                      5    0
                                                      6    0
                                                      7    0
.
.
.
```

Die aufgeführten VLANs basieren auf den PVID, die den Switched-Ethernet-Ports zugewiesen sind. Weitere Informationen über die Zuweisung von PVID zu Switched-Ethernet-Ports finden Sie unter Abschnitt 8.1.2, „Einen Switched-Ethernet-Port konfigurieren“.

Abschnitt 8.5.4.2

VLANs für Switched-Ethernet-Ports konfigurieren

Wenn einem Switched-Ethernet-Port eine VLAN-ID zugeordnet ist, erscheint das VLAN in der Tabelle All-VLANs, wo es weiter konfiguriert werden kann.

Um ein VLAN für einen Switched-Ethernet-Port zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***switch » vlans » all-vlans » {id}***, wobei *{id}* die ID des VLAN ist, und konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
ip-address-src { ip-address-src }	**Zusammenfassung:** { static, dynamic } Zeigt an, ob die IP-Adresse statisch oder dynamisch über das Dynamic Host Configuration Protocol (DHCP) oder das Bootstrap Protocol (BOOTP) zugewiesen ist. Die Option DYNAMIC wird gewöhnlich für eine dynamisch zugewiesene IP-Adresse eingesetzt. Sie schaltet zwischen BOOTP und DHCP, bis sie die Antwort vom entsprechenden Server erhält. Bei nicht verwalteten Schnittstellen muss dies statisch sein. Dieser Parameter ist obligatorisch.
ipv6-address-src { ipv6-address-src }	**Zusammenfassung:** { static, dynamic } **Standard:** static Zeigt an, ob die IPv6-Adresse statisch oder dynamisch über das Dynamic Host Configuration Protocol (DHCP) zugewiesen ist. Bei nicht verwalteten Schnittstellen muss dies statisch sein.
proxyarp	Aktiviert/deaktiviert, dass das VLAN auf ARP-Anfragen für andere Hosts als sich selbst antwortet.
on-demand	Diese Schnittstelle wird nur on-Demand angesprochen.
mtu { mtu }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 68 und 9216 **Standard:** 1500 Die maximale Übertragungseinheit (die größte zulässige Paketgröße für diese Schnittstelle).

3. Fügen Sie Dienstgüte/QoS-Maps zum VLAN hinzu. Für weitere Informationen siehe Abschnitt 15.2.7.2, „Hinzufügen einer QoS-Map“.
4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 8.5.5

Statische VLANs verwalten

Dieser Abschnitt beschreibt, wie Sie statische VLANs konfigurieren und verwalten können.

INHALT

- Abschnitt 8.5.5.1, „Eine Liste der statischen VLANs anzeigen“
- Abschnitt 8.5.5.2, „Hinzufügen eines statischen VLAN“
- Abschnitt 8.5.5.3, „Ein statisches VLAN löschen“

Abschnitt 8.5.5.1

Eine Liste der statischen VLANs anzeigen

Um eine Liste der statischen VLANs anzusehen, geben Sie Folgendes ein:

```
show running-config switch vlans static-vlan
```

Falls statische VLANs konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config switch vlans static-vlan | tab
     IGMP
VID  SNOOPING  MSTI  SLOT  PORT
---------------------------------
1    -         cst

!
```

Falls keine statischen VLANs konfiguriert wurden, fügen Sie je nach Bedarf VLANs hinzu. Weitere Informationen finden Sie unter Abschnitt 8.5.5.2, „Hinzufügen eines statischen VLAN“.

Abschnitt 8.5.5.2

Hinzufügen eines statischen VLAN

Um ein VLAN für entweder einen routingfähigen Ethernet-Port oder einen virtuellen Switch hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie das statische VLAN hinzu, indem Sie Folgendes eingeben:

   ```
   switch vlans static-vlan id
   ```

   Erläuterung:

   - *id* ist die Kennung des VLANs. Die VLAN-Kennung wird zur Identifikation des VLANs in getaggten Ethernet-Frames nach IEEE 802.1Q verwendet.
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
igmp-snooping	Aktiviert oder deaktiviert IGMP Snooping auf dem VLAN.
msti { msti }	**Zusammenfassung:** { cst } oder eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 1 und 16 **Standard:** cst Nur gültig für Multiple Spanning Tree Protocol (MSTP) und wirkungslos, wenn MSTP nicht verwendet wird. Der Parameter legt die Multiple Spanning Tree-Instanz (MSTI) fest, der das VLAN zugeordnet werden soll.

4. Konfigurieren Sie je nach Bedarf eine Liste mit verbotenen Ports. Weitere Informationen finden Sie unter Abschnitt 8.5.6.2, „Einen verbotenen Port hinzufügen“.
5. Konfigurieren Sie das VLAN für den Port. Weitere Informationen finden Sie unter Abschnitt 8.5.4.2, „VLANs für Switched-Ethernet-Ports konfigurieren“.
6. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 8.5.5.3
Ein statisches VLAN löschen

Um ein statisches VLAN zu löschen, das entweder für einen routingfähigen Ethernet-Port oder einen virtuellen Switch konfiguriert ist, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie das statische VLAN durch Eingabe von:

   ```
   no switch vlans static-vlan id
   ```

   Erläuterung:

   - *id* ist die ID des VLAN
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 8.5.6
Verbotene Ports verwalten

Mit der Liste der verbotenen Ports kann ein statisches VLAN so konfiguriert werden, dass bestimmte Ports aus dem VLAN ausgeschlossen werden.

INHALT

- Abschnitt 8.5.6.1, „Eine Liste der verbotenen Ports“
- Abschnitt 8.5.6.2, „Einen verbotenen Port hinzufügen“
- Abschnitt 8.5.6.3, „Einen verbotenen Port löschen“

Abschnitt 8.5.6.1
Eine Liste der verbotenen Ports

Um eine Liste der verbotenen Ports anzuzeigen, geben Sie Folgendes ein:

```
show running-config switch vlans static-vlan forbidden-ports
```

Falls Ports verboten wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config switch vlans static-vlan forbidden-ports | tab
VID  SLOT    PORT
-------------------
50
     swport  1
     swport  2
60
     swport  2
     swport  3
     swport  4
70
     swport  5

!
```

Falls keine Ports verboten wurden, fügen Sie je nach Bedarf verbotene Ports hinzu. Weitere Informationen finden Sie unter Abschnitt 8.5.6.2, „Einen verbotenen Port hinzufügen“.

Abschnitt 8.5.6.2
Einen verbotenen Port hinzufügen

Um einen verbotenen Port hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den verbotenen Port hinzu, indem Sie Folgendes eingeben:

   ```
   switch vlans static-vlan name forbidden-ports swport port
   ```

   Erläuterung:

   - *name* ist die Bezeichnung des statischen VLAN
   - *port* ist die Nummer des Ports (oder eine Liste von Ports, wenn sie in einem Port-Trunk gebündelt sind) für das Modul.
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 8.5.6.3
Einen verbotenen Port löschen

Um einen verbotenen Port zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***switch » vlans » static-vlan » {name} » forbidden-ports***, wobei *{name}* die Bezeichnung des statischen VLAN ist.
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

   ```
   no switch vlans static-vlan name forbidden-ports swport port
   ```

   Erläuterung:

   - *name* ist die Bezeichnung des statischen VLAN
   - *port* ist die Nummer des Ports (oder eine Liste von Ports, wenn sie in einem Port-Trunk gebündelt sind) für das Modul.
4. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 8.5.7
VLANs für Schnittstellen und Tunnel verwalten

Dieser Abschnitt beschreibt, wie Sie Tunnel für bestimmte Schnittstellen und Tunnel ansehen, hinzufügen und löschen können.

- Abschnitt 11.1.8, „VLANs für virtuelle Switches verwalten“
- Abschnitt 11.4.6, „VLANs für L2TPv3-Tunnel verwalten“

Abschnitt 8.6

Spanning Tree Protocol (STP) verwalten

Dieser Abschnitt beschreibt, wie Sie das Spanning Tree Protocol (STP) verwalten können.

INHALT

- Abschnitt 8.6.1, „RSTP-Betrieb“
- Abschnitt 8.6.2, „RSTP-Anwendungen“
- Abschnitt 8.6.3, „MSTP-Betrieb“
- Abschnitt 8.6.4, „Konfigurieren des STP (global)“
- Abschnitt 8.6.5, „Konfigurieren des STP für Switched-Ethernet-Ports und Ethernet-Trunk-Schnittstellen“
- Abschnitt 8.6.6, „MST-Instanzen global verwalten“
- Abschnitt 8.6.7, „MST-Instanzen nach Ports verwalten“
- Abschnitt 8.6.8, „Anzeigen des Status eines RSTP“
- Abschnitt 8.6.9, „RSTP-Statistiken je Port anzeigen“
- Abschnitt 8.6.10, „Statistiken für STP (Spanning Tree Protocol) löschen“

Abschnitt 8.6.1

RSTP-Betrieb

Das Spanning Tree Protocol (STP) IEEE 802.1D wurde entwickelt, um den Aufbau robuster Netzwerke mit Redundanz zu ermöglichen, während gleichzeitig die aktive Topologie des Netzwerks beschnitten wird, um Schleifen zu verhindern. Wenn STP aktiv ist, muss die Frame-Übertragung nach einem Verbindungsausfall anhalten, bis alle Bridges im Netzwerk sicher die neue Topologie erkannt haben. Werden die von IEEE 802.1D empfohlenen Werte verwendet, dauert dieser Vorgang 30 Sekunden.

Das Rapid Spanning Tree Protocol (RSTP), das erstmals mit IEEE 802.1w eingeführt und in IEEE 802.12D-2004 deutlich verbessert wurde, war eine Weiterentwicklung des Spanning Tree Protocol nach dem Standard IEEE 802.1D. Es ersetzte die Anpassungszeit durch einen aktiven Handshake zwischen Bridges, der die schnelle Übermittlung der Topologie-Informationen im Netzwerk gewährleistet.

INHALT

- Abschnitt 8.6.1.1, „RSTP-Zustände und -Funktionen“
- Abschnitt 8.6.1.2, „Edge-Ports“
- Abschnitt 8.6.1.3, „Punkt-zu-Punkt- und Mehrfachpunktverbindung“
- Abschnitt 8.6.1.4, „Pfad- und Portkosten“
- Abschnitt 8.6.1.5, „Bridge-Durchmesser“
- Abschnitt 8.6.1.6, „eRSTP“
- Abschnitt 8.6.1.7, „Fast Root Failover“

Abschnitt 8.6.1.1

RSTP-Zustände und -Funktionen

RSTP-Bridges erfüllen Funktionen, entweder als Root- oder als Designated-Bridge. Eine Bridge – die Root-Bridge – ist das logische Zentrum des Netzwerks. Alle anderen Bridges im Netzwerk werden als Designated-Bridges bezeichnet. RSTP weist jedem Port der Bridge einen Zustand und eine Funktion zu. Der RSTP-Zustand beschreibt, was am Port in Bezug auf Adressenlernen und Frame-Weiterleitung passiert. Die RSTP-Funktion beschreibt, ob der Port auf das Zentrum oder die Ränder des Netzwerks ausgerichtet ist und ob er aktuell verwendet werden kann.

Zustand

Es gibt drei RSTP-Zustände: "Discarding" (Verwerfen), "Learning" (Lernen) und "Forwarding" (Weiterleiten).

Der "Discarding"-Zustand ist gegeben, wenn der Port erstmalig in Betrieb genommen wird. Der Port lernt in diesem Zustand keine Adressen und ist nicht an der Frame-Übertragung beteiligt. Der Port sucht nach RSTP-Datenverkehr, um seine Funktion im Netzwerk festzulegen. Wenn feststeht, dass der Port eine aktive Funktion im Netzwerk einnimmt, wird der Zustand in Lernen geändert.

Der "Learning"-Zustand ist gegeben, wenn der Port sich darauf vorbereitet, ein aktiver Teil im Netzwerk zu werden. Der Port lernt in diesem Zustand Adressen, ist jedoch nicht an der Frame-Übertragung beteiligt. In einem RSTP-Bridge-Netzwerk fällt die in diesem Zustand verbrachte Zeit üblicherweise sehr kurz aus. RSTP-Bridges im STP-Kompatibilitätsmodus bleiben sechs bis 40 Sekunden in diesem Zustand.

Nach dem *Lernen* versetzt die Bridge den Port in den "Forwarding"-Zustand. In diesem Zustand lernt der Port Adressen und beteiligt sich an der Frame-Übertragung.

WICHTIG!
Der RUGGEDCOM ROX II besitzt zu reinen Verwaltungszwecken zwei weitere Zustände: ***Disabled*** *und* ***Link Down****. Der Zustand* ***Disabled*** *bezieht sich auf Verbindungen, für die RSTP deaktiviert wurde. Der Zustand* ***Link Down*** *bezieht sich auf Verbindungen, für die RSTP aktiviert ist, die jedoch aktuell nicht verfügbar sind.*

Funktion

Vier RSTP-Port-Optionen stehen zur Auswahl: Root, Designated, Alternate und Backup. Wenn die Bridge nicht die Root-Bridge ist, muss sie einen einzelnen Root-Port haben. Der Root-Port ist die "beste" (d.h. schnellste) Möglichkeit, den Datenverkehr an die Root-Bridge zu senden.

Ein Port wird als "Designated" gekennzeichnet, wenn es sich um den besten Port handelt, um dem mit ihm verbundenen LAN-Segment zu dienen. Alle Bridges im selben LAN-Segment hören die Nachrichten der jeweils anderen Bridges und werden sich darüber einig, welche die Designated-Bridge wird. Die Ports anderer Bridges im Segment müssen entweder Root-, Alternate- oder Backup-Ports werden.

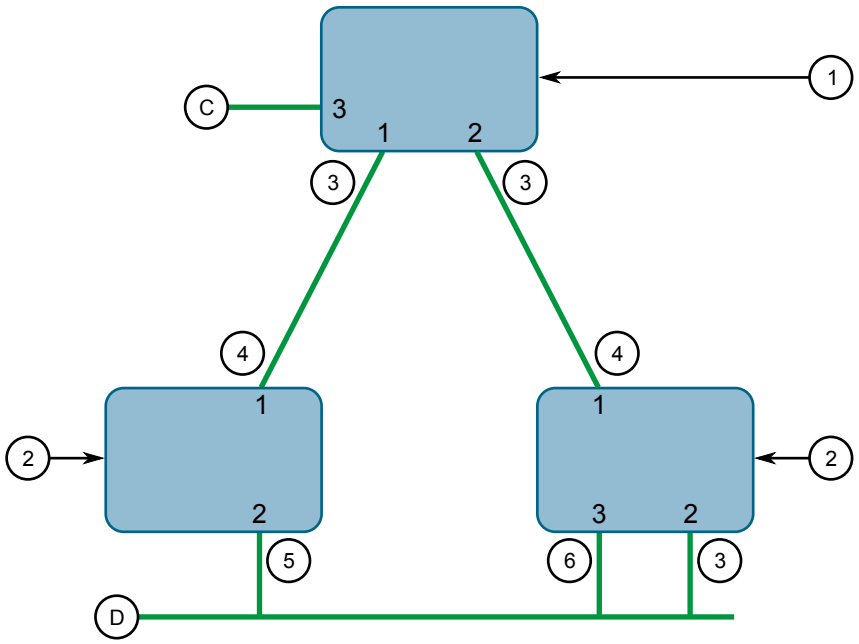


Abbildung 11: Bridge- und Port-Funktionen

1. Root-Bridge **2.** Designated-Bridge **3.** Designated-Port **4.** Root-Port **5.** Alternate-Port **6.** Backup-Port

Ein Port ist ein Alternate-Port, wenn er eine bessere Nachricht von einer anderen Bridge in dem LAN-Segment empfängt, mit dem er verbunden ist. Die Nachricht, die der Alternate-Port empfängt, ist besser als die Nachricht, die der Port selbst generieren würde, jedoch ist sie nicht gut genug, um diesen zu überzeugen, der Root-Port zu werden. Der Port wird zum alternativen Port (Alternate-Port) des aktuellen Root-Ports und wird zum neuen Root-Port, falls der aktuelle Root-Port ausfällt. Der Alternate-Port ist nicht am Netzwerk beteiligt.

Ein Port ist ein Backup-Port, wenn er von dem verbundenen LAN-Segment eine bessere Nachricht empfängt, die von einem anderen Port an derselben Bridge stammt. Der Port dient als Backup für einen anderen Port an der Bridge und wird aktiv, falls dieser Port ausfällt. Der Backup-Port ist nicht am Netzwerk beteiligt.

Abschnitt 8.6.1.2

Edge-Ports

Ein Port kann als Edge-Port bezeichnet werden, wenn er direkt mit einer Endstation verbunden ist. Er kann dann keine Bridging-Schleifen im Netzwerk anlegen und somit direkt zur Weiterleitung übergehen, ohne die Hör- und Lernstufen zu durchlaufen.

Edge-Ports, die Konfigurationsmeldungen empfangen, verlieren sofort Ihren Status als Edge-Port und werden zu normalen Spanning-Tree-Ports. Eine Schleife, die an einem fehlerhaft verschalteten Edge-Port entstanden ist, kann dadurch schnell repariert werden.

Da ein Edge-Port nur Endstationen bedient, werden beim Umschalten seiner Links keine Meldungen über Topologieänderungen generiert.

Abschnitt 8.6.1.3
Punkt-zu-Punkt- und Mehrfachpunktverbindung

RSTP verwendet ein Peer-Peer-Protokoll, das Proposing-Agreeing bezeichnet wird. Dieses soll den Übergang im Falle eines Verbindungsfehlers sicherstellen. Hierbei handelt es sich um ein Punkt-zu-Punkt-Protokoll, das in Mehrfachpunktsituationen abbricht, d. h. wenn mehr als zwei Bridges auf einer gemeinsamen Medienverbindung arbeiten.

Erkennt RSTP diesen Umstand (anhand des Halbduplex-Zustands des Ports nach dem Verbinden), schaltet es das Proposing-Agreeing aus. Der Port muss den Übergang durch die Lern- und Weiterleitungszustände durchlaufen und in jedem Zustand ein Forward-Delay verbringen.

Es gibt Umstände, unter denen RSTP eine falsche Entscheidung über den Punkt-zu-Punkt-Zustand der Verbindung trifft, indem es nur den Halbduplex-Zustand prüft. Diese Umstände sind:

- Der Port ist nur an einen einzelnen Partner angeschlossen, jedoch über eine Halbduplex-Verbindung.
- Der Port ist über eine Vollduplex-Verbindung an einen gemeinsamen Medien-Hub angeschlossen. Die gemeinsame Medienverbindung ist an mehr als eine RSTP-fähige Bridge angeschlossen.

In diesen Fällen kann der Benutzer die Bridge so konfigurieren, dass sie den Halbduplex-Bestimmungsmechanismus außer Kraft setzt und die Verbindung korrekt behandelt wird.

Abschnitt 8.6.1.4
Pfad- und Portkosten

Die STP-Pfadkosten sind die Hauptmetrik, anhand der Root- und Designated-Ports ausgewählt werden. Die Pfadkosten für eine Designated-Bridge ist die Summe der einzelnen Portkosten der Verbindungen zwischen der Root-Bridge und dieser Designated-Bridge. Der Port mit den niedrigsten Pfadkosten ist die beste Route zur Root-Bridge und wird daher als Root-Port gewählt.

HINWEIS
Faktisch ist die primäre Bestimmungsgröße für die Root-Port-Auswahl die Root-Bridge-ID. Die Bridge-ID spielt insbesondere beim Netzwerk-Startup eine wichtige Rolle, wenn die Bridge mit der kleinsten ID als Root-Bridge gewählt wird. Nach dem Startup (d.h. wenn alle Bridges der Root-Bridge-ID zugestimmt haben) werden die Pfadkosten zur Auswahl der Root-Ports herangezogen. Wenn die Pfadkosten der Kandidaten für den Root-Port identisch sind, dann wird die ID der Peer-Bridge für die Portauswahl genutzt. Wenn die Kandidaten für den Root-Port schließlich dieselben Pfadkosten und dieselbe Peer-Bridge-ID haben, dann wird die Port-ID der Peer-Bridge zur Auswahl des Root-Ports verwendet. In allen Fällen wird die kleinste ID, die niedrigsten Pfadkosten bzw. die kleinste Port-ID als beste Lösung ausgewählt.

» Generierung von Portkosten

Portkosten können entweder als Ergebnis einer Verbindungs-Autonegotiation oder einer manuellen Konfiguration generiert werden. Wenn das Verbindungs-Autonegotiations-Verfahren verwendet wird, dann werden die Portkosten aus der Geschwindigkeit der Verbindung abgeleitet. Dieses Verfahren ist dann von Vorteil, wenn ein gut vernetztes Netzwerk aufgebaut wurde. Das Verfahren kann angewandt werden, wenn der Netzwerkentwickler keine allzu großen Probleme in der resultierenden Topologie sieht, solange die Konnektivität sichergestellt ist.

Eine manuelle Konfiguration ist dann von Vorteil, wenn die genaue Topologie des Netzwerks unter allen Umständen vorhersehbar sein muss. Die Pfadkosten können beim Aufbau der Topologie des Netzwerks exakt nach den Vorstellungen des Netzwerkentwicklers herangezogen werden.

» STP- vs. RSTP-Kosten

Die STP-Spezifikation begrenzt die Portkosten auf Werte zwischen 1 und 65536. Das Verfahren, das zu einem Zeitpunkt entwickelt wurde, als 9600 Bit/s dem aktuellen Stand der Technik entsprachen, kann in der heutigen modernen Zeit nicht mithalten, da es für Verbindungsraten über 10 Gbit/s nicht geeignet ist.

Um dieses Problem in künftigen Anwendungen abzustellen, begrenzt die RSTP-Spezifikation die Portkosten auf Werte zwischen 1 und 20000000; und eine Verbindungsrate bis zu 10 Tbit/s kann mit dem Wert 2 dargestellt werden.

Abschnitt 8.6.1.5

Bridge-Durchmesser

Der Bridge-Durchmesser ist die Höchstanzahl an Bridges zwischen zwei möglichen Anschlusspunkten von Endstellen am Netzwerk.

Der Bridge-Durchmesser spiegelt die Tatsache wider, dass Topologieinformationen Zeit benötigen, um Hop für Hop durch ein Netzwerk zu propagieren. Wenn Konfigurationsnachrichten zu lange brauchen, um sich von Ende zu Ende durch das Netzwerk zu verbreiten, führt dies zu einem instabilen Netzwerk.

Zwischen dem Bridge-Durchmesser und dem Höchstalter-Parameter besteht ein Zusammenhang.

HINWEIS
Die RSTP-Algorithmus ist wie folgt:

- *STP-Konfigurationsnachrichten enthalten Daten zum **Alter**.*
- *Die von der Root Bridge übertragenen Nachrichten haben ein Alter von 0. Da jede anschließend vorgesehene Brücke die Konfigurationsnachricht sendet, muss sie das Alter um mindestens 1 Sekunde erhöhen.*
- *Wenn das Alter den Wert des Höchstalter-Parameters überschreitet, verwirft die nächste empfangende Brücke die Nachricht sofort.*

Um die Ringgrößen zu erweitern, setzt das eRSTP™ von Siemens eine Alterssteigerung von einer Viertelsekunde ein. Damit beträgt der Wert des maximalen Bridge-Durchmessers das Vierfache des konfigurierten Höchstalter-Parameters.

WICHTIG!
Erhöhen Sie den Wert des Höchstalter-Parameters, sofern Sie sehr große überbrückte Netzwerke oder Ringe implementieren.

Abschnitt 8.6.1.6

eRSTP

Das erweiterte Rapid Spanning Tree Protocol (eRSTP) von Siemens verbessert die Leistung von RSTP auf zwei Arten:

- Verbesserung der Wiederherstellungszeit nach einem Fehler (< 5 ms per Hop)
- Verbesserung der Leistung für große Ringnetzwerk-Topologien (bis zu 160 Switches)

eRSTP ist auch mit Standard-RSTP kompatible für die Interoperabilität mit kommerziellen Switches.

In einem Netzwerk mit 15 RUGGEDCOM-fähigen Ethernet-Switches in einer Ringtopologie würde man eine Wiederherstellungszeit nach einem Fehler von unter 75 ms erwarten (d. h. 5 ms x 15). Mit eRSTP ist jedoch die schlechteste Wiederherstellungszeit kürzer als 26 ms.

Abschnitt 8.6.1.7
Fast Root Failover

Die *Fast Root Failover*-Funktion des Siemens ist eine Erweiterung des RSTP, die aktiviert bzw. deaktiviert werden kann. Das Fast Root Failover verbessert die Handhabung des RSTP von Root-Bridge-Ausfällen in Mesh-Netzwerken, was leicht verbesserte Failover-Zeiten in bestimmten Nicht-Root-Bridge-Szenarien zur Folge hat.

WICHTIG!
Bei Netzwerken, in denen RUGGEDCOM- und Nicht-RUGGEDCOM-Switches vermischt werden, oder bei Netzwerken, in denen Fast Root Failover-Algorithmen vermischt werden, funktioniert RSTP Fast Root Failover nicht ordnungsgemäß und der Ausfall der Root-Bridge führt zu einer nicht vorhersehbaren Failover-Zeit. Zur Vermeidung eventueller Probleme beachten Sie Folgendes:

- *Bei Verwendung des Robust-Algorithmus müssen alle Switches RUGGEDCOM-Switches sein*
- *Bei Verwendung des Relaxed-Algorithmus müssen alle Switches RUGGEDCOM-Switches sein, mit Ausnahme des Root-Switch*
- *Alle RUGGEDCOM-Switches im Netzwerk müssen denselben Fast Root Failover-Algorithmus verwenden.*

Es sind zwei Fast Root Failover-Algorithmen verfügbar:

- **Robust** – Garantiert eine deterministische Root Failover-Zeit, setzt jedoch die Unterstützung aller Switches im Netzwerk, einschließlich des Root-Switch, voraus.
- **Relaxed** – Gewährleistet eine deterministische Root Failover-Zeit in den meisten Netzwerkkonfigurationen, erlaubt jedoch die Verwendung einer Standard-Bridge in der Funktion einer Root-Bridge.

HINWEIS
Das Mindestintervall für Root-Ausfälle beträgt eine Sekunde. Mehrere, nahezu gleichzeitige Root-Ausfälle (innerhalb einer Sekunde nacheinander) werden von der Fast Root Failover-Funktion nicht unterstützt.

» Fast Root Failover und RSTP-Performanz

- RSTP mit deaktiviertem Fast Root Failover wirkt sich nicht auf die RSTP-Performanz aus.
- Fast Root Failover hat keine Auswirkungen auf die RSTP-Performanz bei Ausfällen, bei denen die Root-Bridge oder eine ihrer Verbindungen nicht betroffen sind.
- Die durch das Fast Root Failover bedingte zusätzliche Verarbeitung senkt die Failover-Zeit in Mesh-Netzwerken im schlimmsten Fall erheblich, mit mäßiger Verbesserung der Failover-Zeit im besten Fall. Die Auswirkung auf die Failover-Zeit in Ring-Netzwerken ist jedoch ausschließlich eine Verbesserung.

» Empfohlene Verwendung der Fast Root Failover-Funktion

- Die Aktivierung der Fast Root Failover-Funktion in Einzelring-Netzwerktopologien wird nicht empfohlen.
- Es wird dringend empfohlen, die Root-Bridge immer mit einer ihrer benachbarten Bridges mit mehr als einer Verbindung zu verbinden.

Abschnitt 8.6.2

RSTP-Anwendungen

Dieser Abschnitt beschreibt verschiedene Anwendungen von RSTP.

INHALT

- Abschnitt 8.6.2.1, „RSTP in Konfigurationen mit strukturierter Verdrahtung“
- Abschnitt 8.6.2.2, „RSTP in Ring-Backbone-Konfigurationen“
- Abschnitt 8.6.2.3, „RSTP-Port-Redundanz“

Abschnitt 8.6.2.1

RSTP in Konfigurationen mit strukturierter Verdrahtung

RSTP kann zum Aufbauen von Systemen mit strukturierter Verdrahtung verwendet werden, bei denen die Konnektivität bei einem Verbindungsausfall aufrecht erhalten wird. Ein einzelner Verbindungsausfall einer beliebigen Verbindung zwischen A und N in Abbildung 12 führt beispielsweise dazu, dass alle Ports der Bridges 555 bis 888 mit dem Netzwerk verbunden bleiben.

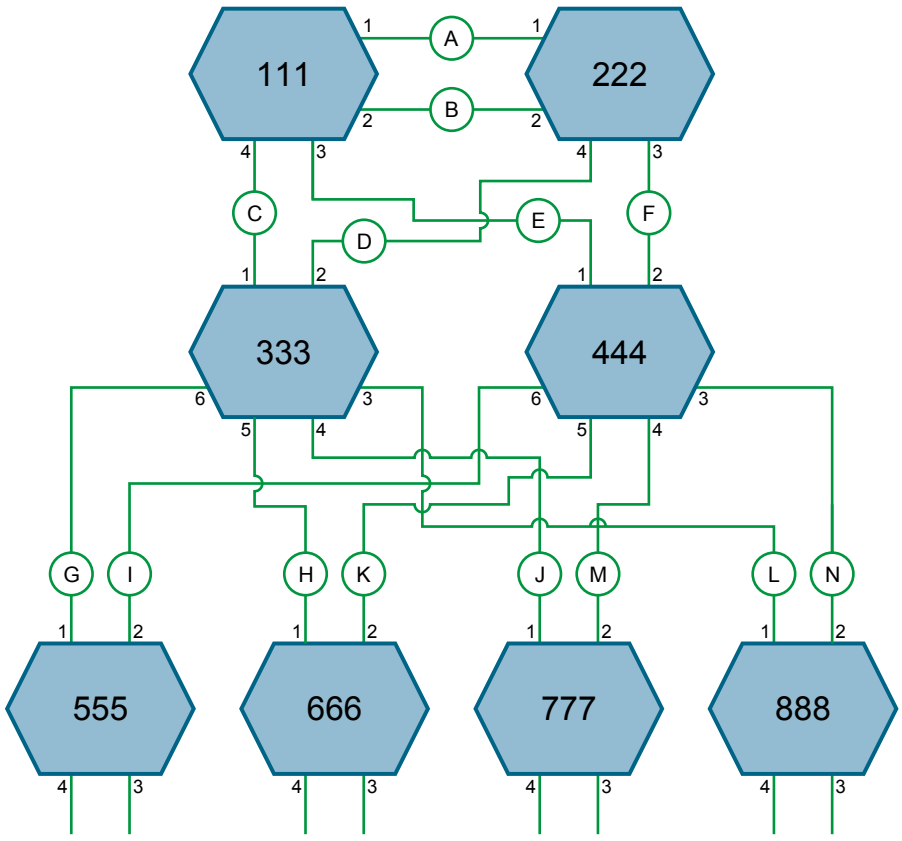


Abbildung 12: Beispiel - Strukturierte Verkabelung

Um eine strukturierte Verkabelung aufzubauen, gehen Sie wie folgt vor:

1. **Wählen Sie die Designparameter für das Netzwerk.**

   Welche Anforderungen gelten für Robustheit und Netzwerk-Failover/Wiederherstellungszeiten? Gibt es spezielle Anforderungen für das Diverse Routing zu einem zentralen Hostcomputer? Gibt es spezielle Anforderungen im Hinblick auf die Portredundanz?

2. **Identifizieren Sie eine erforderliche Legacy-Unterstützung.**

   Werden STP-Bridges im Netzwerk verwendet? Diese Bridges unterstützen den schnellen Übergang in den Forwarding-Zustand nicht. Wenn diese Bridges vorhanden sind, können sie näher am Netzwerkrand eingesetzt werden?

3. **Identifizieren Sie Edge-Ports und Ports mit Einschränkungen hinsichtlich Halbduplex und gemeinsamen Medien.**

   Ports, die sich mit Hostcomputern, IEDs und Controllern verbinden, können auf Edge-Ports gesetzt werden, um einen schnellen Übergang in den Forwarding-Zustand zu gewährleisten und um die Anzahl der Topologieänderungs-Benachrichtigungen im Netzwerk zu reduzieren. Ports mit Einschränkungen hinsichtlich Halbduplex und gemeinsamen Medien erfordern besondere Aufmerksamkeit, um sicherzustellen, dass diese keine übermäßigen Failover-/Wiederherstellungszeiten verursachen.

4. **Wählen Sie die Root-Bridge und die Backup-Root-Bridge sorgfältig aus.**

   Die Root-Bridge sollte so ausgewählt werden, dass sie sich am Konzentrationspunkt des Netzwerkverkehrs befindet. Positionieren Sie die Backup-Root-Bridge neben der Root-Bridge. Eine anwendbare Strategie ist die Abstimmung der Bridge-Priorität für den Aufbau der Root-Bridge und die anschließende Abstimmung der Priorität jeder Bridge, damit sie ihrer Entfernung von der Root-Bridge entspricht.

5. **Identifizieren Sie die gewünschte Steady-State-Topologie.**

   Identifizieren Sie die gewünschte Steady-State-Topologie und berücksichtigen Sie dabei die Verbindungsgeschwindigkeiten, den gebotenen Verkehr und die QoS. Überprüfen Sie die Auswirkungen auf einen Bruch ausgewählter Verbindungen und berücksichtigen Sie dabei die Netzwerklast und die Qualität alternativer Verbindungen.

6. **Entscheiden Sie sich für eine Strategie für die Berechnung der Portkosten.**

   Wählen Sie, ob feste oder automatisch verhandelte Kosten verwendet werden sollen. Es wird empfohlen, den automatisch verhandelten Kostenstil zu verwenden, sofern eine Änderung des automatisch verhandelten Kostenstils für den Netzwerkaufbau nicht erforderlich ist. Wählen Sie, ob der STP- oder RSTP-Kostenstil verwendet werden soll. Stellen Sie sicher, dass Sie denselben Kostenstil an allen Geräten im Netzwerk konfigurieren.

7. **Aktivieren Sie die Option RSTP Fast Root Failover.**

   Hierbei handelt es sich um eine eigene Funktion des Siemens. Bei einem Mesh-Netzwerk mit ausschließlich RUGGEDCOM-Geräten im Kern des Netzwerks wird die Aktivierung der Option RSTP Fast Root Failover empfohlen, um bei Ausfall der Root-Bridge die Netzwerkausfallzeit zu minimieren.

8. Kalkulieren und konfigurieren Sie Prioritäten und Kosten.
9. Implementieren Sie das Netzwerk und führen Sie einen Test unter Last aus.

Abschnitt 8.6.2.2
RSTP in Ring-Backbone-Konfigurationen

RSTP kann in Ring-Backbone-Konfigurationen verwendet werden, wo eine schnelle Wiederherstellung nach Verbindungsausfällen erforderlich ist. Im Normalbetrieb blockiert RSTP den Verkehr an einer der Verbindungen. Ein Beispiel finden Sie unter Verbindung H in Abbildung 13. Bei einem Ausfall an Verbindung D hebt Bridge 444 die Sperrung von Verbindung H auf und die Bridge 333 kommuniziert mit dem Netzwerk über Verbindung F.

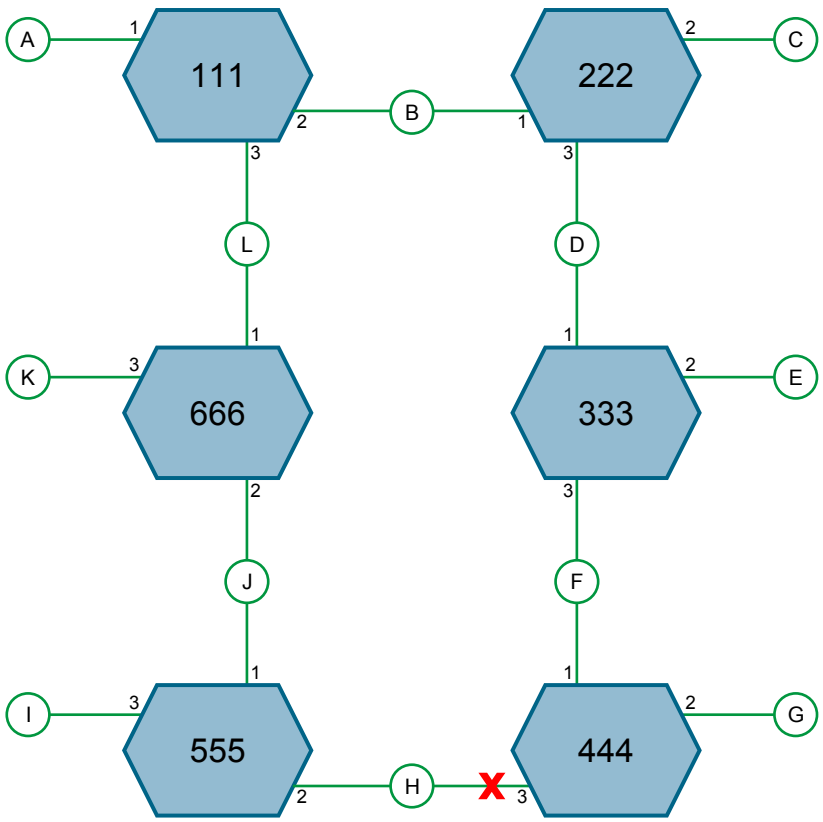


Abbildung 13: Beispiel - Ring-Backbone-Konfiguration

Um eine Ring-Backbone-Konfiguration mit RSTP aufzubauen, gehen Sie wie folgt vor:

1. **Wählen Sie die Designparameter für das Netzwerk.**

   Welche Anforderungen gelten für Robustheit und Netzwerk-Failover/Wiederherstellungszeiten? Ring-Backbones werden üblicherweise gewählt, wenn kosteneffektive und zugleich robuste Netzwerkaufbauten erforderlich sind.

2. **Identifizieren Sie erforderliche Legacy-Unterstützung und Ports mit Einschränkungen hinsichtlich Halbduplex und gemeinsamen Medien.**

   Diese Bridges dürfen nicht verwendet werden, wenn die Netzwerk-Failover/Wiederherstellungszeiten minimiert werden sollen.

3. **Identifizieren Sie Edge-Ports.**

   Ports, die sich mit Hostcomputern, IEDs und Controllern verbinden, können auf Edge-Ports gesetzt werden, um einen schnellen Übergang in den Forwarding-Zustand zu gewährleisten und um die Anzahl der Topologieänderungs-Benachrichtigungen im Netzwerk zu reduzieren.

4. **Wählen Sie die Root-Bridge.**

   Die Root-Bridge kann zum Gleichsetzen der Anzahl an Bridges, der Anzahl an Stationen oder der Datenverkehrsmenge an jedem ihrer Enden gewählt werden. Es gilt zu berücksichtigen, dass der Ring an einer Stelle immer unterbrochen ist und dass der Verkehr immer durch die Root fließt.

5. **Weisen Sie dem Ring Bridge-Prioritäten zu.**

   Weitere Informationen finden Sie im RUGGEDCOM White Paper *Performance of the RSTP in Ring Network Topologies* unter https://www.siemens.com/ruggedcom.

6. **Entscheiden Sie sich für eine Strategie für die Berechnung der Portkosten.**

   Es wird empfohlen, den automatisch verhandelten Kostenstil zu verwenden, sofern eine Änderung des automatisch verhandelten Kostenstils für den Netzwerkaufbau nicht erforderlich ist. Wählen Sie, ob der STP- oder RSTP-Kostenstil verwendet werden soll. Stellen Sie sicher, dass Sie denselben Kostenstil an allen Geräten im Netzwerk konfigurieren.

7. **Deaktivieren Sie die Option RSTP Fast Root Failover.**

   Hierbei handelt es sich um eine eigene Funktion des Siemens. Im RUGGEDCOM ROX II ist die Funktion RSTP Fast Root Failover standardmäßig aktiviert. Für den Betrieb in einem Ringnetzwerk wird die Deaktivierung dieser Funktion empfohlen.

8. Implementieren Sie das Netzwerk und führen Sie einen Test unter Last aus.

Abschnitt 8.6.2.3
RSTP-Port-Redundanz

Wenn die Port-Redundanz von wesentlicher Bedeutung ist, kann mit RSTP mehr als ein Bridge-Port ein LAN bedienen. Im folgenden Beispiel ist Port 3 ausgewählt, um den Netzwerkverkehr von LAN A weiterzuleiten, Port 4 blockiert den Verkehr. Tritt an Port 3 ein Schnittstellenfehler auf, übernimmt Port 4 die Steuerung des LAN.

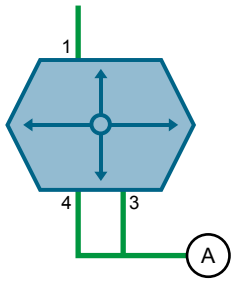


Abbildung 14: Beispiel - Port-Redundanz

Abschnitt 8.6.3
MSTP-Betrieb

Der Multiple Spanning Tree (MST)-Algorithmus und das entsprechende Protokoll bieten eine größere Kontrollmöglichkeit und Flexibilität als RSTP und das veraltete STP. Das MSTP (Multiple Spanning Tree-Protokoll) ist eine Erweiterung des RSTP, bei dem mehrere Spannbäume im selben überbrückten Netzwerk erhalten werden. Der Datenverkehr wird einem oder mehreren Spannbäumen zugeordnet, indem ein oder mehrere VLANs in verschiedenen Multiple Spanning Tree-Instanzen (MSTIs) abgebildet werden.

Die Ausgereiftheit und der Nutzen der MSTP-Implementierung in einem gegebenen überbrückten Netzwerk verhält sich proportional zum Aufwand, der hinsichtlich Planung und Aufbau in die MSTP-Konfigurierung zu investieren ist.

Wenn MSTP an bestimmten oder allen Bridges in einem Netzwerk ohne zusätzliche Konfiguration aktiviert ist, ist das Resultat ein vollständiges und einfach verschaltetes Netzwerk. Im besten Fall ist das Resultat im Hinblick auf ein Netzwerk, für das ausschließlich RSTP genutzt wird, identisch. Um die von MSTP gebotenen Funktionen voll auszuschöpfen, ist eine potenziell große Anzahl an Konfigurationsvariablen erforderlich, die aus einer Analyse des Datenverkehrs im überbrückten Netzwerk und aus den Anforderungen bezüglich Lastteilung, Redundanz und Pfadoptimierung abzuleiten sind. Nach der Ableitung dieser Parameter ist es wichtig, diese über alle Bridges in einer MST-Region konsistent anzuwenden und zu verwalten.

Die MSTP-Verarbeitungszeit verhält sich proportional zur Anzahl der aktiven STP-Instanzen. Das bedeutet, dass das MSTP wahrscheinlich erheblich langsamer als das RSTP ist. Bei aufgabenkritischen Anwendungen sollte daher das RSTP anstelle von MSTP als bessere Netzwerkredundanz-Lösung in Erwägung gezogen werden.

INHALT

- Abschnitt 8.6.3.1, „MSTP-Regionen und -Interoperabilität“
- Abschnitt 8.6.3.2, „MSTP-Bridge- und -Port-Funktionen“
- Abschnitt 8.6.3.3, „Vorteile von MSTP“
- Abschnitt 8.6.3.4, „MSTP an einem überbrückten Netzwerk implementieren“

Abschnitt 8.6.3.1

MSTP-Regionen und -Interoperabilität

Neben der Unterstützung von Multiple Spanning Trees in einem Netzwerk mit MSTP-fähigen Bridges kann MSTP mit Bridges interagieren, die nur RSTP oder das veraltete STP unterstützen, ohne dass eine spezielle Konfiguration notwendig ist.

Eine MST-Region kann als eine Gruppe miteinander verbundener Bridges definiert werden, deren MST-Regionskennung identisch ist. Die Schnittstelle zwischen MSTP-Bridges und Nicht-MSTP-Bridges oder zwischen MSTP-Bridges mit unterschiedlicher MST-Regionskennung werden Teil einer Grenze der MST-Region.

Bridges außerhalb einer MST-Region sehen die gesamte Region als eine einzelne (R)STP-Bridge, mit der internen Information, dass die MST-Region dem restlichen überbrückten Netzwerk verborgen bleibt. Als Unterstützung dafür besitzt MSTP separate *Hop Counter* für Spanning-Tree-Informationen, die an der Grenze der MST-Region ausgetauscht werden bzw. Informationen, die innerhalb der Region verbreitet werden. Bei an der Grenze der MST-Region empfangenen Informationen wird der Parameter (R)STP Message Age nur einmalig erhöht. Innerhalb der Region wird ein separater Remaining Hop Count gepflegt, jeweils einer für jede Spanning-Tree-Instanz. Der externe Parameter Message Age wird als (R)STP Maximum Age Time bezeichnet, wobei die internen Remaining Hop Counts mit einem MST-Region-weiten Maximum-Hops-Parameter verglichen werden.

» MSTI

Eine MSTI (Multiple-Spanning-Tree-Instanz) ist eine von sechszehn unabhängigen Spanning-Tree-Instanzen, die in einer MST-Region (nicht einschließlich IST) definiert werden kann. Eine MSTI entsteht durch Abbilden einer Gruppe von VLANs auf einer gegebenen MSTI-ID. Dieselbe Abbildung muss an allen Bridges konfiguriert werden, die Teil der MSTI sein sollen. Außerdem müssen alle VLAN-auf-MSTI-Abbildungen für alle Bridges in einer MST-Region identisch sein.

Der RUGGEDCOM ROX II unterstützt 16 MSTIs zusätzlich zum IST.

Jede MSTI hat eine Topologie, die von anderen unabhängig ist. Datenverkehr, der von derselben Quelle stammt und an dasselbe Ziel gerichtet ist, jedoch in verschiedenen VLANs in verschiedenen MSTIs, kann demzufolge einen anderen Pfad durch das Netzwerk nehmen.

» IST

Eine MST-Region definiert immer einen IST (Internal Spanning Tree). Der IST überspannt die gesamte MST-Region und trägt den gesamten Datenverkehr, der nicht einer bestimmten MSTI (vom VLAN) spezifisch zugewiesen ist. Der IST wird immer berechnet und als MSTI Null festgelegt.

Der IST ist außerdem die Erweiterung innerhalb der MST-Region des CIST.

» CST

Der CST (Common Spanning Tree) überspannt das gesamte überbrückte Netzwerk, einschließlich der MST-Regionen und aller angebundenen STP- oder RSTP-Bridges. Eine MST-Region wird vom CST als eine individuelle Bridge betrachtet, mit dem Traversal zugeordneten Einzelkosten.

» CIST

Der CIST (Common and Internal Spanning Tree) ist die Gemeinschaft aus CST und den ISTs in allen MST-Regionen. Der CIST überspannt demnach das gesamte überbrückte Netzwerk und reicht über den IST in jede MST-Region, um jede Bridge im Netzwerk zu erreichen.

Abschnitt 8.6.3.2

MSTP-Bridge- und -Port-Funktionen

MSTP unterstützt die folgenden Bridge- und Port-Funktionen:

» Bridge-Funktionen

Funktion	Beschreibung
CIST-Root	Die CIST-Root ist die gewählte Root-Bridge des CIST (Common and Internal Spanning Tree), die alle verbundenen STP- und RSTP-Bridges sowie MSTP-Regionen umspannt.
CIST-Regional-Root	Die Root-Bridge von IST innerhalb einer MSTP-Region. Die CIST-Regional-Root ist die Bridge innerhalb einer MSTP-Region mit dem Pfad der geringsten Kosten zur CIST-Root. Beachten Sie, dass die CIST-Regional-Root sich an der Grenze einer MSTP-Region befindet. Beachten Sie auch, dass die CIST-Regional-Root eine CIST-Root sein kann.
MSTI-Regional-Root	Die Root-Bridge für eine MSTI innerhalb einer MSTP-Region. Eine Root-Bridge wird für jede MSTI in einer MSTP-Region unabhängig gewählt.

» Port-Funktionen

Jeder Port an einer MSTP-Bridge kann mehr als eine CIST-Funktion haben, was von der Anzahl und der Topologie der am Port definierten Spanning-Tree-Instanzen abhängt.

Funktion	Beschreibung
CIST-Port-Funktionen	• Der Root-Port stellt den Mindestkostenpfad von der Bridge zur CIST-Root über die CIST-Regional-Root bereit. Wenn die Bridge selbst die CIST-Regional-Root ist, dann ist der Root-Port auch der Master-Port für alle MSTIs und stellt den Mindestkostenpfad zu einer CIST-Root außerhalb der Region bereit. • Der Designated-Port stellt den Mindestkostenpfad von einem verbundenen LAN über die Bridge zur CIST-Regional-Root bereit. • Alternate- und Backup-Ports haben dieselbe Funktionsweise wie bei RSTP, jedoch relativ zur CIST-Regional-Root.

Funktion	Beschreibung
MSTI-Port-Funktionen	Für jede MSTI an einer Bridge gilt: • Der Root-Port stellt den Mindestkostenpfad von der Bridge zur MSTI-Regional-Root bereit, sofern die Bridge nicht die MSTI-Regional-Root ist. • Der Designated-Port stellt den Mindestkostenpfad von einem verbundenen LAN über die Bridge zur MSTI-Regional-Root bereit. • Alternate- und Backup-Ports haben dieselbe Funktionsweise wie bei RSTP, jedoch relativ zur MSTI-Regional-Root. Der Master-Port, der in einer MSTP-Region einmalig ist, ist der CIST-Root-Port der CIST-Regional-Root und stellt den Mindestkostenpfad zur CIST-Root für alle MSTIs bereit.
Boundary-Ports	Ein Boundary-Port ist ein Port an einer Bridge in einer MSTP-Region, der sich mit Folgendem verbindet: mit einer Brücke, die einer anderen MSTP-Region angehört, oder mit einer Brücke, die nur RSTP oder das veraltete STP unterstützt. Ein Boundary-Port blockiert oder leitet alle VLANs von allen MSTIs und dem CIST gleichermaßen weiter. Ein Boundary-Port kann Folgendes sein: • Der CIST-Root-Port der CIST-Regional-Root (und demnach auch der MSTI-Master-Port). • Ein CIST-Designated-Port, CIST-Alternate/Backup-Port oder deaktiviert. An der Grenze der MSTP-Region ist die Funktion des MSTI-Ports mit der Funktion des CIST-Ports identisch. Ein mit einer STP-Bridge verbundener Boundary-Port sendet ausschließlich STP-BPDUs. Ein mit einer RSTP-Bridge verbundener Port braucht das Senden von STP-BPDUs nicht zu unterlassen. Dies wird ermöglicht, da das MSTP die Kennung der CIST-Regional-Root im Feld RSTP trägt, die das RSTP als die Kennung der Designated-Bridge parst.

Abschnitt 8.6.3.3

Vorteile von MSTP

MSTP wird standardmäßig konfiguriert, um automatisch zu einer Spannbaumlösung für jede konfigurierte MSTI zu gelangen. Vorteile können jedoch durch Einflussnahme auf die Topologie der MSTIs in einer MST-Region hinsichtlich der Bridge-Priorität und der Kosten der Ports erzielt werden.

Lastverteilung

MSTP kann zum Verteilen der Datenverkehrslast unter mehreren VLANs verwendet werden, wodurch eine bessere Verwendung eines überbrückten Netzwerks mit mehreren redundanten Verschaltungen zwischen den Bridges ermöglicht wird.

Ein überbrücktes Netzwerk, das durch einen einzelnen Spannbaum gesteuert wird, blockiert redundante Verbindungen aufgrund seines Aufbaus zur Vermeidung schädlicher Schleifen. Bei Verwendung von MSTP kann jede beliebige vorhandene Verbindung einen unterschiedlichen Sperrzustand für MSTI gemäß MSTP aufweisen. Jede vorhandene Verbindung kann sich daher im Sperrzustand für bestimmte VLANs und im Weiterleitungszustand für andere VLANs befinden, was von der Abbildung der VLANs auf die MSTIs abhängt.

Die Spannbaumlösung kann für jede MSTI gesteuert werden, insbesondere der Satz aktiver Verbindungen für jeden Baum, durch MSTI-weise Manipulation der Bridge-Priorität und der Portkosten der Verbindungen im Netzwerk. Wenn der Datenverkehr mehreren VLANs sinnvoll zugewiesen wird, können redundante Verschaltungen in einem überbrückten Netzwerk, die bei Verwendung eines einzelnen Spannbaums ungenutzt wären, den Verkehr transportieren.

Isolierung der Spanning-Tree-Neukonfiguration

Ein Verbindungsausfall in einer MSTP-Region, der sich nicht auf die Funktionen der Boundary-Ports auswirkt, verursacht weder eine Neukonfiguration des CST, noch wirkt sich die Änderung auf andere MSTP-Regionen aus. Grund dafür ist, dass MSTP-Informationen nicht über die Grenze einer Region hinaus propagiert werden.

MSTP vs. PVST

Ein Vorteil von MSTP gegenüber des Protokolls Per-VLAN Spanning Tree (PVST) von Cisco Systems Inc. ist die Möglichkeit der Abbildung mehrerer VLANs auf einer einzigen MSTI. Da ein Verarbeitungs- und Speicherbedarf für jeden Spannbaum existiert, nimmt der Aufwand für die Nachverfolgung einer zunehmenden Anzahl an VLANs bei PVST wesentlich schneller zu als bei MSTP.

Kompatibilität mit STP und RSTP

Für die Bridges einer MST-Region ist keine spezielle Konfiguration erforderlich, um sich vollständig und einfach mit Nicht-MST-Bridges im selben überbrückten Netzwerk zu verbinden. Für ein optimales Netzwerkdesign wird eine sorgfältige Planung und Konfiguration jedoch empfohlen.

Abschnitt 8.6.3.4

MSTP an einem überbrückten Netzwerk implementieren

Die folgende Vorgehensweise wird für die Konfiguration von MSTP in einem Netzwerk empfohlen. Führen Sie ausgehend von einem Satz MSTP-fähiger Ethernet-Bridges für jede Bridge im Netzwerk Folgendes aus:

HINWEIS
Eine sorgfältige Netzwerkanalyse und -planung sollte jeden Schritt der Erstellung eines MSTP-Netzes stützen.

HINWEIS
MSTP muss nicht aktiviert sein, um ein VLAN einer MSTI zuzuordnen. Das Mapping muss jedoch für jede Bridge, die zur MSTP-Region gehört, identisch sein.

1. Deaktivieren Sie STP. Weitere Informationen finden Sie unter Abschnitt 8.6.4, „Konfigurieren des STP (global)“.
2. Konfigurieren Sie eine oder mehrere MSTI (Multiple Spanning Tree Instances) jeweils mit einer eindeutigen Bridge-Priorität. Weitere Informationen finden Sie unter Abschnitt 8.6.6.3, „Hinzufügen einer Multiple Spanning Tree-Instanz“.
3. Erstellen Sie statische VLANs und ordnen Sie diese den MSTIs zu. Weitere Informationen finden Sie unter Abschnitt 8.5.5.2, „Hinzufügen eines statischen VLAN“.
4. Konfigurieren Sie individuelle MSTI für jeden Switched-Ethernet-Port und/oder jede Ethernet-Trunk-Schnittstelle, der/die MST BPDU (Bridge Protocol Data Unit)-Datenverkehr senden/empfangen wird. Weitere Informationen finden Sie unter Abschnitt 8.6.7, „MST-Instanzen nach Ports verwalten“.
5. Stellen Sie die STP-Protokollversion auf MSTP ein, konfigurieren Sie die MST-Regionskennung und den Revisionsstand und aktivieren Sie STP. Weitere Informationen finden Sie unter Abschnitt 8.6.4, „Konfigurieren des STP (global)“.

Abschnitt 8.6.4

Konfigurieren des STP (global)

Um globale Einstellungen für das Spanning Tree Protocol (STP) zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***switch » spanning-tree***.
3. Konfigurieren Sie die STP-Einstellungen mithilfe der folgenden Parameter:

Parameter	Beschreibung
enabled	**Zusammenfassung:** { true, false } **Standard:** true Aktiviert STP/RSTP/MSTP global für die Bridge. Beachten Sie, dass STP/RSTP/MSTP an einem Port aktiviert ist, wenn es global aktiviert und je Port eingestellt ist.
version { version }	**Zusammenfassung:** { stp, rstp, mstp } **Standard:** rstp Die Version (entweder STP, Rapid STP oder Multiple STP) des zu unterstützenden Spanning Tree Protocol (STP).
hello-time { hello-time }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 1 und 10 **Standard:** 2 Die Zeit zwischen den Konfigurationsnachrichten der Root Bridge. Kürzere "Hello"-Zeiten führen zu einer schnelleren Erkennung von Topologieänderungen auf Kosten moderater Steigerungen des STP-Verkehrs. (Beziehung: maxAgeTime >= 2 * (helloTime + 1,0 Sekunden))
max-age { max-age }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 6 und 40 **Standard:** 20 Die Zeitdauer, für die eine Konfigurationsnachricht gültig bleibt, nachdem sie von der Root Bridge ausgegeben wurde. Konfigurieren Sie diesen Parameter mit Vorsicht, wenn mehrere Ebenen von Bridges vorhanden oder langsame Verbindungen (wie z. B. in WANs) Teil des Netzwerks sind. (Beziehung: maxAgeTime >= 2 * (helloTime + 1,0 Sekunden))
tx-hold-count { tx-hold-count }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 0 und 100 **Standard:** 0 Die maximale Anzahl an Konfigurationsnachrichten an jedem Port, die in einem besonderen Ereignis gesendet werden dürfen, z. B. nach einem Ausfall oder beim Aufbau einer neuen Verbindung. Ist die maximale Anzahl an Nachrichten erreicht, wird das Rapid Spanning Tree Protocol (RSTP) auf eine Nachricht pro Sekunde begrenzt. Mithilfe höherer Werte kann sich das Netzwerk nach ausgefallenen Verbindungen schneller wiederherstellen. Wenn RSTP in einer Ringarchitektur verwendet wird, sollte der Transmit Count größer sein als die Anzahl der Switches im Ring. Ist keine Zahl festgelegt, gilt der Wert als unbegrenzt.
forward-delay { forward-delay }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 4 und 30 **Standard:** 15 Die Zeit, die eine Bridge mit dem Lernen von MAC-Adressen an einem aufkommenden Port verbringt, bevor sie mit der Weiterleitung des Verkehrs beginnt. Niedrigere Werte erlauben es dem Port, den Weiterleitungszustand schneller zu erreichen, wobei aber ungelernte Adressen an alle Ports überflutet werden.
max-hops { max-hops }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 6 und 40 **Standard:** 20 Der größtmögliche Bridge-Durchmesser in einer Multiple Spanning Tree (MST)-Region. MST BPDUs, die sich innerhalb einer MST-Region verbreiten, tragen einen Lebenszeit-Parameter, der von jedem BPDU verbreitenden Switch verringert wird. Wenn die maximale Anzahl an Hops innerhalb der Region das konfigurierte Maximum überschreitet, können die BPDUs aufgrund ihrer Lebenszeitinformationen verworfen

Parameter	Beschreibung
	werden. Dieser Parameter gilt nur für Multiple Spanning Tree Protocol (MSTP)-Konfigurationen.
mst-region-name { mst-region-name }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 32 Zeichen Der Name der MST-Region. Für alle Geräte in derselben MST-Region muss derselbe Regionname konfiguriert sein.
mst-revision-level { mst-revision-level }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 0 und 65535 **Standard:** 0 Der Revisionsstand für die MST-Konfiguration. In der Regel sind alle Geräte in derselben MST-Region mit dem gleichen Revisionsstand konfiguriert. Mit unterschiedlichen Revisionsständen können jedoch unter einem identischen Regionnamen Unterregionen erstellt werden.

4. Konfigurieren Sie die eRSTP-Einstellungen mithilfe der folgenden Parameter:

Parameter	Beschreibung
max-net-diameter-multiplier { max-net-diameter-multiplier }	**Zusammenfassung:** { 1, 4 } **Standard:** 4 Der "Max Network Diameter" als Multiplikator des Werts MaxAgeTime.
bpdu-guard { bpdu-guard }	**Zusammenfassung:** { specify, noshutdown, untilreset } **Standard:** noshutdown Der Standard des Rapid Spanning Tree Protocol (RSTP) behandelt nicht die Netzwerksicherheit. RSTP muss jede empfangene BPDU (Bridge Protocol Data Unit) verarbeiten und eine geeignete Maßnahme ergreifen. Dadurch hat ein Angreifer die Möglichkeit, die RSTP-Topologie zu beeinflussen, indem er RSTP BPDUs in das Netzwerk einspeist. Der "BPDU Guard" ist eine Funktion, die das Netzwerk vor BPDUs schützt, die von einem Port empfangen werden, an dem keine RSTP-fähigen Geräte angeschlossen werden sollen. Wenn eine BPDU von einem Port empfangen wird, für den der Parameter 'Edge' auf 'TRUE' gesetzt oder RSTP deaktiviert ist, wird der Port für den durch diesen Parameter angegebenen Zeitraum abgeschaltet. • NO SHUTDOWN: BPDU Guard ist deaktiviert. • UNTIL RESET: Der Port bleibt ausgeschaltet, bis der Benutzer den Befehl zum Zurücksetzen gibt. • SPECIFY: Für den Port wird mit dem BPDU-Timeout-Parameter eine Timeout-Dauer festgelegt.
bpdu-timeout { bpdu-timeout }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 1 und 86400 Die Dauer, für die ein Port ausgeschaltet wird. Nur verfügbar, wenn der Modus "BPDU Guard" auf *specify* eingestellt ist.
fast-root-failover { fast-root-failover }	**Zusammenfassung:** { on, off, on-with-standard-root } **Standard:** on Der Fast-Root-Failover-Algorithmus. Mögliche Optionen sind: • Off: Der Fast-Root-Failover-Algorithmus ist deaktiviert. Daher kann ein Root-Switch-Ausfall in einem Mesh-Netzwerk zu einer übermäßigen Dauer für die Konnektivitätswiederherstellung führen. • On: Fast-Root-Failover ist aktiviert und es wird der robusteste Algorithmus verwendet, der die Netzwerkkonnektivität im Falle eines Root-Bridge-Ausfalls in einem Mesh-Netzwerk schnell wiederherstellt. • On with standard root: Fast-Root-Failover ist aktiviert, aber es wird ein gelockerter Algorithmus verwendet, der Standard-Switches in der Root-Rolle zulässt.
dot1w-interop	**Zusammenfassung:** { true, false } **Standard:** true Aktiviert/deaktiviert die IEEE 802.1w-Interoperabilität
cost-style { cost-style }	**Zusammenfassung:** { stp, rstp } **Standard:** stp

Parameter	Beschreibung
	Die Höhe der aufzuwendenden Link-Kosten. STP verwendet 16-Bit-Pfadkosten auf Grundlage von 1x10E9/Verbindungsgeschwindigkeit (4 für 1 Gbit/s, 19 für 100 Mbit/s und 100 für 10 Mbit/s), während RSTP 32-Bit-Kosten auf Grundlage von 2x10E13/Verbindungsgeschwindigkeit (20.000 für 1 Gbit/s, 200.000 für 100 Mbit/s und 2.000.000 für 10 Mbit/s) verwendet. Beachten Sie, dass RSTP-Link-Kosten nur dann verwendet werden, wenn die unterstützte Bridge-Version RSTP zulässt und der Port nicht zum Spanning Tree Protocol (STP) migriert.

5. Konfigurieren Sie die RSTP-Instanz-Einstellungen mithilfe der folgenden Parameter:

Parameter	Beschreibung
bridge-priority { bridge-priority }	**Zusammenfassung:** { 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440 } **Standard:** 32768 Die dem RSTP/der Common Bridge Instance zugewiesene Priorität.

6. Fügen Sie je nach Bedarf Multiple Spanning Tree-Instanzen (MSTI) hinzu. Weitere Informationen finden Sie unter Abschnitt 8.6.6.3, „Hinzufügen einer Multiple Spanning Tree-Instanz“.
7. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 8.6.5

Konfigurieren des STP für Switched-Ethernet-Ports und Ethernet-Trunk-Schnittstellen

Um ein Spanning Tree Protocol (STP) für einen Switched-Ethernet-Port zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu:
   - **Bei Switched-Ethernet-Ports:**
     interface » switch » swport » {port} » spanning-tree, wobei *{port}* die Port-Nummer des Switched-Ethernet-Ports ist.
   - **Bei Ethernet-Trunk-Schnittstellen:**
     interface » trunks » {id} » spanning-tree, wobei *{id}* die ID für die Schnittstelle ist.
3. Konfigurieren Sie den/die folgenden Parameter:

Parameter	Beschreibung
enabled	**Zusammenfassung:** { true, false } **Standard:** true Aktiviert/deaktiviert STP/RSTP an der Schnittstelle.
admin-edge { admin-edge }	**Zusammenfassung:** { forceTrue, forceFalse, auto } **Standard:** auto Edge-Ports sind Ports, die nicht am Spanning Tree teilnehmen, aber trotzdem Konfigurationsmeldungen senden. Edge-Ports gehen direkt über, Frames weiterzuleiten, ohne Verzögerungen zu empfangen oder zu lernen. Die MAC-Tabellen der Edge-Ports müssen nicht geleert werden, wenn sich die Topologie im STP-Netzwerk ändert. Im Gegensatz zu einem deaktivierten STP-Port führt das versehentliche Anschließen eines Edge-Ports an einen anderen Port im Spanning Tree zu einer erkennbaren Schleife. Die

Parameter	Beschreibung
	Edgeness des Ports wird ausgeschaltet und die RSTP-Standardregeln gelten (bis zum nächsten Link-Ausfall).
admin-point-to-point { admin-point-to-point }	**Zusammenfassung:** { forceTrue, forceFalse, auto } **Standard:** auto RSTP verwendet ein Peer-Peer-Protokoll, das für einen schnellen Übergang an Punkt-zu-Punkt-Verbindungen sorgen soll. Dieses Protokoll wird automatisch ausgeschaltet, wenn mehrere STP-Bridges über ein gemeinsames LAN (nicht Punkt-zu-Punkt) kommunizieren. Die Bridge nimmt automatisch Punkt-zu-Punkt als TRUE an, wenn der Link im Vollduplex-Modus ausgeführt wird. Der Punkt-zu-Punkt-Parameter lässt dieses Verhalten zu oder überschreibt es und erzwingt so, dass Punkt-zu-Punkt TRUE oder FALSE ist. Parameter TRUE wird erzwungen, wenn der Port über eine Punkt-zu-Punkt-Verbindung verfügt, der Link aber nicht im Vollduplex-Modus ausgeführt werden kann. Parameter FALSE wird erzwungen; wenn der Port die Verbindung im Vollduplex-Modus ausführt, diese aber nicht Punkt-zu-Punkt ist (z. B. eine Vollduplex-Verbindung zu einer Unmanaged Bridge, die zwei weitere STP-Bridges umfasst).
restricted-role	Wenn dies aktiviert ist, wird der Port nicht als Root-Port für den CIST oder eine MSTI ausgewählt, obwohl er den besten Spanning-Tree-Prioritätsvektor hat. Dieser Parameter sollte auf FALSE voreingestellt sein.
restricted-tcn	Ist der Parameter TRUE, wird der Port keine empfangenen Benachrichtigungen zu Topologieänderungen und Topologieänderungen nicht an andere Ports weitergeben. Dieser Parameter sollte auf FALSE voreingestellt sein. Wenn der Parameter eingestellt ist, kann es nach Änderungen in der aktiven Topologie eines Spanning Trees zu einem vorübergehenden Verlust der Konnektivität kommen, was auf persistente, falsch erlernte Informationen über den Stationsstandort zurückzuführen ist.
rstp-priority { rstp-priority }	**Zusammenfassung:** { 0, 16, 32, 64, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240 } **Standard:** 128 Die STP-Portpriorität. Ports mit identischen Kosten, die an ein gemeinsames LAN angeschlossen sind, wählen den Port, den sie verwenden, anhand der Portpriorität.
stp-cost { stp-cost }	**Zusammenfassung:** { auto-cost } oder eine vorzeichenlose 32-Bit-Ganzzahl zwischen 0 und 65535 **Standard:** auto-cost Die Kosten, die in der Kostenkalkulation verwendet werden sollen, wenn in der Konfiguration der Bridge-RSTP-Parameter der Kostenstil-Parameter auf STP gesetzt ist. Wenn Sie die Kosten manuell festlegen, können Sie bestimmte Ports für die Übertragung von Datenverkehr vorziehen. Belassen Sie die Einstellung in diesem Feld auf 'auto', um die Standard-STP-Portkosten wie verhandelt zu verwenden (vier für 1 Gbit/s-, 19 für 100 Mbit/s- und 100 für 10 Mbit/s-Verbindungen). Für MSTP gilt dieser Parameter sowohl für externe als auch für interne Pfadkosten.
rstp-cost { rstp-cost }	**Zusammenfassung:** { auto-cost } oder eine vorzeichenlose 32-Bit-Ganzzahl zwischen 0 und 2147483647 **Standard:** auto-cost Die Kosten, die in der Kostenkalkulation verwendet werden sollen, wenn in der Konfiguration der Bridge-RSTP-Parameter der Kostenstil-Parameter auf RSTP gesetzt ist. Wenn Sie die Kosten manuell festlegen, können Sie bestimmte Ports für die Übertragung von Datenverkehr vorziehen. Belassen Sie die Einstellung in diesem Feld auf 'auto', um die Standard-STP-Portkosten wie verhandelt zu verwenden (20.000 für 1 Gbit/s-, 200.000 für 100 Mbit/s- und 2.000.000 für 10 Mbit/s-Verbindungen). Für MSTP gilt dieser Parameter sowohl für externe als auch für interne Pfadkosten.

4. Fügen Sie je nach Bedarf Multiple Spanning Tree-Instanzen (MSTI) hinzu. Weitere Informationen finden Sie unter Abschnitt 8.6.6.3, „Hinzufügen einer Multiple Spanning Tree-Instanz“.
5. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 8.6.6

MST-Instanzen global verwalten

MSTP (Multiple Spanning Tree Protocol) weist laut Definition des IEEE 802.1 Standards mehrere VLANs einer einzigen Spanning Tree Instance (STI) zu, die auch als MSTI (Multiple Spanning Tree Instance) bezeichnet wird.

Jeder MSTI ist eine MST-ID und eine Bridge-Priorität zugeordnet:

- Mit Hilfe der MST-ID wird die MSTI einem VLAN zugeordnet.
- Die Bridge-Priorität wird von allen Geräten in der Spanning-Tree-Topologie benutzt, um festzustellen, welches Gerät als Root-Gerät oder Backbone ausgewählt ist. Ein ideales Root-Gerät ist eines, das zentral im Netzwerk installiert und nicht mit Endgeräten verbunden ist.

Weitere Informationen über MSTIP finden Sie unter Abschnitt 8.6.3, „MSTP-Betrieb“.

INHALT

- Abschnitt 8.6.6.1, „Anzeigen der Statistik von Multiple Spanning Tree-Instanzen“
- Abschnitt 8.6.6.2, „Eine Liste der MST-Instanzen anzeigen“
- Abschnitt 8.6.6.3, „Hinzufügen einer Multiple Spanning Tree-Instanz“
- Abschnitt 8.6.6.4, „Eine MSTI (Multiple Spannung Tree Instance) löschen“

Abschnitt 8.6.6.1

Anzeigen der Statistik von Multiple Spanning Tree-Instanzen

Um die Statistik von Multiple Spanning Tree-Instanzen (MSTI) anzuzeigen, geben Sie Folgendes ein:

```
show switch spanning-tree msti-status
```

Eine Tabelle oder Liste ähnlich dem folgenden Beispiel wird angezeigt:

```
ruggedcom# show switch spanning-tree msti-status | tab
                                                                                ROOT  ROOT  ROOT  TOTAL
INSTANCE          ROOT                          BRIDGE                          PORT  PORT  PATH  TOP
ID        STATUS  PRIORITY  ROOT MAC            PRIORITY  BRIDGE MAC          SLOT  PORT  COST  CHANGES
--------------------------------------------------------------------------------------------------------
1         none    0         00:00:00:00:00:00   0         00:00:00:00:00:00   ---   -1    0     0
2         none    0         00:00:00:00:00:00   0         00:00:00:00:00:00   ---   -1    0     0
3         none    0         00:00:00:00:00:00   0         00:00:00:00:00:00   ---   -1    0     0
4         none    0         00:00:00:00:00:00   0         00:00:00:00:00:00   ---   -1    0     0
5         none    0         00:00:00:00:00:00   0         00:00:00:00:00:00   ---   -1    0     0
6         none    0         00:00:00:00:00:00   0         00:00:00:00:00:00   ---   -1    0     0
7         none    0         00:00:00:00:00:00   0         00:00:00:00:00:00   ---   -1    0     0
8         none    0         00:00:00:00:00:00   0         00:00:00:00:00:00   ---   -1    0     0
9         none    0         00:00:00:00:00:00   0         00:00:00:00:00:00   ---   -1    0     0
10        none    0         00:00:00:00:00:00   0         00:00:00:00:00:00   ---   -1    0     0
11        none    0         00:00:00:00:00:00   0         00:00:00:00:00:00   ---   -1    0     0
12        none    0         00:00:00:00:00:00   0         00:00:00:00:00:00   ---   -1    0     0
13        none    0         00:00:00:00:00:00   0         00:00:00:00:00:00   ---   -1    0     0
14        none    0         00:00:00:00:00:00   0         00:00:00:00:00:00   ---   -1    0     0
15        none    0         00:00:00:00:00:00   0         00:00:00:00:00:00   ---   -1    0     0
16        none    0         00:00:00:00:00:00   0         00:00:00:00:00:00   ---   -1    0     0
```

Diese Tabelleoder Liste liefert die folgenden Informationen:

Parameter	Beschreibung
instance-id	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 1 und 16

Parameter	Beschreibung
	Die Bridge-Kennung dieser Bridge.
status	**Zusammenfassung:** { none, designatedBridge, notDesignatedForAnyLAN, rootBridge } Der Spanning Tree-Status der Bridge. Der Status kann "root" oder "designated" sein. Im Feld kann 'not designated for any LAN' stehen, falls die Bridge für keinen der Ports bestimmt (designated) ist. Dieser Parameter ist obligatorisch.
root-priority	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl Die Bridge-Kennung der Root-Bridge. Dieser Parameter ist obligatorisch.
root-mac	**Zusammenfassung:** Eine Zeichenkette mit 17 Zeichen Die Bridge-Kennung der Root-Bridge. Dieser Parameter ist obligatorisch.
bridge-priority	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl Die Bridge-Kennung dieser Bridge. Dieser Parameter ist obligatorisch.
bridge-mac	**Zusammenfassung:** Eine Zeichenkette mit 17 Zeichen Die Bridge-Kennung dieser Bridge. Dieser Parameter ist obligatorisch.
root-port-slot	**Zusammenfassung:** { { --- }{ sm, lm1, lm2, lm3, lm4, lm5, lm6, swport, eth, serport, celport, wlanport }{ trnk } } Wenn die Bridge "designated" ist, ist dies der Steckplatz mit dem Port, der die Verbindung zur Root-Bridge des Netzwerks herstellt. Dieser Parameter ist obligatorisch.
root-port-port	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl Wenn die Bridge "designated" ist, ist dies der Port des Steckplatzes, der die Verbindung zur Root-Bridge des Netzwerks herstellt. Dieser Parameter ist obligatorisch.
root-path-cost	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Gesamtkosten des Pfads zur Root-Bridge, zusammengesetzt aus Summe der Kosten jeder Verbindung im Pfad. Wenn keine benutzerdefinierten Kosten konfiguriert wurden, tragen 1-Gbit/s-Ports Kosten von vier, 100-Mbit/s-Ports von 19 und 10-Mbit/s-Ports von 100 bei. Für die Common und Internal Spanning Tree (CIST)-Instanz des Multiple Spanning Tree Protocol (MSTP) sind dies externe Root-Pfadkosten, die die Kosten des Pfades von der (regionalen) Root-Bridge des Internal Spanning Tree (IST) zur (globalen Netzwerk-) Root-Bridge des Common Spanning Tree (CST) sind. Dieser Parameter ist obligatorisch.
total-top-changes	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Eine Zählung der Topologieänderungen im Netzwerk, wie sie an dieser Bridge über Link-Ausfälle erkannt oder von anderen Bridges signalisiert werden. Zu hohe oder schnell ansteigende Zählungen signalisieren Netzwerkprobleme. Dieser Parameter ist obligatorisch.

Abschnitt 8.6.6.2

Eine Liste der MST-Instanzen anzeigen

Um eine Liste der MST-(Multiple Spanning Tree)-Instanzen (MSTIs) anzusehen, geben Sie Folgendes ein:

```
show running-config switch spanning-tree mstp-instance
```

Falls Instanzen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config switch spanning-tree mstp-instance | tab
INSTANCE  BRIDGE
ID        PRIORITY
--------------------
1         32768
2         57344

!
```

Falls keine MSTIs konfiguriert wurden, fügen Sie je nach Bedarf Instanzen hinzu. Weitere Informationen finden Sie unter Abschnitt 8.6.6.3, „Hinzufügen einer Multiple Spanning Tree-Instanz“.

Abschnitt 8.6.6.3
Hinzufügen einer Multiple Spanning Tree-Instanz

Um eine Multiple Spanning Tree-Instanz (MSTI) hinzuzufügen, gehen Sie wie folgt vor:

HINWEIS
RUGGEDCOM ROX II unterstützt bis zu 16 MSTIs.

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.

   WICHTIG!
   Da jede MSTI als unabhängige RSTP-Instanz agiert, ist ihre Konfiguration mit der RSTP-Konfiguration vergleichbar. Eine MSTI wird jedoch solange als inaktiv betrachtet, bis ein oder mehrere VLANs einer MSTI zugeordnet werden.

2. Fügen Sie die Multiple Spanning Tree-Instanz hinzu, indem Sie Folgendes eingeben:

   ```
   switch spanning-tree mstp-instance id
   ```

   Erläuterung:

   - *id* ist die ID für die Multiple Spanning Tree-Instanz

3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
{ instance-id }	**Zusammenfassung:** Eine Zeichenkette Die Instanz-ID des Multiple Spanning Tree Protocol (MSTP)
bridge-priority { bridge-priority }	**Zusammenfassung:** { 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440 } **Standard:** 32768 Die Bridge-Priorität bietet eine Möglichkeit, die Topologie des mit dem Spanning Tree Protocol (STP) verbundenen Netzwerks zu steuern. Die gewünschten Root-Bridges und "designated" Bridges können für eine bestimmte Topologie konfiguriert werden. Root-Bridge wird die Bridge mit der niedrigsten Priorität. Bei einem Ausfall der Root-Bridge wird die Bridge mit der nächstniedrigen Priorität zur Root-Bridge. "Designated" Bridges, die (zu Redundanzzwecken) ein gemeinsames Local Area Network (LAN) bedienen, legen ebenfalls mit der Priorität fest, welche Brücke aktiv ist. Auf diese Weise kann durch eine sorgfältige Auswahl der Bridge-Prioritäten der Pfad des Verkehrsflusses unter normalen und anormalen Bedingungen bestimmt werden.

4. Ordnen Sie ein oder mehrere statische VLANs zu und ordnen Sie diese den MSTIs zu. Weitere Informationen finden Sie unter Abschnitt 8.5.5.2, „Hinzufügen eines statischen VLAN“.
5. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 8.6.6.4
Eine MSTI (Multiple Spannung Tree Instance) löschen

Um eine MSTI (Multiple Spanning Tree Instance) zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die MST-Instanz durch Eingabe von:

   ```
   no switch spanning-tree mstp-instance ID
   ```

   Erläuterung:

   - *`ID`* ist die ID der MST-Instanz
3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 8.6.7
MST-Instanzen nach Ports verwalten

Dieser Abschnitt beschreibt, wie Sie MSTIs (Multiple Spanning Tree Instances) für einzelne Ports konfigurieren und verwalten können.

INHALT

- Abschnitt 8.6.7.1, „Statistiken für MST-Instanzen je Port anzeigen“
- Abschnitt 8.6.7.2, „Anzeigen einer Liste der Multiple Spanning Tree-Instanzen (MSTI) pro Port“
- Abschnitt 8.6.7.3, „Hinzufügen einer portspezifischen Multiple Spanning Tree-Instanz“
- Abschnitt 8.6.7.4, „Löschen von portspezifischen Multiple Spanning Tree-Instanzen“

Abschnitt 8.6.7.1
Statistiken für MST-Instanzen je Port anzeigen

Um MSTI (Multiple Spanning Tree Instance)-Statistiken für einzelne Switched-Ethernet-Ports und/oder Ethernet-Trunk-Schnittstellen anzuzeigen, geben Sie Folgendes ein:

```
show switch spanning-tree port-msti-id
```

Eine Tabelle ähnlich dem folgenden Beispiel wird angezeigt:

```
ruggedcom# show switch spanning-tree port-msti-id
                                                DESIG
INSTANCE                STP       STP           BRIDGE
ID        SLOT    PORT  STATE     ROLE  COST    PRIORITY  DESIG BRIDGE MAC
-------------------------------------------------------------------------
1
```

```
          swport  1     disabled  ----  0     0          00:00:00:00:00:00
          swport  2     disabled  ----  0     0          00:00:00:00:00:00
          swport  3     disabled  ----  0     0          00:00:00:00:00:00
          swport  4     disabled  ----  0     0          00:00:00:00:00:00
          swport  5     disabled  ----  0     0          00:00:00:00:00:00
          swport  6     disabled  ----  0     0          00:00:00:00:00:00
2
          swport  1     disabled  ----  0     0          00:00:00:00:00:00
          swport  2     disabled  ----  0     0          00:00:00:00:00:00
          swport  3     disabled  ----  0     0          00:00:00:00:00:00
          swport  4     disabled  ----  0     0          00:00:00:00:00:00
          swport  5     disabled  ----  0     0          00:00:00:00:00:00
          swport  6     disabled  ----  0     0          00:00:00:00:00:00
.
.
.
```

Diese Tabelle liefert die folgenden Informationen:

Parameter	Beschreibung
instance-id	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 1 und 16 Die Instanz-ID des Multiple Spanning Tree Protocol (MSTP).
slot	**Zusammenfassung:** { { sm, lm1, lm2, lm3, lm4, lm5, lm6, swport, eth, serport, celport, wlanport }{ trnk } } Der Steckplatz des Moduls, das diesen Port enthält.
port	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 1 und 16 Die Portnummer, wie auf der Frontscheibe des Switch aufgedruckt.
stp-state	**Zusammenfassung:** { disabled, blocking, listening, learning, forwarding, linkDown, discarding } Der Status dieser Schnittstelle im Spanning Tree: • Disabled: Das Spanning Tree Protocol (STP) ist an diesem Port deaktiviert. • Link Down: STP ist an diesem Port aktiviert, aber die Verbindung ist "down". • Discarding: Die Verbindung wird in der STP-Topologie nicht verwendet, aber sie ist in Bereitschaft. • Learning: Der Port lernt MAC-Adressen, um eine Überflutung zu verhindern, wenn er mit der Weiterleitung des Verkehrs beginnt. • Forwarding: Der Port leitet Verkehr weiter. Dieser Parameter ist obligatorisch.
stp-role	**Zusammenfassung:** { ----, root, designated, alternate, backup, master } Die Rolle dieses Ports im Spanning Tree: • Designated: Der Port ist für das Local Area Network (LAN) bestimmt, mit dem er verbunden ist (d. h. an dessen Root er Verkehr leitet). • Root: Der einzige Port auf der Bridge, der für Konnektivität zur Root-Bridge sorgt. • Backup: Der Port ist an ein LAN angeschlossen, das von einem anderen Port auf der Bridge bedient wird. Er wird nicht verwendet, ist aber in Bereitschaft. • Alternate: Der Port ist an eine Bridge angebunden, die für Konnektivität zur Root-Bridge sorgt. Er wird nicht verwendet, ist aber in Bereitschaft. • Master: Gibt es nur im Multiple Spanning Tree Protocol (MSTP). Der Port ist ein Boundary-Port der Multiple Spanning Tree (MST)-Region und der einzige Port auf der Bridge, der für Konnektivität für die Multiple Spanning Tree-Instanz zur Root-Bridge des Common Spanning Tree (CST) sorgt (d. h. dieser Port ist der Root-Port für die Common Spanning Tree-Instanz). Dieser Parameter ist obligatorisch.
cost	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl

Parameter	Beschreibung
	Die Gesamtkosten des Pfads zur Root-Bridge, zusammengesetzt aus Summe der Kosten jeder Verbindung im Pfad. Wenn keine benutzerdefinierten Kosten konfiguriert wurden, tragen 1-Gbit/s-Ports Kosten von vier, 100-Mbit/s-Ports von 19 und 10-Mbit/s-Ports von 100 bei. Für die Common und Internal Spanning Tree (CIST)-Instanz des Multiple Spanning Tree Protocol (MSTP) sind dies externe Root-Pfadkosten, die die Kosten des Pfades von der (regionalen) Root-Bridge des Internal Spanning Tree (IST) zur (globalen Netzwerk-) Root-Bridge des Common Spanning Tree (CST) sind. Dieser Parameter ist obligatorisch.
desig-bridge-priority	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl Die Bridge-Kennung dieser Bridge. Dieser Parameter ist obligatorisch.
desig-bridge-mac	**Zusammenfassung:** Eine Zeichenkette mit 17 Zeichen Die Bridge-Kennung dieser Bridge. Dieser Parameter ist obligatorisch.

Abschnitt 8.6.7.2

Anzeigen einer Liste der Multiple Spanning Tree-Instanzen (MSTI) pro Port

Um eine Liste der Multiple Spanning Tree-Instanzen (MSTI) für Switched-Ethernet-Ports oder Ethernet-Trunk-Schnittstellen anzuzeigen, geben Sie Folgendes ein:

- **Bei Switched-Ethernet-Ports:**

  ```
  show running-config interface switch swport port spanning-tree msti
  ```

  Erläuterung:

  - *port* ist die Nummer des Ports (oder eine Liste von Ports, wenn sie in einem Port-Trunk gebündelt sind) für das Modul.

- **Bei Ethernet-Trunk-Schnittstellen:**

  ```
  show running-config interface trunk id spanning-tree msti
  ```

  Erläuterung:

  - *id* ist die ID für die Schnittstelle

Falls Instanzen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config interface trunks 1 spanning-tree msti | tab
INSTANCE  MSTP
ID        PRIORITY  STP COST   RSTP COST
----------------------------------------
1         128       auto-cost  auto-cost
2         128       auto-cost  auto-cost

 !
!

show running-config interface trunk id spanning-tree msti
```

Erläuterung:

- *id* ist die ID für die Schnittstelle

Falls MSTIs konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config interface trunks 1 spanning-tree msti | tab
INSTANCE  MSTP
```

```
ID        PRIORITY  STP COST   RSTP COST
------------------------------------------
1         128       auto-cost  auto-cost
2         128       auto-cost  auto-cost

 !
!
```

Falls keine MSTIs konfiguriert wurden, fügen Sie sie je nach Bedarf hinzu. Weitere Informationen finden Sie unter Abschnitt 8.6.7.3, „Hinzufügen einer portspezifischen Multiple Spanning Tree-Instanz“.

Abschnitt 8.6.7.3

Hinzufügen einer portspezifischen Multiple Spanning Tree-Instanz

Um einem Switched-Ethernet-Port oder einer Ethernet-Trunk-Schnittstelle eine Multiple Spanning Tree-Instanz (MSTI) hinzuzufügen, gehen Sie wie folgt vor:

HINWEIS
RUGGEDCOM ROX II unterstützt bis zu 16 MSTIs pro Port/Schnittstelle.

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.

   WICHTIG!
   Da jede MSTI als unabhängige RSTP-Instanz agiert, ist ihre Konfiguration mit der RSTP-Konfiguration vergleichbar. Eine MSTI wird jedoch solange als inaktiv betrachtet, bis ein oder mehrere VLANs einer MSTI zugeordnet werden.

2. Fügen Sie die MSTI hinzu, indem Sie Folgendes eingeben:

   - **Bei Switched-Ethernet-Ports:**

     ```
     interface switch swport port spanning-tree msti id
     ```

     Erläuterung:

     - *slot* ist die Bezeichnung des Modul-Einbauorts
     - *port* ist die Nummer des Ports (oder eine Liste von Ports, wenn sie in einem Port-Trunk gebündelt sind) für das Modul.
     - *id* ist die ID für die Multiple Spanning Tree-Instanz

   - **Bei Ethernet-Trunk-Schnittstellen:**

     ```
     interface trunks id spanning-tree msti mstp-id
     ```

     Erläuterung:

     - *id* ist die ID für die Schnittstelle
     - *mstp-id* ist die ID für die Multiple Spanning Tree-Instanz

3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
mstp-priority { mstp-priority }	**Zusammenfassung:** { 0, 16, 32, 64, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240 } **Standard:** 128 Die STP-Portpriorität. Ports mit identischen Kosten, die an ein gemeinsames LAN angeschlossen sind, wählen den Port, den sie verwenden, anhand der Portpriorität.
stp-cost { stp-cost }	**Zusammenfassung:** { auto-cost } oder eine vorzeichenlose 32-Bit-Ganzzahl zwischen 0 und 65535

Parameter	Beschreibung
	Standard: auto-cost Die Kosten, die in der Kostenkalkulation verwendet werden sollen, wenn in der Konfiguration der Bridge-RSTP-Parameter der Kostenstil-Parameter auf STP gesetzt ist. Wenn Sie die Kosten manuell festlegen, können Sie bestimmte Ports für die Übertragung von Datenverkehr vorziehen. Belassen Sie die Einstellung in diesem Feld auf 'auto', um die Standard-STP-Portkosten wie verhandelt zu verwenden (vier für 1 Gbit/s-, 19 für 100 Mbit/s- und 100 für 10 Mbit/s-Verbindungen). Für MSTP gilt dieser Parameter sowohl für externe als auch für interne Pfadkosten.
rstp-cost { rstp-cost }	**Zusammenfassung:** { auto-cost } oder eine vorzeichenlose 32-Bit-Ganzzahl zwischen 0 und 2147483647 **Standard:** auto-cost Die Kosten, die in der Kostenkalkulation verwendet werden sollen, wenn in der Konfiguration der Bridge-RSTP-Parameter der Kostenstil-Parameter auf RSTP gesetzt ist. Wenn Sie die Kosten manuell festlegen, können Sie bestimmte Ports für die Übertragung von Datenverkehr vorziehen. Belassen Sie die Einstellung in diesem Feld auf 'auto', um die Standard-STP-Portkosten wie verhandelt zu verwenden (20.000 für 1 Gbit/s-, 200.000 für 100 Mbit/s- und 2.000.000 für 10 Mbit/s-Verbindungen). Für MSTP gilt dieser Parameter sowohl für externe als auch für interne Pfadkosten.

4. Ordnen Sie ein oder mehrere statische VLANs zu und ordnen Sie diese den MSTIs zu. Weitere Informationen finden Sie unter Abschnitt 8.5.5.2, „Hinzufügen eines statischen VLAN“.
5. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 8.6.7.4

Löschen von portspezifischen Multiple Spanning Tree-Instanzen

Um zu einem Switched-Ethernet-Port oder einer Ethernet-Trunk-Schnittstelle eine Multiple Spanning Tree-Instanz (MSTI) zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die MSTI, indem Sie Folgendes eingeben:
   - **Bei Switched-Ethernet-Ports:**
     ```
     no interface switch swport port spanning-tree msti id
     ```
     Erläuterung:
     - *`slot`* ist die Bezeichnung des Modul-Einbauorts
     - *`port`* ist die Nummer des Ports (oder eine Liste von Ports, wenn sie in einem Port-Trunk gebündelt sind) für das Modul.
     - *`id`* ist die ID für die Multiple Spanning Tree-Instanz
   - **Bei Ethernet-Trunk-Schnittstellen:**
     ```
     no interface trunks id spanning-tree msti mstp-id
     ```
     Erläuterung:
     - *`id`* ist die ID für die Schnittstelle
     - *`mstp-id`* ist die ID für die Multiple Spanning Tree-Instanz
3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 8.6.8

Anzeigen des Status eines RSTP

Um den Status eines RSTP-Netzwerks anzuzeigen, geben Sie Folgendes ein:

```
show switch spanning-tree rstp-status
```

Eine Liste ähnlich dem folgenden Beispiel wird angezeigt:

```
ruggedcom# show switch spanning-tree rstp-status
rstp-status
 status                   notDesignatedForAnyLAN
 bridge priority          32768
 bridge mac               00:0a:dc:f6:c6:ff
 root priority            32768
 root mac                 00:0a:dc:00:71:57
 regional root priority   32768
 regional root mac        00:0a:dc:f6:c6:ff
 root port slot           swport
 root port port           1
 root path cost           38
 regional root path cost  0
 configured hello time    2
 learned hello time       2
 configured forward delay 15
 learned forward delay    15
 configured max age       20
 learned max age          20
 total top changes        5
```

Diese Liste liefert die folgenden Informationen:

Parameter	Beschreibung
status	**Zusammenfassung:** { none, designatedBridge, notDesignatedForAnyLAN, rootBridge } Der Spanning Tree-Status der Bridge. Der Status kann "root" oder "designated" sein. Im Feld kann 'not designated for any LAN' stehen, falls die Bridge für keinen der Ports bestimmt (designated) ist. Dieser Parameter ist obligatorisch.
bridge-priority	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl Die Bridge-Kennung dieser Bridge. Dieser Parameter ist obligatorisch.
bridge-mac	**Zusammenfassung:** Eine Zeichenkette mit 17 Zeichen Die Bridge-Kennung dieser Bridge. Dieser Parameter ist obligatorisch.
root-priority	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl Die Ports, an die der Verkehr der Multicast-Gruppen weitergeleitet wird. Dieser Parameter ist obligatorisch.
root-mac	**Zusammenfassung:** Eine Zeichenkette mit 17 Zeichen Die Ports, an die der Verkehr der Multicast-Gruppen weitergeleitet wird. Dieser Parameter ist obligatorisch.
regional-root-priority	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl Die Bridge-Kennung der regionalen Root-Bridge des Internal Spanning Tree (IST) für die Multiple Spanning Tree (MST)-Region, zu der dieses Gerät gehört. Dieser Parameter ist obligatorisch.

Parameter	Beschreibung
regional-root-mac	**Zusammenfassung:** Eine Zeichenkette mit 17 Zeichen Die Bridge-Kennung der regionalen Root-Bridge des Internal Spanning Tree (IST) für die Multiple Spanning Tree (MST)-Region, zu der dieses Gerät gehört. Dieser Parameter ist obligatorisch.
root-port-slot	**Zusammenfassung:** { { --- }{ sm, lm1, lm2, lm3, lm4, lm5, lm6, swport, eth, serport, celport, wlanport }{ trnk } } Wenn die Bridge "designated" ist, ist dies der Steckplatz mit dem Port, der die Verbindung zur Root-Bridge des Netzwerks herstellt. Dieser Parameter ist obligatorisch.
root-port-port	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl Wenn die Bridge "designated" ist, ist dies der Port des Steckplatzes, der die Verbindung zur Root-Bridge des Netzwerks herstellt. Dieser Parameter ist obligatorisch.
root-path-cost	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Gesamtkosten des Pfads zur Root-Bridge, zusammengesetzt aus Summe der Kosten jeder Verbindung im Pfad. Wenn keine benutzerdefinierten Kosten konfiguriert wurden. 1-Gbit/s-Ports tragen Kosten von vier, 100-Mbit/s-Ports von 19 und 10-Mbit/s-Ports von 100 bei. Für die Common und Internal Spanning Tree (CIST)-Instanz des Multiple Spanning Tree Protocol (MSTP) sind dies externe Root-Pfadkosten, die die Kosten des Pfades von der (regionalen) Root-Bridge des Internal Spanning Tree (IST) zur (globalen Netzwerk-) Root-Bridge des Common Spanning Tree (CST) sind. Dieser Parameter ist obligatorisch.
regional-root-path-cost	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Für die Common und Internal Spanning Tree (CIST)-Instanz des Multiple Spanning Tree Protocol (MSTP) sind dies Pfadkosten zur (regionalen) Root-Bridge des Internal Spanning Tree (IST). Dieser Parameter ist obligatorisch.
configured-hello-time	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl Die konfigurierte "Hello"-Zeit aus dem Menü "Bridge RSTP Parameters". Dieser Parameter ist obligatorisch.
learned-hello-time	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl Die tatsächliche von der Root-Bridge gegebene "Hello“-Zeit, wie von den Konfigurationsnachrichten gelernt. Diese Zeit wird bei "designated" Bridges verwendet. Dieser Parameter ist obligatorisch.
configured-forward-delay	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl Die konfigurierte Weiterleitungsverzögerungszeit aus dem Menü "Bridge RSTP Parameters". Dieser Parameter ist obligatorisch.
learned-forward-delay	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl Die tatsächliche von der Root-Bridge gegebene Weiterleitungsverzögerungszeit, wie von den Konfigurationsnachrichten gelernt. Diese Zeit wird bei "designated" Bridges verwendet. Dieser Parameter ist obligatorisch.
configured-max-age	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl Die konfigurierte "maximum age"-Zeit aus dem Menü "Bridge RSTP Parameters". Dieser Parameter ist obligatorisch.
learned-max-age	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl Die tatsächliche von der Root-Bridge gegebene "maximum age“-Zeit, wie von den Konfigurationsnachrichten gelernt. Diese Zeit wird bei "designated" Bridges verwendet.

Parameter	Beschreibung
	Dieser Parameter ist obligatorisch.
total-top-changes	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Eine Zählung der Topologieänderungen im Netzwerk, wie sie an dieser Bridge über Link-Ausfälle erkannt oder von anderen Bridges signalisiert werden. Zu hohe oder schnell ansteigende Zählungen signalisieren Netzwerkprobleme. Dieser Parameter ist obligatorisch.

Abschnitt 8.6.9

RSTP-Statistiken je Port anzeigen

Um für jeden Port die Rapid Spanning Tree Protocol (RSTP)-Statistiken anzuzeigen, geben Sie Folgendes ein:

```
show switch spanning-tree port-rstp-stats
```

Eine Tabelle oder Liste ähnlich dem folgenden Beispiel wird angezeigt:

```
ruggedcom# show switch spanning-tree port-rstp-stats | tab DESG BRIDGE OPER RX TX RX TX RX TX SLOT
 PORT STP STATE STP ROLE COST PRIORITY DESG BRIDGE MAC EDGE RSTS RSTS CONFIGS CONFIGS TCNS TCNS
 ------------------------------------------------------------------------------------------ swport 4
 forwarding designated 19 0 00:00:00:00:00:00 true 0 43086 0 0 0 0
```

Diese Tabelle oder Liste liefert die folgenden Informationen:

Parameter	Beschreibung
slot	**Zusammenfassung:** { { sm, lm1, lm2, lm3, lm4, lm5, lm6, swport, eth, serport, celport, wlanport }{ trnk } } Der Steckplatz des Moduls, das diesen Port enthält.
port	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 1 und 16 Die Portnummer, wie auf der Frontscheibe des Switch aufgedruckt.
stp-state	**Zusammenfassung:** { disabled, blocking, listening, learning, forwarding, linkDown, discarding } Beschreibt den Status dieser Schnittstelle im Spanning Tree: • Disabled: Spanning Tree Protocol (STP) ist an diesem Port deaktiviert. • Link Down: STP ist an diesem Port aktiviert, aber die Verbindung ist "down". • Discarding: Die Verbindung wird in der STP-Topologie nicht verwendet, aber sie ist in Bereitschaft. • Learning: Der Port lernt MAC-Adressen, um eine Überflutung zu verhindern, wenn er mit der Weiterleitung des Verkehrs beginnt. • Forwarding: Der Port leitet Verkehr weiter. Dieser Parameter ist obligatorisch.
stp-role	**Zusammenfassung:** { ----, root, designated, alternate, backup, master } Die Rolle dieses Ports im Spanning Tree: • Designated: Der Port ist für das Local Area Network (LAN) bestimmt, mit dem er verbunden ist (d. h. an dessen Root er Verkehr leitet). • Root: Der einzige Port auf der Bridge, der für Konnektivität zur Root-Bridge sorgt. • Backup: Der Port ist an ein LAN angeschlossen, das von einem anderen Port auf der Bridge bedient wird. Er wird nicht verwendet, ist aber in Bereitschaft. • Alternate: Der Port ist an eine Bridge angebunden, die für Konnektivität zur Root-Bridge sorgt. Er wird nicht verwendet, ist aber in Bereitschaft. • Master: Gibt es nur im Multiple Spanning Tree Protocol (MSTP). Der Port ist ein Boundary-Port der Multiple Spanning Tree (MST)-Region und der einzige Port auf der Bridge, der für

Parameter	Beschreibung
	Konnektivität für die Multiple Spanning Tree-Instanz (MSTI) zur Root-Bridge des Common Spanning Tree (CST) sorgt (d. h. dieser Port ist der Root-Port für die Common Spanning Tree-Instanz). Dieser Parameter ist obligatorisch.
cost	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die von diesem Port angebotenen Kosten. Wenn unter Bridge RSTP Parameters der Kostenstil auf STP eingestellt ist, tragen 1-Gbit/s-Ports Kosten von vier, 100-Mbit/s-Ports von 19 und 10-Mbit/s-Ports von 100 bei. Wenn der Kostenstil auf RSTP eingestellt ist, tragen 1-Gbit/s-Ports Kosten von 20.000, 100-Mbit/s-Ports von 200.000 und 10-Mbit/s-Ports von 2.000.000 bei. Beachten Sie, dass, selbst wenn der Kostenstil auf RSTP eingestellt ist, die Kosten eines Ports, der zu STP migriert, auf maximal 65535 begrenzt sind. Dieser Parameter ist obligatorisch.
desg-bridge-priority	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 0 und 65535 An den Root-Ports der "designated" Bridges, die Kennung der Bridge, an die dieser Port angebunden ist. Dieser Parameter ist obligatorisch.
desg-bridge-mac	**Zusammenfassung:** Eine Zeichenkette mit 17 Zeichen An den Root-Ports der "designated" Bridges, die Kennung der Bridge, an die dieser Port angebunden ist. Dieser Parameter ist obligatorisch.
oper-edge	**Zusammenfassung:** { true, false } Gibt an, ob der Port als Edge-Port dient. Dieser Parameter ist obligatorisch.
rx-rsts	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl an Konfigurationsnachrichten des Rapid Spanning Tree Protocol (RSTP), die an diesem Port empfangen werden. Dieser Parameter ist obligatorisch.
tx-rsts	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl an Konfigurationsnachrichten des Rapid Spanning Tree Protocol (RSTP), die an diesem Port übertragen werden. Dieser Parameter ist obligatorisch.
rx-configs	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl an Konfigurationsnachrichten des Spanning Tree Protocol (STP), die an diesem Port empfangen werden. Dieser Parameter ist obligatorisch.
tx-configs	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl an Konfigurationsnachrichten des Spanning Tree Protocol (STP), die an diesem Port übertragen werden. Dieser Parameter ist obligatorisch.
rx-tcns	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl an Nachrichten zu Konfigurationsänderungen, die an diesem Port empfangen werden. Zu hohe oder schnell ansteigende Zählungen signalisieren Netzwerkprobleme. Dieser Parameter ist obligatorisch.
tx-tcns	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl an Konfigurationsnachrichten, die von diesem Port übertragen werden. Dieser Parameter ist obligatorisch.

Abschnitt 8.6.10

Statistiken für STP (Spanning Tree Protocol) löschen

Um alle STP-Statistiken zu löschen, geben Sie Folgendes ein:

```
switch spanning-tree clear-stp-stats
```

9 Serieller Server

Dieses Kapitel beschreibt, wie Sie den seriellen Server mit seriellen Ports, Protokollen, entfernten Hosts und den Tabellen mit Geräteadressen verwalten und konfigurieren können.

INHALT

- Abschnitt 9.1, „Serielle Ports verwalten“
- Abschnitt 9.2, „Serielle Port-Protokolle verwalten“
- Abschnitt 9.3, „Geräteadressentabellen verwalten“
- Abschnitt 9.4, „Serielles Multicast-Streaming verwalten“
- Abschnitt 9.5, „Entfernte Hosts verwalten“
- Abschnitt 9.6, „Lokale Hosts verwalten“
- Abschnitt 9.7, „Entfernte Host-Schnittstellen verwalten“
- Abschnitt 9.8, „Lokale Host-Schnittstellen verwalten“

Abschnitt 9.1

Serielle Ports verwalten

Dieser Abschnitt beschreibt, wie Sie serielle Ports im Gerät konfigurieren, überwachen und verwalten können.

INHALT

- Abschnitt 9.1.1, „Eine Liste der seriellen Ports anzeigen“
- Abschnitt 9.1.2, „Anzeigen der Statistik für serielle Ports“
- Abschnitt 9.1.3, „Anzeigen der Statistik der Transportverbindungen“
- Abschnitt 9.1.4, „Statiken für DNP-Gerätetabellen anzeigen“
- Abschnitt 9.1.5, „Statistiken für serielle Ports löschen“
- Abschnitt 9.1.6, „Einen seriellen Port konfigurieren“
- Abschnitt 9.1.7, „Den seriellen Server neu starten“
- Abschnitt 9.1.8, „Einen seriellen Port zurücksetzen“

Abschnitt 9.1.1

Eine Liste der seriellen Ports anzeigen

Um eine Liste der seriellen Ports, die auf einem Gerät konfiguriert sind, anzuzeigen, geben Sie Folgendes ein:

```
show running-config interface serial
```

Eine Tabelle oder Liste ähnlich dem folgenden Beispiel wird angezeigt:

```
ruggedcom# show running-config interface serial | tab BAUD DATA STOP FLOW
 PORT SLOT PORT ENABLED ALIAS RATE BITS PARITY BITS CONTROL TYPE PROTOCOL
 ------------------------------------------------------------------------------ serport 1 true - 9600
 8 none 1 none rs232 serport 2 true - 9600 8 none 1 none rs232 !
```

Abschnitt 9.1.2

Anzeigen der Statistik für serielle Ports

Um die für einen bestimmten seriellen Port erhobene Statistik anzuzeigen, geben Sie Folgendes ein:

```
show interfaces serial port
```

Eine Tabelle oder Liste ähnlich dem folgenden Beispiel wird angezeigt:

```
ruggedcom# show interfaces serial port | tab TX TX RX RX PACKET PARITY FRAMING OVERRUN
 IFNAME MEDIA SPEED PROTOCOL CHARS PACKETS CHARS PACKETS ERRORS ERRORS ERRORS ERRORS
 ------------------------------------------------------------------------------------------------------
 ser-1 RS232 9.6K none 0 0 0 0 0 0 0 0 ser-2 RS232 9.6K none 0 0 0 0 0 0 0 0
```

Diese Tabelle oder Liste liefert die folgenden Informationen:

Parameter	Beschreibung
media	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 31 Zeichen Der Typ des Portmediums { RS232 RS422 RS485 }. Dieser Parameter ist obligatorisch.
speed	**Zusammenfassung:** { auto, 1.5M, 2.4M, 10M, 100M, 1G, 10G, 1.776M, 3.072M, 7.2M, 1.2K, 2.4K, 9.6K, 19.2K, 38.4K, 57.6K, 115.2K, 230.4K, 4.8K, 76.8K } Die Geschwindigkeit (in "Kilobits-per-second"). Dieser Parameter ist obligatorisch.
protocol	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 31 Zeichen Das dem Port zugewiesene serielle Protokoll. Dieser Parameter ist obligatorisch.
tx-chars	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl der über den seriellen Port übertragenen Bytes. Dieser Parameter ist obligatorisch.
tx-packets	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl der über den seriellen Port übertragenen Pakete. Dieser Parameter ist obligatorisch.
rx-chars	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl der vom seriellen Port empfangenen Bytes. Dieser Parameter ist obligatorisch.
rx-packets	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl der vom seriellen Port empfangenen Pakete. Dieser Parameter ist obligatorisch.
packet-errors	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl

Parameter	Beschreibung
	Die Anzahl der Paketfehler an diesem seriellen Port. Dieser Parameter ist obligatorisch.
parity-errors	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl der Paritätsfehler an diesem seriellen Port. Dieser Parameter ist obligatorisch.
framing-errors	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl der Framing Errors an diesem seriellen Port. Dieser Parameter ist obligatorisch.
overrun-errors	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl der Overrun-Fehler an diesem seriellen Port. Dieser Parameter ist obligatorisch.

Abschnitt 9.1.3

Anzeigen der Statistik der Transportverbindungen

Um die für alle Transportverbindungen erhobene Statistik anzuzeigen, geben Sie Folgendes ein:

```
show interfaces serial transport-connections
```

Eine Tabelle oder Liste ähnlich dem folgenden Beispiel wird angezeigt:

```
ruggedcom# show interfaces serial transport-connections | tab
                     REMOTE  LOCAL             RX       TX       TARGET
INDEX  REMOTE IP     PORT    PORT   TRANSPORT  PACKETS  PACKETS  PORT      STATUS
-------------------------------------------------------------------------------
1      10.200.22.199 15836   20000  TCP        177      0        ser-1,  Active
```

Um die für eine bestimmte Transportverbindung erhobene Statistik anzuzeigen, geben Sie Folgendes ein:

```
show interfaces serial transport-connections index
```

Eine Tabelle oder Liste ähnlich dem folgenden Beispiel wird angezeigt:

Diese Tabellen oder Listen liefern die folgenden Informationen:

Parameter	Beschreibung
remote-ip	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 32 Zeichen Die IP-Adresse des entfernten seriellen Servers. Dieser Parameter ist obligatorisch.
remote-port	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl Der Port des entfernten seriellen Servers. Dieser Parameter ist obligatorisch.
local-port	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl Der lokale Port für die eingehende Verbindung. Dieser Parameter ist obligatorisch.
transport	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 8 Zeichen Das Transport-Protokoll (UDP oder TCP) für diesen seriellen Port. Dieser Parameter ist obligatorisch.

Parameter	Beschreibung
rx-packets	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl der vom TCP/UDP empfangenen Pakete. Dieser Parameter ist obligatorisch.
tx-packets	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl der an das TCP/UDP übertragenen Pakete. Dieser Parameter ist obligatorisch.
target-port	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 1024 Zeichen Der serielle Zielport. Dieser Parameter ist obligatorisch.
status	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 31 Zeichen Der Verbindungszustand des seriellen Ports. Dieser Parameter ist obligatorisch.

Abschnitt 9.1.4

Statiken für DNP-Gerätetabellen anzeigen

Um die Statistiken für DNP-Gerätetabellen anzusehen, geben Sie Folgendes ein:

```
show interfaces serial dnp-device-table
```

Eine Tabelle oder Liste ähnlich der Folgenden wird angezeigt:

```
ruggedcom# show interfaces serial dnp-device-table | tab
DEVICE                  SERIAL
ADDRESS  REMOTE IP      PORT
---------------------------------
10       -              ser-1
20       10.200.22.199  -
```

Diese Tabelle oder Liste liefert die folgenden Informationen:

Parameter	Beschreibung
device-address	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 32 Zeichen Die DNP-Geräteadresse.
remote-ip	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 32 Zeichen Die IP-Adresse des dezentralen Hosts, der zur DNP-Geräteadresse eine Verbindung herstellt. Dieser Parameter ist obligatorisch.
serial-port	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 128 Zeichen Der serielle Zielport. Dieser Parameter ist obligatorisch.

Abschnitt 9.1.5

Statistiken für serielle Ports löschen

Um die Statistiken für einen bestimmten seriellen Port zu löschen, geben Sie Folgendes ein:

```
interfaces serial port name clear-port-stats
```

Erläuterung:

- *name* ist die dem Port zugewiesene Bezeichnung

Abschnitt 9.1.6

Einen seriellen Port konfigurieren

Um einen seriellen Port zu konfigurieren, gehen Sie wie folgt vor:

WICHTIG!
Aktivieren Sie nicht die Flusskontrolle, solange das Modbus TCP-Protokoll aktiv ist.

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***interface » serial » {port}***, wobei *{port}* der serielle Port ist.
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
enabled	**Zusammenfassung:** { true, false } **Standard:** true Bietet die Option, diese Schnittstelle zu aktivieren oder zu deaktivieren. Wenn die Option nicht markiert ist (d. h. deaktiviert), verhindert die Schnittstelle, dass Frames an dieser Schnittstelle gesendet oder empfangen werden.
alias { alias }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 64 Zeichen Der SNMP-Aliasname der Schnittstelle.
baud-rate { baud-rate }	**Zusammenfassung:** { 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200, 230400, 76800 } **Standard:** 9600 Die eingestellte Baudrate des seriellen Ports.
data-bits { data-bits }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 7 und 8 **Standard:** 8 Die Anzahl an Datenbits.
parity { parity }	**Zusammenfassung:** { none, even, odd } **Standard:** none Die Parität des seriellen Ports.
stop-bits { stop-bits }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 1 und 2 **Standard:** 1 Die Anzahl an Stoppbits des seriellen Ports.
flow-control { flow-control }	**Zusammenfassung:** { none, xonxoff } **Standard:** none Flusskontrolle des seriellen Ports.
port-type { port-type }	**Zusammenfassung:** { rs232, rs422, rs485 } **Standard:** rs232 Der Typ des seriellen Ports.

4. Konfigurieren Sie ein oder mehrere serielle Protokolle. Weitere Informationen finden Sie unter Abschnitt 9.2.3, „Hinzufügen eines Protokolls des seriellen Ports“.

5. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 9.1.7
Den seriellen Server neu starten

Um den seriellen Server neu zu starten, geben Sie Folgendes ein:

```
interfaces serial restart-serserver
```

Abschnitt 9.1.8
Einen seriellen Port zurücksetzen

Um einen seriellen Port zurückzusetzen, geben Sie Folgendes ein:

```
interfaces serial port name reset
```

Erläuterung:

- *`name`* ist die dem Port zugewiesene Bezeichnung

Abschnitt 9.2
Serielle Port-Protokolle verwalten

Dieser Abschnitt beschreibt, wie Sie Protokolle für serielle Ports konfigurieren und verwalten können.

INHALT

- Abschnitt 9.2.1, „Konzepte serieller Port-Protokolle“
- Abschnitt 9.2.2, „Eine Liste der Protokolle für serielle Ports anzeigen“
- Abschnitt 9.2.3, „Hinzufügen eines Protokolls des seriellen Ports“
- Abschnitt 9.2.4, „DNP-Protokoll konfigurieren“
- Abschnitt 9.2.5, „Das Modbus TCP-Protokoll konfigurieren“
- Abschnitt 9.2.6, „Konfigurieren des Raw-Socket-Protokolls“
- Abschnitt 9.2.7, „Ein Protokoll des seriellen Ports löschen“

Abschnitt 9.2.1

Konzepte serieller Port-Protokolle

Dieser Abschnitt beschreibt einige wesentliche Konzepte für die Implementierung serieller Port-Protokolle in RUGGEDCOM ROX II.

INHALT

- Abschnitt 9.2.1.1, „Raw-Socket-Anwendungen“
- Abschnitt 9.2.1.2, „Modbus TCP-Anwendungen“
- Abschnitt 9.2.1.3, „DNP-Anwendungen“
- Abschnitt 9.2.1.4, „Ein-/ausgehende serielle Verbindungen“

Abschnitt 9.2.1.1

Raw-Socket-Anwendungen

Das Raw-Socket-Protokoll transportiert Zeichenströme von einem seriellen Port am Gerät zu einer angegebenen dezentralen IP-Adresse und Port. Das Raw-Socket-Protokoll unterstützt den TCP- und UDP-Transport.

» Broadcast RTU Polling

Das Broadcast-Polling erlaubt einem einzelnen, mit dem Gerät verbundenen Host, einen Polling-Strom an mehrere dezentrale RTUs zu übertragen.

Der Host ist über einen seriellen Port mit dem Gerät verbunden. Es können bis zu 32 dezentrale TCP-RTUs über das Netzwerk mit dem Hostende des Geräts verbunden werden. Beim UDP-Transport kann das Gerät einen Polling-Strom an bis zu 64 dezentrale Hosts (RTUs) senden.

Zu Beginn platzieren die dezentralen Hosts TCP-Verbindungen an das Hostende des Geräts. Das Hostende wird wiederum so konfiguriert, dass es die erforderliche Anzahl eingehender TCP-Verbindungen akzeptiert. Der mit dem Gerät verbundene Host sendet dann nacheinander Polling-Anfragen an jeden dezentralen Host. Wenn eine Polling-Anfrage empfangen wird, leitet (d.h. überträgt) das Gerät diese Anfrage an alle dezentralen Hosts. Alle dezentralen Hosts empfangen die Anfrage und der entsprechende dezentrale Host gibt eine Antwort aus. Die Antwort wird an das Gerät zurückgesandt, von wo aus sie an den Host weitergeleitet wird.

» Host- und dezentrale Funktionen

Das Raw-Socket-Protokoll kann eine TCP-Verbindung für die serielle Kapselung entweder initiieren oder akzeptieren. Es kann eine Verbindung herstellen, die von einem dezentralen Host, umgekehrt oder bidirektional initiiert wurde.

Konfigurieren Sie das Gerät am Hostende, um eine Verbindung zum dezentralen Host herzustellen, wenn:

- Das Hostende eine Portumleitung nutzt, die die Verbindung herstellen muss
- Das Hostende nur gelegentlich aktiviert ist und die Verbindung herstellen wird, wenn es aktiv wird
- Eine Firewall am Hostende voraussetzt, dass die Verbindung ausgehend hergestellt wird

Wenn das Hostende mehrere Verbindungen zu dezentralen Enden zur Implementierung des Broadcast-Pollings öffnen will, konfigurieren Sie das Gerät so, dass es Verbindungen zu dezentralen Enden akzeptiert.

Konfigurieren Sie das Gerät so, dass es sich von jeder Seite (Host oder dezentral) zur anderen Seite verbindet, falls beide Seiten diese Funktion unterstützen.

Paketierung von Nachrichten

Der serielle Server puffert empfangene Zeichen in Paketen, um die Netzwerkeffizienz zu verbessern und Nachrichten abzugrenzen.

Der serielle Server wendet drei Verfahren an, um zu entscheiden, wann die Paketierung und Weiterleitung der gepufferten Zeichen zum Netzwerk erfolgen sollen:

- Paketierung bei einem bestimmten Zeichen
- Paketierung bei Zeitüberschreitung
- Paketierung bei einem vollen Paket

Wenn die Paketierung bei einem bestimmten Zeichen konfiguriert ist, überprüft der serielle Server jedes empfangene Zeichen, paketiert es und leitet es nach dem Empfangen des bestimmten Zeichens weiter. Bei dem Zeichen handelt es sich üblicherweise um ein <CR>- oder ein <LF>-Zeichen oder ein beliebiges ASCII-Zeichen.

Wenn die Paketierung bei Zeitüberschreitung konfiguriert ist, wartet der serielle Server eine konfigurierbare Zeit nach dem Empfangen eines Zeichens ab, bevor er mit der Paketierung und Weiterleitung beginnt. Wenn ein anderes Zeichen während des Warteintervalls empfangen wird, wird der Timer neu gestartet. Bei diesem Verfahren können als Teil einer Gesamtnachricht übertragene Zeichen in einem einzigen Paket an das Netzwerk weitergeleitet werden, wenn der Timer abläuft, nachdem er das allerletzte Zeichen der Nachricht erhalten hat. Dies ist üblicherweise der einzige Paketierer, wenn die Modbus TCP-Kommunikation unterstützt wird.

Der serielle Server führt die Paketierung und Weiterleitung bei einem vollen Paket immer aus, insbesondere dann, wenn die Anzahl an Zeichen seinen Kommunikationspuffer (1024 Bytes) ausfüllt.

Abschnitt 9.2.1.2

Modbus TCP-Anwendungen

Die Modbus TCP-Serveranwendung wird für den Transport von Modbus-Anfragen und -Antworten über IP-Netzwerke verwendet. Die Quelle der Abfragen ist ein Modbus-*Master*. Dabei handelt es sich um einen Host-Computer, der die Abfragen an einen dezentralen Host (RTU) ausgibt, der mit dem seriellen Port des Geräts verbunden ist, auf dem die Modbus TCP-Serveranwendung ausgeführt wird. Die in TCP-Paketen verpackten Modbus-Abfragen, die das Gerät empfängt, werden in Abhängigkeit von der in der RTU-Liste festgelegten Hostadresse über den seriellen Port an den dezentralen Host weitergeleitet. Die Antworten des dezentralen Host werden in TCP-Paketen verpackt und an den *Master* zurückgesendet, von dem die Abfragen stammen.

Portnummern

Die TCP-Portnummer für die Modbus-Nutzung ist Port 502. Die Modbus TCP-Serveranwendung kann auch so konfiguriert werden, dass sie eine Verbindung an einer konfigurierbaren Portnummer akzeptiert. Dieser Hilfsport kann von Mastern genutzt werden, die den Port 502 nicht unterstützen.

Erneute Übertragungen

Das Server-Gateway bietet die Möglichkeit einer erneuten Sendung einer Anfrage an einen dezentralen Host, falls der dezentrale Host die Anfrage fälschlicherweise empfängt bzw. falls das Server-Gateway die Antwort des dezentralen Host fälschlicherweise empfängt.

Die Entscheidung für die Verwendung erneuter Übertragungen und die Anzahl der Verwendungen hängt u.a. von den folgenden Faktoren ab:

- Die Wahrscheinlichkeit eines Leitungsfehlers.
- Die Anzahl an dezentralen Hosts und die Datenverkehrsmenge am Port.

- Die Kosten für die erneute Übertragung der Anfrage vom Server gegenüber der Zeitüberschreitung und der erneuten Übertragung am Master. Diese Kosten werden durch die Geschwindigkeit der Ports und des Netzwerks beeinflusst.

» Behandlung von ModBus-Ausnahmen

Wenn das Server-Gateway eine Anfrage für einen nicht-konfigurierten dezentralen Host empfängt, antwortet es dem Ersteller mit einer speziellen Nachricht, die als Ausnahme (Typ 10) bezeichnet wird. Eine Ausnahme vom Typ 11 wird vom Server zurückgegeben, falls der dezentrale Host nicht auf die Anfragen antwortet.

Native Modbus TCP-Polling-Pakete wollen diese Nachrichten empfangen. Die unmittelbare Anzeige eines Versäumnisses kann die Wiederherstellungssequenzen beschleunigen und den Bedarf an langen Zeitüberschreitungen reduzieren.

Abschnitt 9.2.1.3

DNP-Anwendungen

Der RUGGEDCOM ROX II unterstützt das Distributed-Network-Protokoll (DNP) der Version 3.0, das allgemein von Hilfsprogrammen in Prozessautomatisierungssystemen verwendet wird. DNP3-Protokollnachrichten legen Quell- und Zieladressen fest. Eine Zieladresse gibt an, welches Gerät die Daten verarbeiten soll, und eine Quelladresse gibt an, welches Gerät die Nachricht senden soll. Sowohl die Ziel- als auch die Quelladresse erfüllen mindestens eine Anforderung für die Peer-to-Peer-Kommunikation, da der Empfänger weiß, wohin eine Antwort zu leiten ist.

Jedes Gerät, das DNP unterstützt, muss eine eindeutige Adresse innerhalb des Pools an Geräten haben, die DNP-Nachrichten senden und empfangen.

» Adressenlernen für DNP

Der RUGGEDCOM ROX II implementiert sowohl das Lernen lokaler als auch dezentraler Adressen für DNP. Eine Tabelle mit lokalen Geräteadressen wird mit DNP-Adressen gefüllt, die für lokale und dezentrale DNP-Geräte gelernt wurden. Jeder DNP-Adresse wird entweder ein lokaler serieller Port oder eine dezentrale IP-Adresse zugewiesen.

Wenn eine Nachricht mit einer unbekannten DNP-Quelladresse an einem lokalen seriellen Port empfangen wird, dann werden die DNP-Quelladresse und die Nummer des seriellen Ports in die Tabelle mit den Geräteadressen eingegeben. Wenn eine Nachricht mit einer unbekannten DNP-Quelladresse vom IP-Netzwerk an der IP-Schnittstelle empfangen wird, die als DNP-Lernschnittstelle konfiguriert ist, dann werden die DNP-Quelladresse und die IP-Adresse des Absenders in die Tabelle mit den Geräteadressen eingegeben.

Wenn eine Nachricht mit einer unbekannten DNP-Zieladresse an einem lokalen seriellen Port empfangen wird, dann wird die Nachricht in einem UDP-Broadcast an die Netzwerkschnittstelle gesendet, die als DNP-Lernschnittstelle konfiguriert ist. Wenn eine Nachricht mit einer unbekannten DNP-Zieladresse vom IP-Netzwerk empfangen wird, dann wird die Nachricht an alle lokalen seriellen Ports gesendet, die als DNP-Ports konfiguriert sind.

HINWEIS
Gelernte Adressen werden in der Tabelle mit den Geräteadressen nicht aufgezeichnet.

Der UDP-Transport wird während der DNP-Adresslernphase verwendet.

Ein Aging-Timer existiert für jede DNP-Adresse in der Tabelle und wird zurückgesetzt, wenn eine DNP-Nachricht für die spezifizierte Adresse gesendet oder empfangen wird.

Aufgrund dieser Lernmethode kann das DNP3-Protokoll mit einer minimalen Anzahl an Parametern konfiguriert werden: eine TCP/UDP-Portnummer, eine lernende Netzwerkschnittstelle und ein Aging-Timer.

DNP-Broadcast-Nachrichten

Die DNP-Adressen 65521 bis 65535 sind als DNP-Broadcast-Adressen reserviert. Der RUGGEDCOM ROX II unterstützt DNP3-Broadcast-Nachrichten. An lokalen seriellen Ports empfangene DNP-Broadcast-Nachrichten werden an alle IP-Adressen in der Tabelle mit den Geräteadressen übertragen (unabhängig davon, ob gelernt oder statisch konfiguriert).

Wenn eine DNP-Broadcast-Nachricht vom IP-Netzwerk empfangen wird, dann wird die Nachricht an alle lokalen seriellen Ports übertragen, die als DNP-Ports konfiguriert sind.

Abschnitt 9.2.1.4
Ein-/ausgehende serielle Verbindungen

RUGGEDCOM RX1400 unterstützt bis zu 32 TCP/UDP-Verbindungen je seriellem Port, bis zu 64 TCP/UDP-Verbindungen zum seriellen Server.

Abschnitt 9.2.2
Eine Liste der Protokolle für serielle Ports anzeigen

Um eine Liste der Protokolle für serielle Ports, die auf einem Gerät konfiguriert sind, anzuzeigen, geben Sie Folgendes ein:

```
show interfaces serial port protocol
```

Falls Protokolle konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show interfaces serial port protocol IFNAME PROTOCOL ------------------ ser-1 none ser-2
 none
```

Falls keine Protokolle konfiguriert wurden, fügen Sie je nach Bedarf Protokolle hinzu. Weitere Informationen finden Sie unter Abschnitt 9.2.3, „Hinzufügen eines Protokolls des seriellen Ports“.

Abschnitt 9.2.3
Hinzufügen eines Protokolls des seriellen Ports

Um ein Protokoll des seriellen Ports hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie das Protokoll hinzu, indem Sie Folgendes eingeben:

   ```
   interface serial serport port protocols protocol
   ```

   Erläuterung:

   - *port* ist die Nummer des Ports (oder eine Liste von Ports, wenn sie in einem Port-Trunk gebündelt sind) für das Modul.
   - *protocol* ist der Protokolltyp Optionen sind u.a. dnp, tcpmodbus, rawsocket und vmserial.

3. Wenn `dnp`, `tcpmodbus`oder `rawsocket` ausgewählt wurden, konfigurieren Sie das Protokoll.
   - Weitere Informationen über das Konfigurieren eines DNP-Protokolls finden Sie in Abschnitt 9.2.4, „DNP-Protokoll konfigurieren“.
   - Weitere Informationen über das Konfigurieren eines Modbus TCP-Protokolls finden Sie in Abschnitt 9.2.5, „Das Modbus TCP-Protokoll konfigurieren“.
   - Weitere Informationen über das Konfigurieren eines Raw Socket-Protokolls finden Sie in Abschnitt 9.2.6, „Konfigurieren des Raw-Socket-Protokolls“.
4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 9.2.4
DNP-Protokoll konfigurieren

Um für einen seriellen Port das DNP-Protokoll zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***interface » serial » {interface} » protocols » dnp » setdnp***, wobei *{interface}* der serielle Port ist.
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
address-learning { address-learning }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 15 Zeichen Die Schnittstelle, von der die RTU-Adresse zu lernen ist.
aging-timer { aging-timer }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 60 und 10800 **Standard:** 1000 Die Zeitdauer, die ein gelerntes DNP-Gerät in der Tabelle "Device Address" ohne DNP-Kommunikation bleiben kann, bevor es aus der Tabelle entfernt wird.
max-connection { max-connection }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 1 und 32 **Standard:** 1 Die maximale Anzahl eingehender DNP-Verbindungen.

4. Fügen Sie eine Tabelle mit Geräteadressen hinzu. Für weitere Informationen über das Hinzufügen von Tabellen mit Geräteadressen siehe Abschnitt 9.3.2, „Hinzufügen einer Tabelle mit Geräteadressen“.
5. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 9.2.5
Das Modbus TCP-Protokoll konfigurieren

Um das Modbus TCP-Protokoll für einen seriellen Port zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***interface » serial » {interface} » protocols » tcpmodbus » settcpmodbus***, wobei *{interface}* der serielle Port ist.
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
response-timer { response-timer }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 50 und 10000 **Standard:** 100 Die maximale Zeit vom letzten übertragenen Zeichen der ausgehenden Abfrage bis zum ersten Zeichen der Antwort. Wenn die RTU in dieser Zeit nicht antwortet, gilt die Abfrage als fehlgeschlagen.
pack-timer { pack-timer }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 5 und 1000 **Standard:** 1000 Die maximal zulässige Zeit, nach dem Start einer Modbus-Anfrage auf die Antwort zu warten, bis sie beendet ist.
turnaround { turnaround }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 0 und 1000 **Standard:** 0 Die Zeitverzögerung (gegebenenfalls), die nach der Übertragung von Modbus-Broadcast-Nachrichten vom seriellen Port einzufügen ist.
retransmit { retransmit }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 0 und 2 **Standard:** 0 Die Häufigkeit, zu der die Anfrage erneut an die RTU übertragen wird, bevor die Versuche abgebrochen werden.
max-connection { max-connection }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 1 und 32 **Standard:** 1 Die maximale Anzahl eingehender Verbindungen.
local-port { local-port }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl **Standard:** 502 Die alternative lokale TCP-Portnummer. Sofern dieses Feld konfiguriert ist, kann eine einzige Verbindung (je serieller Port) zu dieser Portnummer hergestellt werden. Beachten Sie, dass Modbus TCP die voreingestellte lokale Portnummer 502 verwendet. Die Anzahl der Verbindungen zum Standard-TCP-Port ist unbegrenzt.
rtu-list { rtu-list }	**Zusammenfassung:** Eine Zeichenkette Die ID der RTU(s), die an den seriellen Port angeschlossen sind. Geben Sie mehrere RTUs mit einem Leerzeichen (z. B. 1 2 3 4) oder mit Komma und Leerzeichen (z. B. 1, 2, 3, 4) an. Eine streng durch Kommata getrennte Liste (z. B. 1,2,3,4) ist nicht zulässig. Dieser Parameter ist obligatorisch.

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 9.2.6

Konfigurieren des Raw-Socket-Protokolls

Um das Raw-Socket-Protokoll zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***interface » serial » {interface} » protocols » rawsocket***, wobei *{interface}* der serielle Port ist.
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
pack-char { pack-char }	**Zusammenfassung:** { off } oder eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 0 und 255

Parameter	Beschreibung
	Standard: off Der numerische Wert des ASCII-Zeichens, der die Weiterleitung akkumulierter Daten an das Netzwerk erzwingt.
pack-timer { pack-timer }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 5 und 1000 **Standard:** 1000 Die Verzögerung vom letzten empfangenen Zeichen bis zur Weiterleitung der Daten.
pack-size { pack-size }	**Zusammenfassung:** { max } oder eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 16 und 1400 **Standard:** max Die maximale Bytezahl, die vom seriellen Port zur Weiterleitung empfangen wurde.
turnaround { turnaround }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 0 und 1000 **Standard:** 0 Die Zeitverzögerung (gegebenenfalls), die zwischen Übertragung von einzelner Nachrichten vom seriellen Port einzufügen ist.
call-direction { call-direction }	**Zusammenfassung:** { in, out, both } **Standard:** out Zeigt an, ob Sie eine eingehende Verbindung angenommen, eine ausgehende Verbindung aufgebaut wird oder beides.
max-connection { max-connection }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 1 und 32 **Standard:** 1 Die maximale Anzahl zulässiger eingehender Verbindungen, wenn die Aufrufrichtung eingehend ist.
remote-ip { remote-ip }	**Zusammenfassung:** Eine Zeichenkette mit 7 bis 15 Zeichen oder eine Zeichenkette mit 6 bis 40 Zeichen Die IP-Adresse, die beim Aufbau einer ausgehenden Verbindung verwendet wird.
remote-port { remote-port }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 1024 und 65535 Der für ausgehende Verbindungen verwendete TCP-Zielport.
local-ip { local-ip }	**Zusammenfassung:** Eine Zeichenkette mit 7 bis 15 Zeichen oder eine Zeichenkette mit 6 bis 40 Zeichen Die zum Herstellen einer Verbindung verwendete IP-Adresse. Bleibt das Feld leer, kann zu jeder Schnittstelle eine eingehende Verbindung hergestellt werden.
local-port { local-port }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 1024 und 65535 Der lokale TCP/UDP-Port, über den eingehende Verbindungen angenommen werden.
transport { transport }	**Zusammenfassung:** { tcp, udp } **Standard:** tcp Das Transport-Connection-Protokoll (UDP oder TCP).

4. Wenn das Transport-Connection-Protokoll auf UDP gesetzt ist, konfigurieren Sie einen oder mehrere dezentrale Hosts für den Port. Weitere Informationen über das Hinzufügen eines dezentralen Hosts finden Sie in Abschnitt 9.5.2, „Hinzufügen eines entfernten Hosts“.
5. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 9.2.7
Ein Protokoll des seriellen Ports löschen

Um ein Protokoll des seriellen Ports zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie das Protokoll des seriellen Ports, indem Sie Folgendes eingeben:

   ```
   no interface serial serport port protocols protocol
   ```

   Erläuterung:

   - *port* ist die Nummer des Ports (oder eine Liste von Ports, wenn sie in einem Port-Trunk gebündelt sind) für das Modul.
   - *protocol* ist der Protokolltyp
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 9.3
Geräteadressentabellen verwalten

Dieser Abschnitt beschreibt, wie Sie DNP-Adressen in der lokalen Geräteadressentabelle verwalten können.

INHALT

- Abschnitt 9.3.1, „Eine Liste der Tabellen mit Geräteadressen anzeigen“
- Abschnitt 9.3.2, „Hinzufügen einer Tabelle mit Geräteadressen“
- Abschnitt 9.3.3, „Löschen einer Tabelle mit Geräteadressen“

Abschnitt 9.3.1
Eine Liste der Tabellen mit Geräteadressen anzeigen

Um eine Liste der Tabellen mit Geräteadressen anzuzeigen, die für einen seriellen Port mit DNP-Protokoll konfiguriert wurden, geben Sie Folgendes ein:

```
show running-config interface serial slot/port protocols dnp setdnp device-table
```

Erläuterung:

- *slot/port* ist die Bezeichnung des Slots und die Port-Nummer des seriellen Ports

Falls Tabellen mit Geräteadressen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config interface serial protocols dnp setdnp device-table
interface
 serial serport 1
  protocols dnp
   setdnp device-table 12
    remote-ip     172.30.130.2
    remote-device
   !
  !
```

```
  !
!
```

Falls keine Tabellen mit Geräteadressen konfiguriert wurden, fügen Sie je nach Bedarf Tabellen hinzu. Weitere Informationen finden Sie unter Abschnitt 9.3.2, „Hinzufügen einer Tabelle mit Geräteadressen“.

Abschnitt 9.3.2
Hinzufügen einer Tabelle mit Geräteadressen

Um eine Tabelle mit Geräteadressen für einen seriellen Port mit DNP-Protokoll hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. ```
   interface serial serport port protocols dnp setdnp device-table address
   ```

   Erläuterung:

   - *port* ist die Nummer des Ports (oder eine Liste von Ports, wenn sie in einem Port-Trunk gebündelt sind) für das Modul.
   - *address* ist die lokale oder dezentrale Adresse des DNP-Geräts. Die Adresse kann eine Adresse eines DNP-Geräts sein, das an einen lokalen seriellen Port angeschlossen ist, oder eine Adresse, die über den seriellen Port eines dezentralen IP-Host abrufbar ist.
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
remote-ip { remote-ip }	**Zusammenfassung:** Eine Zeichenkette mit 7 bis 15 Zeichen oder eine Zeichenkette mit 6 bis 40 Zeichen Die IP-Adresse des dezentralen Hosts, die mit der konfigurierten Adresse eine Verbindung zum DNP-Gerät liefert. Um DNP-Nachrichten, die mit der konfigurierten Adresse übereinstimmen, an den lokalen seriellen Port weiterzuleiten, lassen Sie dieses Feld leer.
remote-device	Aktiviert die Weiterleitung von DNP-Nachrichten, die mit der Geräteadresse übereinstimmen, an die entfernte IP.

4. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 9.3.3
Löschen einer Tabelle mit Geräteadressen

Um eine Tabelle mit Geräteadressen zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die Tabelle mit Geräteadressen, indem Sie Folgendes eingeben:

   ```
   no interface serial serport port protocols dnp setdnp device-table address
   ```

   Erläuterung:

   - *port* ist die Nummer des Ports (oder eine Liste von Ports, wenn sie in einem Port-Trunk gebündelt sind) für das Modul.
   ```

- *address* ist die lokale oder dezentrale Adresse des DNP-Geräts. Die Adresse kann eine Adresse eines DNP-Geräts sein, das an einen lokalen seriellen Port angeschlossen ist, oder eine Adresse, die über den seriellen Port eines dezentralen IP-Host abrufbar ist.

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 9.4
Serielles Multicast-Streaming verwalten

RUGGEDCOM ROX II unterstützt den Ein- und Ausgang serieller Multicast-Streams über Rawsocket UDP.

Dieser Abschnitt beschreibt, wie Sie serielle Multicast-Streams konfigurieren und verwalten können.

INHALT

- Abschnitt 9.4.1, „Serielles Multicast-Streaming verstehen“
- Abschnitt 9.4.2, „Serielles Multicast-Streaming konfigurieren“
- Abschnitt 9.4.3, „Beispiel: Serielle Schnittstellen, die als "Sink"-Gerät für Multicast-Streams konfiguriert sind“
- Abschnitt 9.4.4, „Beispiel: Für Multicast-Streams als stromliefernd konfigurierte serielle Schnittstellen“
- Abschnitt 9.4.5, „Beispiel: Für Multicast-Streams als stromliefernd und stromziehend konfigurierte serielle Schnittstellen“

Abschnitt 9.4.1
Serielles Multicast-Streaming verstehen

Serielles Multicast-Streaming gestattet die Übertragung serieller Datenströme an einzelne oder Gruppen entfernter Hosts über das UDP-Protokoll.

Ein Ethernet-Multicast-Stream besteht aus einer IP-Adresse einer Multicast-Gruppe (z. B. 232.1.1.1), einem UDP-Zielport (z. B. 1 bis 65535) und einer Schnittstelle.

Ein serieller Port kann funktionieren als:

- *Ziel (sink)* für Daten von IP-Multicast-Streams oder als
- *Quelle (source)* von Daten, die an mehrere IP-Multicast-Empfänger übertragen werden sollen.

INHALT

- Abschnitt 9.4.1.1, „Zielports (Sink) und Quellports (Source)“
- Abschnitt 9.4.1.2, „Beispiele für das Multicast-Streaming“

Abschnitt 9.4.1.1
Zielports (Sink) und Quellports (Source)

Ein serieller Port kann entweder als *Zielport (Sink)* und/oder als *Quellport (Source)* fungieren:

- **Zielport (Sink)**
  Ein Zielport empfängt Multicast-Pakete. Er meldet sich selbst für den Empfang von Multicast-Verkehr von einer IPv4-Adresse einer bekannten Multicast-Gruppe und eines UDP-Zielports an und leitet den Verkehr über die serielle Verbindung weiter. Der Verkehr wird von einem angeschalteten seriellen Gerät eines anderen Herstellers empfangen und verarbeitet.
- **Quellport (Source)**
  Ein Quellport erzeugt Multicast-Pakete. Er empfängt seriellen Verkehr von einem angeschalteten seriellen Gerät eines anderen Herstellers und packt diesen in Multicast-IPv4-Pakete. Jedem Paket wird eine bestimmte IPv4-Adresse einer Multicast-Gruppe, ein UDP-Zielport und ein UDP-Quellport zugewiesen.

Abschnitt 9.4.1.2
Beispiele für das Multicast-Streaming

Das serielle Multicast-Streaming kann auf unterschiedliche Arten bereitgestellt werden:

» Serielle Schnittstellen, die als "Sink"-Gerät für Multicast-Streams konfiguriert sind

Bei dieser Konfiguration kommt die Quelle der Multicast-Daten von den Ethernet-Netzwerk-Schnittstellen und wird an mehrere serielle "Sink"-Geräte übertragen. Der Vorteil dieses Szenarios besteht in der einfachen Konfiguration auf der Ethernet-Netzwerk-Seite. Statt anzugeben, an welchen seriellen Port über Unicast-Pakete gesendet werden soll, kann der Controller einen einzelnen Multicast-Stream an alle oder bestimmte verbundene serielle Geräte senden.

» Serielle Schnittstellen, die als "Source"-Geräte für Multicast-Streams konfiguriert sind

Bei dieser Konfiguration kommt die Quelle der Multicast-Daten vom seriellen Port und der Geräteseite und wird über einen Multicast-Stream an mehrere Ethernet-Schnittstellen gesendet. Der Vorteil dieses Szenarios besteht in der einfachen Konfiguration der hörenden Geräte. Es besteht eine geringere Notwendigkeit, die IP-Adressen der Schnittstellen zu beobachten, und hörende Geräte können einfach ersetzt werden, ohne sich Gedanken über ein Beibehalten derselben IP-Adresse machen zu müssen.

» Serielle Schnittstellen, die als "Source"- und "Sink"-Geräte für Multicast-Streams konfiguriert sind

Bei dieser Konfiguration werden die seriellen Daten an andere serielle Geräte weitergeleitet. Es besteht die Möglichkeit einer Übertragung an mehrere Ethernet-Schnittstellen über einen einzigen Multicast-Stream. Hierbei handelt es sich um eine Erweiterung der beiden vorstehenden Beispiele. Der Vorteil dieser Konfiguration besteht darin, einem seriellen "Source"-Gerät zu erlauben, Daten über ein Ethernet-Netzwerk an mehrere Empfänger zu senden, bei denen es sich entweder um einen anderen seriellen Port oder ein hörendes Gerät handelt.

Abschnitt 9.4.2
Serielles Multicast-Streaming konfigurieren

Um serielles Multicast-Streaming zu konfigurieren, gehen Sie wie folgt vor:

1. Fügen Sie das Rawsocket-Protokoll hinzu. Weitere Informationen finden Sie unter Abschnitt 9.2.3, „Hinzufügen eines Protokolls des seriellen Ports“.

2. Konfigurieren Sie den entfernten Host für die Kapselung von Rawsocket Serial über Multicast mit der Ziel-Multicast IP-Adresse, UDP-Port und den notwendigen Schnittstellen. Für weitere Informationen siehe Abschnitt 9.5.2, „Hinzufügen eines entfernten Hosts“ und Abschnitt 9.7.2, „Hinzufügen einer Schnittstelle des entfernten Hosts“.
3. Konfigurieren Sie den lokalen Port, die lokale Host-Multicast-IP und die lokalen Host-Schnittstelle(n) für die Entkapselung des/der Multicast-Streams in Rawsocket Serial. Für weitere Informationen siehe Abschnitt 9.6.2, „Hinzufügen eines lokalen Hosts“ und Abschnitt 9.8.2, „Hinzufügen einer lokalen Host-Schnittstelle“.
4. Überprüfen Sie, ob der Multicast-Verkehr an den ein- und abgehenden Schnittstellen sichtbar ist, indem Sie Folgendes eingeben:

```
traceserial
```

Abschnitt 9.4.3

Beispiel: Serielle Schnittstellen, die als "Sink"-Gerät für Multicast-Streams konfiguriert sind

Dieses Konfigurationsbeispiel zeigt Multicast-Nachrichten von der Gruppe 232.1.1.1, die an den UDP-Port 5001 geleitet werden und ser-1-1 von der Schnittstelle switch.0010 über Raw-Socket-Verbindungen erreichen. Nach dem Empfang dieser Nachrichten leitet Ser-1-1 die Daten an das serielle Gerät S1 weiter, mit dem es direkt verbunden ist.

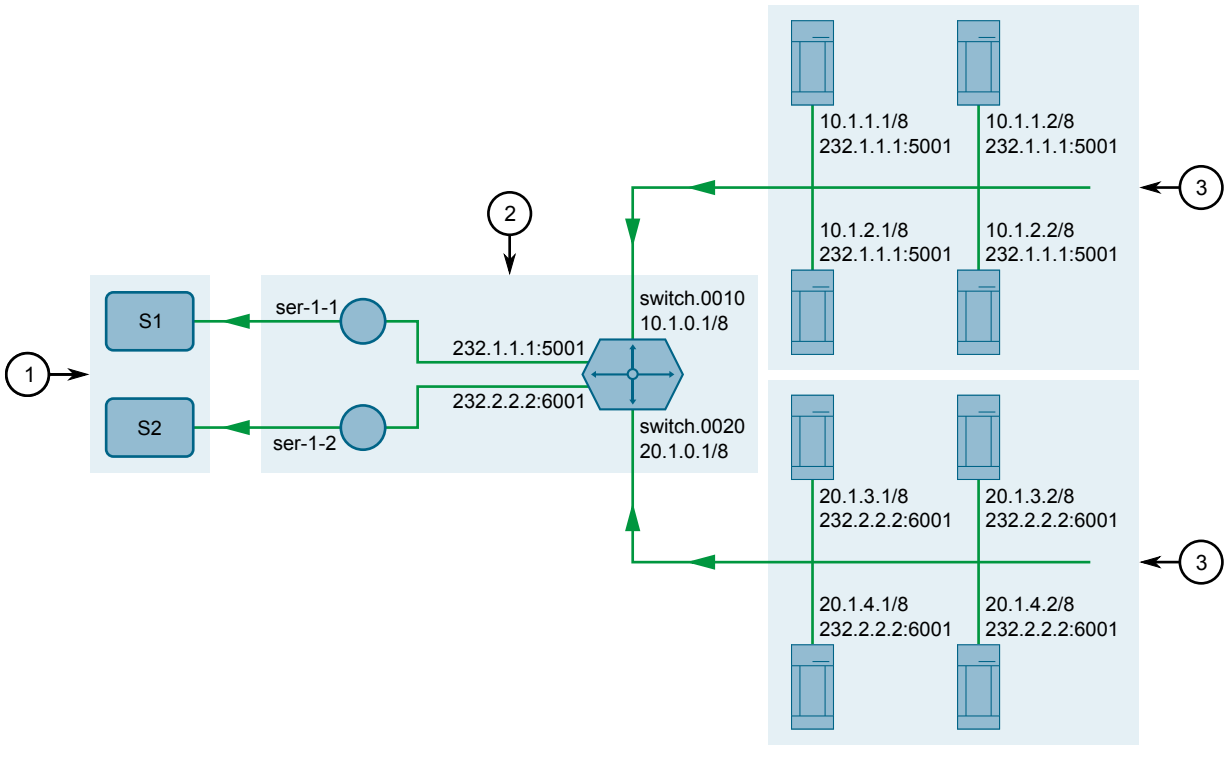


Abbildung 15: Topologie – Serielle Schnittstellen, die als "Sink"-Gerät für Multicast-Ströme konfiguriert sind

1. Serielle Geräte **2.** Sink-Gerät (Gerät der Serie RUGGEDCOM RX1400) **3.** Ethernet-Netzwerk-Schnittstellen

Schritt 1: Konfigurieren Sie ser-1-1

1. Konfigurieren Sie die IP-Adressen für die Schnittstellen (switch.0010 und switch.0020). Weitere Informationen finden Sie unter Abschnitt 7.1.3.2, „Eine IPv4-Adresse hinzufügen“.
2. Erstellen Sie eine Raw-Socket-Verbindung für ser-1-1:

   ```
   interface serial serport 1 protocols rawsocket
   ```

   Weitere Informationen finden Sie unter Abschnitt 9.2.3, „Hinzufügen eines Protokolls des seriellen Ports“.
3. Setzen Sie das Raw Socket des lokalen Ports auf 5001:

   ```
   setrawsocket local-port 5001
   ```

   Weitere Informationen finden Sie unter Abschnitt 9.2.6, „Konfigurieren des Raw-Socket-Protokolls“.
4. Setzen Sie das Transportverfahren auf *UDP*:

   ```
   setrawsocket transport udp
   ```

   Weitere Informationen finden Sie unter Abschnitt 9.2.6, „Konfigurieren des Raw-Socket-Protokolls“.
5. Setzen Sie die Multicast-Gruppe für den lokalen Host auf 232.1.1.1:

   ```
   setrawsocket local-host 232.1.1.1
   ```

   Weitere Informationen finden Sie unter Abschnitt 9.6.2, „Hinzufügen eines lokalen Hosts“.
6. Stellen Sie *switch.0010* als die Schnittstelle für den lokalen Host ein:

   ```
   interface switch.0010
   ```

   Weitere Informationen finden Sie unter Abschnitt 9.8.2, „Hinzufügen einer lokalen Host-Schnittstelle“.
7. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Schritt 2: Konfigurieren Sie ser-1-2

1. Erstellen Sie eine Raw-Socket-Verbindung für ser-1-2:

   ```
   interface serial serport 2 protocols rawsocket
   ```

   Weitere Informationen finden Sie unter Abschnitt 9.2.3, „Hinzufügen eines Protokolls des seriellen Ports“.
2. Setzen Sie den lokalen Port für Raw Socket auf 6001:

   ```
   setrawsocket local-port 6001
   ```

   Weitere Informationen finden Sie unter Abschnitt 9.2.6, „Konfigurieren des Raw-Socket-Protokolls“.
3. Setzen Sie das Transportverfahren für Raw Socket auf *UDP*:

   ```
   setrawsocket transport udp
   ```

   Weitere Informationen finden Sie unter Abschnitt 9.2.6, „Konfigurieren des Raw-Socket-Protokolls“.
4. Setzen Sie die Multicast-Gruppe für den lokalen Host auf 232.2.2.2:

   ```
   setrawsocket local-host 232.2.2.2
   ```

   Weitere Informationen finden Sie unter Abschnitt 9.6.2, „Hinzufügen eines lokalen Hosts“.
5. Stellen Sie *switch.0020* als die Schnittstelle für den lokalen Host ein:

   ```
   interface switch.0020
   ```

Weitere Informationen finden Sie unter Abschnitt 9.8.2, „Hinzufügen einer lokalen Host-Schnittstelle“.

6. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.
7. Überprüfen Sie die Konfiguration, indem Sie Folgendes eingeben:

```
traceserial
```

» Beispiel einer finalen Konfiguration

Konfiguration von ser-1-1

```
serial serport 1
  no alias
  protocols rawsocket
   setrawsocket local-port 5001
   setrawsocket transport udp
   setrawsocket local-host 232.1.1.1
    interface switch.0010
```

ser-1-2 Configuration

```
serial serport 2
  no alias
  protocols rawsocket
   setrawsocket local-port 6001
   setrawsocket transport udp
   setrawsocket local-host 232.2.2.2
    interface switch.0020
```

Abschnitt 9.4.4

Beispiel: Für Multicast-Streams als stromliefernd konfigurierte serielle Schnittstellen

In diesem Konfigurationsbeispiel wird gezeigt, dass ser-1-1 Daten über die Leitung von S1 empfängt, dann mehrere entfernte Raw-Socket-Host-Schnittstellen erstellt, um die Daten an beide Schnittstellen, switch.0010 und switch.0020, zu senden. Diese Daten werden dann als Multicast-Pakete verpackt und an Zielgruppe 232.1.1.1 und Ziel-UDP-Port 5001 gesendet.

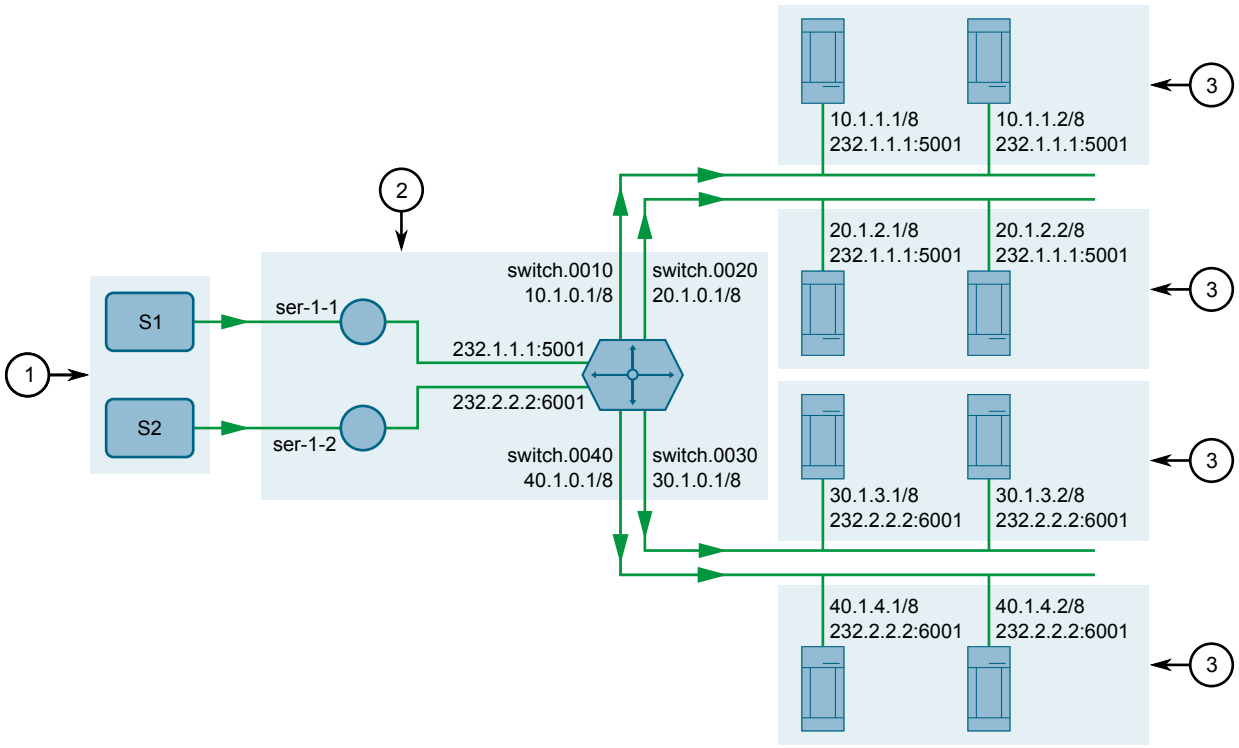


Abbildung 16: Topologie - Für Multicast-Streams als stromliefernd konfigurierte serielle Schnittstellen

1. Serielle Geräte **2.** Stromlieferndes Gerät (Gerät der RUGGEDCOM Serie RX1400) **3.** Listener

» Schritt 1: ser-1-1 konfigurieren

1. Konfigurieren Sie IP-Adressen für die Schnittstellen (switch.0010, switch.0020, switch.0030 und switch.0040). Weitere Informationen finden Sie unter Abschnitt 7.1.3.2, „Eine IPv4-Adresse hinzufügen“.
2. Erstellen Sie eine Raw-Socket-Verbindung für ser-1-1:

   ```
   interface serial serport 1 protocols rawsocket
   ```

   Weitere Informationen finden Sie unter Abschnitt 9.2.3, „Hinzufügen eines Protokolls des seriellen Ports“.
3. Setzen Sie den Raw-Socket des lokalen Ports auf 10001:

   ```
   setrawsocket local-port 10001
   ```

   Weitere Informationen finden Sie unter Abschnitt 9.2.6, „Konfigurieren des Raw-Socket-Protokolls“.
4. Stellen Sie für das Transportverfahren *UDP* ein:

   ```
   setrawsocket transport udp
   ```

   Weitere Informationen finden Sie unter Abschnitt 9.2.6, „Konfigurieren des Raw-Socket-Protokolls“.
5. Setzen Sie die Multicast-Gruppe für den lokalen Host auf 232.1.1.1 und den UDP-Zielport auf 5001:

   ```
   setrawsocket remote-host 232.1.1.1 5001
   ```

   Weitere Informationen finden Sie unter Abschnitt 9.5.2, „Hinzufügen eines entfernten Hosts“.
6. Stellen Sie *switch.0010* und *switch.0020* als die Schnittstellen für den entfernten Host ein:

```
interface switch.0010
interface switch.0020
```

Weitere Informationen finden Sie unter Abschnitt 9.7.2, „Hinzufügen einer Schnittstelle des entfernten Hosts“.

7. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Schritt 2: ser-1-2 konfigurieren

1. Erstellen Sie eine Raw-Socket-Verbindung für ser-1-2:

```
interface serial serport 2 protocols rawsocket
```

Weitere Informationen finden Sie unter Abschnitt 9.2.3, „Hinzufügen eines Protokolls des seriellen Ports“.

2. Setzen Sie den Raw-Socket des lokalen Ports auf 10002:

```
setrawsocket local-port 10002
```

Weitere Informationen finden Sie unter Abschnitt 9.2.6, „Konfigurieren des Raw-Socket-Protokolls“.

3. Stellen Sie für das Transportverfahren *UDP* ein:

```
setrawsocket transport udp
```

Weitere Informationen finden Sie unter Abschnitt 9.2.6, „Konfigurieren des Raw-Socket-Protokolls“.

4. Setzen Sie die Multicast-Gruppe für den lokalen Host auf 232.2.2.2 und den UDP-Zielport auf 6001:

```
setrawsocket local-host 232.2.2.2 6001
```

Weitere Informationen finden Sie unter Abschnitt 9.6.2, „Hinzufügen eines lokalen Hosts“.

5. Stellen Sie *switch.0030* und *switch.0040* als die Schnittstellen für den entfernten Host ein:

```
interface switch.0030
interface switch.0040
```

Weitere Informationen finden Sie unter Abschnitt 9.7.2, „Hinzufügen einer Schnittstelle des entfernten Hosts“.

6. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.
7. Überprüfen Sie die Konfiguration durch folgende Eingabe:

```
traceserial
```

Beispiel für die endgültige Konfiguration

Konfiguration des seriellen Ports 1

```
serial serport 1
  no alias
  protocols rawsocket
   setrawsocket local-port 10001
   setrawsocket transport udp
   setrawsocket remote-host 232.1.1.1 5001
    interface switch.0010
    !
```

```
    interface switch.0020
```

Serial Port 2 Configuration

```
serial serport 2
  no alias
  protocols rawsocket
   setrawsocket local-port 10002
   setrawsocket transport udp
   setrawsocket remote-host 232.2.2.2 6001
    interface switch.0030
    !
    interface switch.0040
```

Abschnitt 9.4.5

Beispiel: Für Multicast-Streams als stromliefernd und stromziehend konfigurierte serielle Schnittstellen

In diesem Konfigurationsbeispiel wird gezeigt, dass ser-1-1 Daten über die Leitung von S1 empfängt, dann mehrere Raw-Socket-Verbindungen erstellt, um die Daten an beide Schnittstellen, switch.0010 und switch.0020, zu senden. Diese Daten werden dann als Multicast-Pakete verpackt und an Zielgruppe 232.1.1.1 und Ziel-UDP-Port 5001 gesendet. Zusätzlich leitet ser-1-1 denselben Datenstrom an ser-1-2 weiter, der die Daten dann an S2 sendet.

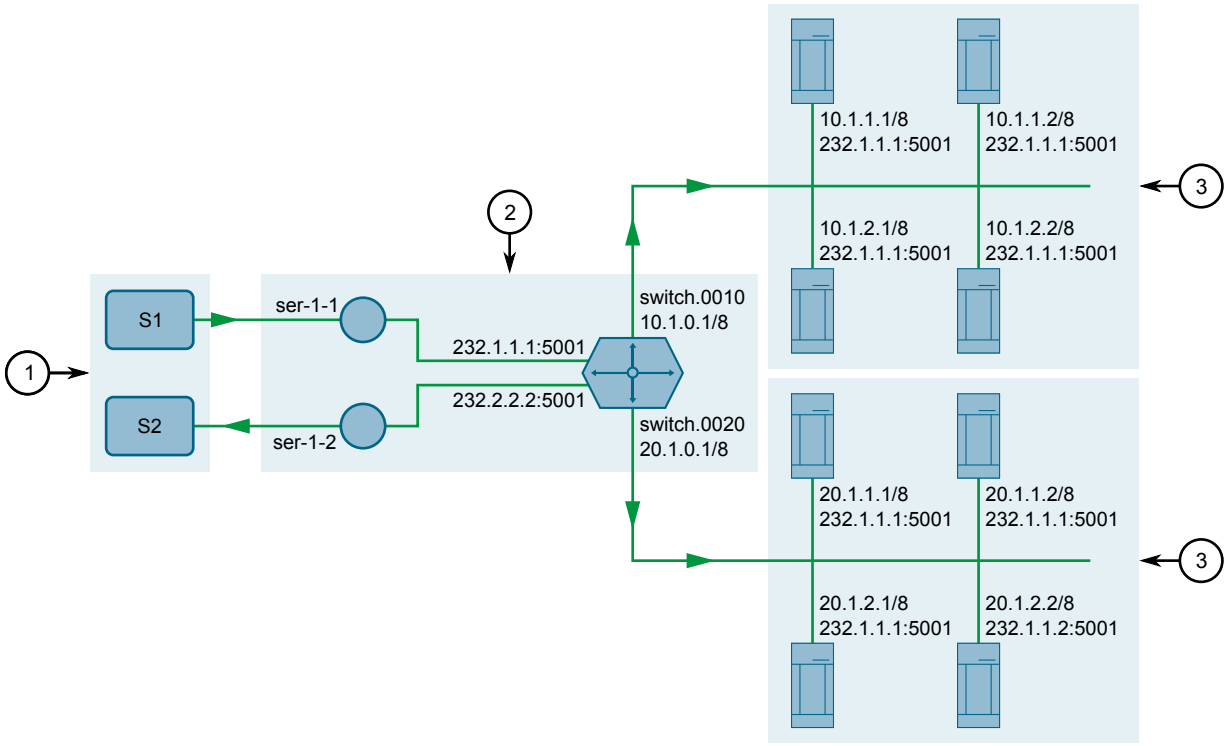


Abbildung 17: Topologie - Für Multicast-Streams als stromliefernd und stromziehend konfigurierte serielle Schnittstellen

1. Serielle Geräte **2.** Stromlieferndes und stromziehendes Gerät (Gerät der RUGGEDCOM Serie RX1400) **3.** Listener **4.** Ethernet-Netzwerkschnittstellen

» ser-1-1 und ser-1-2 konfigurieren

1. Konfigurieren Sie IP-Adressen für die Schnittstellen (switch.0010 und switch.0020). Weitere Informationen finden Sie unter Abschnitt 7.1.3.2, „Eine IPv4-Adresse hinzufügen“.
2. Erstellen Sie eine Raw-Socket-Verbindung für ser-1-1:

   ```
   interface serial serport 1 protocols rawsocket
   ```

   Weitere Informationen finden Sie unter Abschnitt 9.2.3, „Hinzufügen eines Protokolls des seriellen Ports“.
3. Setzen Sie den Raw-Socket des lokalen Ports auf 10001:

   ```
   setrawsocket local-port 10001
   ```

   Weitere Informationen finden Sie unter Abschnitt 9.2.6, „Konfigurieren des Raw-Socket-Protokolls“.
4. Stellen Sie für das Transportverfahren *UDP* ein:

   ```
   setrawsocket transport udp
   ```

   Weitere Informationen finden Sie unter Abschnitt 9.2.6, „Konfigurieren des Raw-Socket-Protokolls“.
5. Setzen Sie die Multicast-Gruppe für den entfernten Host auf 232.1.1.1 und den UDP-Zielport auf 5001:

   ```
   setrawsocket remote-host 232.1.1.1 5001
   ```

Weitere Informationen finden Sie unter Abschnitt 9.5.2, „Hinzufügen eines entfernten Hosts“.

6. Stellen Sie *switch.0010* und *switch.0020* als die Schnittstellen für den entfernten Host ein:

```
interface switch.0010
interface switch.0020
```

Weitere Informationen finden Sie unter Abschnitt 9.7.2, „Hinzufügen einer Schnittstelle des entfernten Hosts“.

7. Aktivieren Sie Loopback für den entfernten Host:

```
loopback true
```

Weitere Informationen finden Sie unter Abschnitt 9.6.2, „Hinzufügen eines lokalen Hosts“.

8. Erstellen Sie eine Raw-Socket-Verbindung für ser-1-2:

```
interface serial serport 2 protocols rawsocket
```

Weitere Informationen finden Sie unter Abschnitt 9.2.3, „Hinzufügen eines Protokolls des seriellen Ports“.

9. Setzen Sie den Raw-Socket des lokalen Ports auf 5001. Dies muss der gleiche wie der UDP-Zielport des für ser-1-1 konfigurierten entfernten Multicast-Hosts sein:

```
setrawsocket local-port 5001
```

Weitere Informationen finden Sie unter Abschnitt 9.6.2, „Hinzufügen eines lokalen Hosts“.

10. Stellen Sie für das Transportverfahren *UDP* ein:

```
setrawsocket transport udp
```

Weitere Informationen finden Sie unter Abschnitt 9.2.6, „Konfigurieren des Raw-Socket-Protokolls“.

11. Setzen Sie die Multicast-Gruppe für den lokalen Host auf 232.1.1.1. Dies muss die gleiche wie die Multicast-Zielgruppe des für ser-1-1 konfigurierten entfernten Multicast-Hosts sein.

```
setrawsocket local-host 232.1.1.1
```

Weitere Informationen finden Sie unter Abschnitt 9.6.2, „Hinzufügen eines lokalen Hosts“.

12. Aktivieren Sie Loopback für den lokalen Host:

```
loopback true
```

Weitere Informationen finden Sie unter Abschnitt 9.6.2, „Hinzufügen eines lokalen Hosts“.

13. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.
14. Überprüfen Sie die Konfiguration durch folgende Eingabe:

```
traceserial
```

» Beispiel für die endgültige Konfiguration

Konfiguration des seriellen Ports 1

```
serial serport 1
  no alias
  protocols rawsocket
   setrawsocket local-port 10001
   setrawsocket transport udp
   setrawsocket remote-host 232.1.1.1 5001
    loopback true
```

```
    interface switch.0010
    !
    interface switch.0020
```

Serial Port 2 Configuration

```
serial serport 2
  no alias
  protocols rawsocket
   setrawsocket local-port 5001
   setrawsocket transport udp
   setrawsocket local-host 232.1.1.1
    loopback true
```

Abschnitt 9.5

Entfernte Hosts verwalten

Entfernte Hosts sind erforderlich, wenn das UDP-Transportprotokoll für das Raw-Socket-Protokoll ausgewählt ist.

INHALT

- Abschnitt 9.5.1, „Eine Liste der entfernten Hosts anzeigen“
- Abschnitt 9.5.2, „Hinzufügen eines entfernten Hosts“
- Abschnitt 9.5.3, „Einen entfernten Host löschen“

Abschnitt 9.5.1

Eine Liste der entfernten Hosts anzeigen

Um eine Liste der entfernten Hosts, die für einen seriellen Port mit Raw-Socket-Protokoll konfiguriert sind, anzuzeigen, geben Sie Folgendes ein:

```
show running-config interface serial protocols rawsocket setrawsocket remote-host
```

Falls Hosts konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config interface serial protocols rawsocket setrawsocket remote-host interface
 serial serport 1 no alias protocols rawsocket setrawsocket local-port 30001 setrawsocket transport
 udp setrawsocket remote-host 1.1.1.2 60001 ! setrawsocket remote-host 232.1.1.1 60001 interface
 switch.0010 ! ! ! ! ! !
```

Falls keine entfernten Hosts konfiguriert wurden, fügen Sie je nach Bedarf Hosts hinzu. Weitere Informationen finden Sie unter Abschnitt 9.5.2, „Hinzufügen eines entfernten Hosts“.

Abschnitt 9.5.2

Hinzufügen eines entfernten Hosts

Um mittels Raw-Socket-Protokoll einen entfernten Host für einen seriellen Port hinzuzufügen, gehen Sie wie folgt vor:

HINWEIS
Es sind maximal zwei dezentrale Multicast-Hosteinträge pro serieller Schnittstelle zulässig.

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den entfernten Host hinzu, indem Sie Folgendes eingeben:

```
interface serial serport port protocols rawsocket setrawsocket remote-host address remote-port
```

Erläuterung:

- *port* ist die Nummer des Ports (oder eine Liste von Ports, wenn sie in einem Port-Trunk gebündelt sind) für das Modul.
- *address* ist die IP-Adresse für den entfernten Host oder die IP-Adresse einer Multicast-Gruppe, für die die Schnittstelle als Quelle dient.
- *remote-port* ist die Portnummer des entfernten Hosts

3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
{ remote-ip }	**Zusammenfassung:** Eine Zeichenkette mit 7 bis 15 Zeichen oder eine Zeichenkette mit 6 bis 40 Zeichen Die IP-Adresse des entfernten Hosts oder der Multicast-Zielgruppe.
{ remote-port }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 1 und 65535 Der Transportport des entfernten Hosts oder der Multicast-Zielgruppe.
loopback	**Zusammenfassung:** { true, false } **Standard:** false Ermöglicht die Übertragung an die Loopback-Schnittstelle mit der IP-Adresse der Multicast-Zielgruppe und dem entfernten Port. Durch Abgleich lokaler Hosts mit aktiviertem Loopback werden die übertragenen Daten empfangen.

4. [Optional] Fügen Sie eine Schnittstelle des entfernten Hosts hinzu. Weitere Informationen finden Sie unter Abschnitt 9.7.2, „Hinzufügen einer Schnittstelle des entfernten Hosts“.
5. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 9.5.3

Einen entfernten Host löschen

Um einen entfernten Host zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den entfernten Host, indem Sie Folgendes eingeben:

```
no interface serial serport port protocols rawsocket setrawsocket remote-host address remote-port
```

Erläuterung:

- *port* ist die Nummer des Ports (oder eine Liste von Ports, wenn sie in einem Port-Trunk gebündelt sind) für das Modul.
- *address* ist die IP-Adresse des entfernten Hosts
- *remote-port* ist die Portnummer des entfernten Hosts

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 9.6
Lokale Hosts verwalten

Lokale Hosts sind erforderlich, wenn das UDP-Transportprotokoll ausgewählt ist und Multicast-Streams für das Raw-Socket-Protokoll empfangen werden sollen.

INHALT

- Abschnitt 9.6.1, „Eine Liste der lokalen Hosts anzeigen“
- Abschnitt 9.6.2, „Hinzufügen eines lokalen Hosts“
- Abschnitt 9.6.3, „Eine lokalen Host löschen“

Abschnitt 9.6.1
Eine Liste der lokalen Hosts anzeigen

Um eine Liste der lokalen Hosts, die für einen seriellen Port mit Raw-Socket-Protokoll konfiguriert sind, anzuzeigen, geben Sie Folgendes ein:

```
show running-config interface serial protocols rawsocket setrawsocket local-host
```

Falls Hosts konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config interface serial protocols rawsocket setrawsocket local-host
interface
 serial serport 1
  protocols rawsocket
   setrawsocket local-host 172.30.151.11 62011
   !
   setrawsocket local-host 172.30.151.22 63000
   !
  !
 !
!
```

Falls keine lokalen Hosts konfiguriert wurden, fügen Sie je nach Bedarf Hosts hinzu. Weitere Informationen finden Sie unter Abschnitt 9.6.2, „Hinzufügen eines lokalen Hosts“.

Abschnitt 9.6.2
Hinzufügen eines lokalen Hosts

HINWEIS
Es sind maximal zwei lokale Multicast-Hosteinträge pro serieller Schnittstelle zulässig.

Um einen lokalen Host für einen seriellen Port mit Raw-Socket-Protokoll hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.

2. Fügen Sie den lokalen Host hinzu, indem Sie Folgendes eingeben:

```
interface serial serport port protocols rawsocket setrawsocket local-host address local-port
```

Erläuterung:

- *port* ist die Nummer des Ports (oder eine Liste von Ports, wenn sie in einem Port-Trunk gebündelt sind) für das Modul.
- *address* ist eine IP-Adresse einer Multicast-Gruppe, für die die Schnittstelle als "Sink" dient
- *local-port* ist die Portnummer des lokalen Hosts

3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

HINWEIS
Konfigurieren Sie lokale Ports kleiner als 32768 oder größer als 61000, da Ports zwischen diesem Bereich nach dem Zufallsprinzip vom System verwendet werden.

Parameter	Beschreibung
{ multicast-ip }	**Zusammenfassung:** Eine Zeichenkette mit 7 bis 15 Zeichen Die IP-Adresse der Multicast-Quellgruppe (2xx.xxx.xxx.xxx) des lokalen Hosts. Der empfangende UDP-Port für die Multicast-Gruppe verwendet implizit die für den seriellen Port definierte lokale Portnummer.
loopback	**Zusammenfassung:** { true, false } **Standard:** false Ermöglicht den Empfang von der Loopback-Schnittstelle mit der IP-Adresse der Multicast-Quellgruppe und der für den seriellen Port definierten lokalen Portnummer. Erfordert den Abgleich lokaler Hosts mit aktiviertem Loopback, damit Daten über Loopback empfangen werden können.

4. Fügen Sie eine lokale Host-Schnittstelle hinzu. Weitere Informationen finden Sie unter Abschnitt 9.8.2, „Hinzufügen einer lokalen Host-Schnittstelle“.
5. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 9.6.3
Eine lokalen Host löschen

Um einen lokalen Host zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den lokalen Host, indem Sie Folgendes eingeben:

```
no interface serial serport port protocols rawsocket setrawsocket local-host address local-port
```

Erläuterung:

- *port* ist die Nummer des Ports (oder eine Liste von Ports, wenn sie in einem Port-Trunk gebündelt sind) für das Modul.
- *address* ist die IP-Adresse für den lokalen Host
- *local-port* ist die Portnummer des lokalen Hosts

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 9.7
Entfernte Host-Schnittstellen verwalten

Entfernte Host-Schnittstellen sind erforderlich, wenn das UDP-Transportprotokoll für das Raw-Socket-Protokoll ausgewählt ist und der entfernte Host ein Multicast-Stream ist.

INHALT

- Abschnitt 9.7.1, „Anzeigen einer Liste der dezentralen Host-Schnittstellen“
- Abschnitt 9.7.2, „Hinzufügen einer Schnittstelle des entfernten Hosts“
- Abschnitt 9.7.3, „Eine Schnittstelle des entferntem Hosts löschen“

Abschnitt 9.7.1
Anzeigen einer Liste der dezentralen Host-Schnittstellen

Um eine Liste der dezentralen Host-Schnittstellen anzuzeigen, die für einen seriellen Port mit Raw-Socket-Protokoll konfiguriert wurden, geben Sie Folgendes ein:

```
show running-config interface serial serport port protocols rawsocket setrawsocket remote-host remote-host interface
```

Erläuterung:

- *port* ist die Nummer des Ports (oder eine Liste von Ports, wenn sie in einem Port-Trunk gebündelt sind) für das Modul.
- *remote-host* ist der entfernte Host

Falls Schnittstellen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config interface serial serport 1 protocols rawsocket setrawsocket remote-host
 224.1.2.1 interface interface serial serport 1 protocols rawsocket setrawsocket remote-host 224.1.2.1
 interface ge-4-4 ! ! ! ! !
```

Falls keine dezentralen Host-Schnittstellen konfiguriert wurden, fügen Sie je nach Bedarf Schnittstellen hinzu. Weitere Informationen finden Sie unter Abschnitt 9.7.2, „Hinzufügen einer Schnittstelle des entfernten Hosts“.

Abschnitt 9.7.2
Hinzufügen einer Schnittstelle des entfernten Hosts

HINWEIS
Es sind maximal zehn Schnittstellen für jeden entfernten Host zulässig.

Um mittels Raw-Socket-Protokoll eine entfernte Host-Schnittstelle für einen seriellen Port hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu:

   ```
   interface serial serport port protocols rawsocket setrawsocket remote-host remote-host interface
   ```

Erläuterung:

- *port* ist die Nummer des Ports (oder eine Liste von Ports, wenn sie in einem Port-Trunk gebündelt sind) für das Modul.
- *remote-host* ist der entfernte Host

3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
{ name }	**Zusammenfassung:** Eine Zeichenkette Der Name der übertragenden Schnittstelle für die IP-Adresse der Multicast-Zielgruppe und den entfernten Port.

4. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 9.7.3

Eine Schnittstelle des entferntem Hosts löschen

Um eine Schnittstelle des entferntem Hosts zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den entfernten Host, indem Sie Folgendes eingeben:

```
no interface serial serport port protocols rawsocket setrawsocket remote-host interface interface name
```

Erläuterung:

- *port* ist die Nummer des Ports (oder eine Liste von Ports, wenn sie in einem Port-Trunk gebündelt sind) für das Modul.
- *remote-host* ist der entfernte Host
- *interface name* ist die Bezeichnung der Schnittstelle

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 9.8

Lokale Host-Schnittstellen verwalten

Lokale Host-Schnittstellen sind erforderlich, wenn das UDP-Transportprotokoll für das Raw-Socket-Protokoll ausgewählt ist und ein lokaler Host konfiguriert ist.

INHALT

- Abschnitt 9.8.1, „Anzeigen einer Liste der lokalen Host-Schnittstellen“
- Abschnitt 9.8.2, „Hinzufügen einer lokalen Host-Schnittstelle“
- Abschnitt 9.8.3, „Eine lokale Host-Schnittstelle löschen“

Abschnitt 9.8.1
Anzeigen einer Liste der lokalen Host-Schnittstellen

Um eine Liste der lokalen Host-Schnittstellen anzuzeigen, die für einen seriellen Port mit Raw-Socket-Protokoll konfiguriert wurden, geben Sie Folgendes ein:

```
show running-config interface serial serport port protocols rawsocket setrawsocket local-host local-host interface
```

Erläuterung:

- *port* ist die Nummer des Ports (oder eine Liste von Ports, wenn sie in einem Port-Trunk gebündelt sind) für das Modul.
- *local-host* ist der lokale Host

Falls Schnittstellen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config interface serial serport 1 protocols rawsocket setrawsocket local-host
 224.1.2.1 interface
interface
 serial serport 1
  protocols rawsocket
   setrawsocket local-host 224.1.2.1
    interface ge-4-4
    !
   !
  !
 !
!
```

Falls keine lokalen Host-Schnittstellen konfiguriert wurden, fügen Sie je nach Bedarf Schnittstellen hinzu. Weitere Informationen finden Sie unter Abschnitt 9.8.2, „Hinzufügen einer lokalen Host-Schnittstelle“.

Abschnitt 9.8.2
Hinzufügen einer lokalen Host-Schnittstelle

HINWEIS
Es sind maximal zwei Schnittstellen für jeden lokalen Host zulässig.

Um eine lokale Host-Schnittstelle für einen seriellen Port mit Raw-Socket-Protokoll hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu:

   ```
   interface serial serport port protocols rawsocket setrawsocket local-host local-host interface
   ```

   Erläuterung:

   - *port* ist die Nummer des Ports (oder eine Liste von Ports, wenn sie in einem Port-Trunk gebündelt sind) für das Modul.
   - *local-host* ist der lokale Host
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
{ name }	**Zusammenfassung:** Eine Zeichenkette Der Name der empfangenden Schnittstelle für die IP-Adresse der Multicast-Quellgruppe und die für den seriellen Port definierten lokalen Portnummer.

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 9.8.3
Eine lokale Host-Schnittstelle löschen

Um eine lokale Host-Schnittstelle zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den lokalen Host, indem Sie Folgendes eingeben:

```
no interface serial serport port protocols rawsocket setrawsocket local-host interface interface name
```

   Erläuterung:

   - *`port`* ist die Nummer des Ports (oder eine Liste von Ports, wenn sie in einem Port-Trunk gebündelt sind) für das Modul.
   - *`local-host`* ist er lokale Host
   - *`interface name`* ist die Bezeichnung der Schnittstelle
3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

10 Wireless

Dieses Kapitel beschreibt, wie Sie die Wireless-Schnittstellen und -Dienstprogramme in RUGGEDCOM ROX II konfigurieren und verwalten können.

HINWEIS
Für manche Wireless-Funktionen muss das Gerät mit einem speziellen Line-Modul ausgestattet sein.

INHALT

- Abschnitt 10.1, „Die WLAN-Schnittstelle verwalten“
- Abschnitt 10.2, „Mobilfunkmodem-Schnittstellen verwalten“
- Abschnitt 10.3, „AT-Befehle ausführen“
- Abschnitt 10.4, „Herstellen einer Verbindung als PPP-Client“
- Abschnitt 10.5, „Mobilfunkmodem-Profile verwalten“
- Abschnitt 10.6, „Das LTE-Modem verwalten“

Abschnitt 10.1

Die WLAN-Schnittstelle verwalten

Dieser Abschnitt beschreibt, wie Sie eine Schnittstelle zu einem WLAN (Wireless Local Area Network) konfigurieren können. Das Gerät kann als Zugangspunkt (Access Point) oder Client konfiguriert werden.

INHALT

- Abschnitt 10.1.1, „Aktivieren und Konfigurieren der WLAN-Schnittstelle“
- Abschnitt 10.1.2, „WAP (Wireless Access Points) verwalten“
- Abschnitt 10.1.3, „WLAN-Clients verwalten“
- Abschnitt 10.1.4, „Beispiel: Konfigurieren eines WLAN mit einer Firewall“

Abschnitt 10.1.1

Aktivieren und Konfigurieren der WLAN-Schnittstelle

Um die Schnittstelle zu einem WLAN zu aktivieren und zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Aktivieren Sie die WLAN-Schnittstelle, indem Sie Folgendes eingeben:

```
interface wlan wlanport 1 enabled
```

3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

WICHTIG!
Der `country` Parameter definiert den Kanal (oder die Funkfrequenz), die vom Zugriffspunkt geändert werden kann. In einigen Ländern ist die Nutzung bestimmter Kanäle eingeschränkt. Stellen Sie sicher, dass die Kanalauswahl den regionalen Anforderungen entspricht.

HINWEIS
Der `country` Parameter ist nicht auf Geräten konfigurierbar, die nur für den Einsatz in den Vereinigten Staaten zugelassen sind.

Parameter	Beschreibung
link-alarms	**Zusammenfassung:** { true, false } **Standard:** true Das Deaktivieren von Link-Alarmen („link-alarms") verhindert, dass Alarme und "LinkUp"- und "LinkDown"-SNMP-Traps für diese Schnittstelle versendet werden. Link-Alarme können für das gesamte System auch unter "admin / alarm-cfg" verwaltet werden.
alias { alias }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 64 Zeichen Der SNMP-Aliasname der Schnittstelle.
name { name }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 15 Zeichen Der spezifische Name der Schnittstelle.
country { country }	**Zusammenfassung:** { Afghanistan, Åland Islands, Albania, Algeria, American Samoa, Andorra, Angola, Anguilla, Antarctica, Antigua and Barbuda, Argentina, Armenia, Aruba, Australia, Austria, Azerbaijan, Bahamas, Bahrain, Bangladesh, Barbados, Belarus, Belgium, Belize, Benin, Bermuda, Bhutan, Bolivia, Bonaire, Bosnia and Herzegovina, Botswana, Bouvet Island, Brazil, British Indian Ocean Territory, Brunei Darussalam, Bulgaria, Burkina Faso, Burundi, Cambodia, Cameroon, Canada, Cape Verde, Cayman Islands, Central African Republic, Chad, Chile, China, Christmas Island, Cocos (Keeling) Islands, Colombia, Comoros, Congo, Cook Islands, Costa Rica, Côte d'Ivoire, Croatia, Cuba, Curaçao, Cyprus, Czech Republic, Denmark, Djibouti, Dominica, Dominican Republic, Ecuador, Egypt, El Salvador, Equatorial Guinea, Eritrea, Estonia, Ethiopia, Falkland Islands (Malvinas), Faroe Islands, Fiji, Finland, France, French Guiana, French Polynesia, French Southern Territories, Gabon, Gambia, Georgia, Germany, Ghana, Gibraltar, Greece, Greenland, Grenada, Guadeloupe, Guam, Guatemala, Guernsey, Guinea, Guinea-Bissau, Guyana, Haiti, Heard Island and McDonald Islands, Holy See (Vatican City State), Honduras, Hong Kong, Hungary, Iceland, India, Indonesia, Iran, Iraq, Ireland, Isle of Man, Israel, Italy, Jamaica, Japan, Jersey, Jordan, Kazakhstan, Kenya, Kiribati, Korea, Kuwait, Kyrgyzstan, Lao People's Democratic Republic, Latvia, Lebanon, Lesotho, Liberia, Libya, Liechtenstein, Lithuania, Luxembourg, Macao, Macedonia, Madagascar, Malawi, Malaysia, Maldives, Mali, Malta, Marshall Islands, Martinique, Mauritania, Mauritius, Mayotte, Mexico, Micronesia, Moldova, Monaco, Mongolia, Montenegro, Montserrat, Morocco, Mozambique, Myanmar, Namibia, Nauru, Nepal, Netherlands, New Caledonia, New Zealand, Nicaragua, Niger, Nigeria, Niue, Norfolk Island, Northern Mariana Islands, Norway, Oman, Pakistan, Palau, Palestine, Panama, Papua New Guinea, Paraguay, Peru, Philippines, Pitcairn, Poland, Portugal, Puerto Rico, Qatar, Réunion, Romania, Russian Federation, Rwanda, Saint Barthélemy, Saint Helena, Saint Kitts and Nevis, Saint Lucia, Saint Martin (French part), Saint Pierre and Miquelon, Saint Vincent and the Grenadines, Samoa, San Marino, Sao Tome and Principe, Saudi Arabia, Senegal, Serbia, Seychelles, Sierra Leone, Singapore, Sint Maarten (Dutch part), Slovakia, Slovenia, Solomon Islands, Somalia, South Africa, South Georgia and the South Sandwich Islands, South Sudan, Spain, Sri Lanka, Sudan, Suriname, Svalbard and Jan Mayen, Swaziland, Sweden, Switzerland, Syrian Arab Republic, Taiwan, Tajikistan, Tanzania, Thailand, Timor-Leste, Togo, Tokelau, Tonga, Trinidad and Tobago, Tunisia, Turkey, Turkmenistan, Turks and Caicos Islands, Tuvalu, Uganda, Ukraine, United Arab Emirates, United Kingdom, United States, United States Minor Outlying Islands, Uruguay,

Parameter	Beschreibung
	Uzbekistan, Vanuatu, Venezuela, Viet Nam, Virgin Islands, Wallis and Futuna, Western Sahara, Yemen, Zambia, Zimbabwe } **Standard:** United States Das Land, in dem Zugangspunkt und Client aktiv sind.

4. Falls das Gerät als Zugangspunkt agiert, fügen Sie einen oder mehrere Service Set Identifier bzw. SSIDs hinzu. Weitere Informationen finden Sie unter Abschnitt 10.1.2.4, „Hinzufügen eines Wireless Access Point“.
5. Falls das Gerät als Client agiert, fügen Sie einen oder mehrere Aliase hinzu. Weitere Informationen finden Sie unter Abschnitt 10.1.3.3, „Hinzufügen eines WLAN-Clients“.
6. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 10.1.2

WAP (Wireless Access Points) verwalten

Dieser Abschnitt beschreibt, wie Sie das Gerät als WAP (Wireless Access Point) in einem WLAN konfigurieren können.

WICHTIG!
Wenn das Gerät als WAP aktiviert werden soll, stellen Sie sicher, dass der WLAN-Client deaktiviert ist.

WICHTIG!
Es können nicht mehr als zwei WAPs gleichzeitig aktiviert sein.

INHALT

- Abschnitt 10.1.2.1, „Eine Liste der Wireless Access Points (WAP) anzeigen“
- Abschnitt 10.1.2.2, „Den Status der drahtlosen Zugangspunkte anzeigen“
- Abschnitt 10.1.2.3, „Status der WLAN-Client-Zuordnungen anzeigen“
- Abschnitt 10.1.2.4, „Hinzufügen eines Wireless Access Point“
- Abschnitt 10.1.2.5, „Einen WAP (Wireless Access Point) löschen“

Abschnitt 10.1.2.1

Eine Liste der Wireless Access Points (WAP) anzeigen

Um eine Liste der WAPs (Wireless Access Points) anzusehen, geben Sie Folgendes ein:

```
show running-config interface wlan wlanport 1 access-point
```

Eine Tabelle oder Liste ähnlich dem folgenden Beispiel wird angezeigt:

```
ruggedcom# show running-config interface wlan wlanport 1 access-point ssids | tab
                                          CHANNEL  HT                        WEP
SSID        ENABLED  INTERFACE  BAND    MODE   WIDTH    MODE  CHANNEL  SECURITY   KEY  PASSPHRASE
-------------------------------------------------------------------------------------------------------------
```

```
RX1400-Air  X        wlan-ap1   2.4GHz  mixed  -        MIMO  6        wpa2_ccmp  -
 $4$05sxb9ZekzsdprcI0d4IDw==
RX1400AP    -        -          2.4GHz  mixed  -        MIMO  auto     wpa2_ccmp  -
 $4$05sxb9ZekzsdhYYI0d4IDw==

 !
!
```

Falls keine WAPs konfiguriert wurden, fügen Sie je nach Bedarf WAPs hinzu. Weitere Informationen finden Sie unter Abschnitt 10.1.2.4, „Hinzufügen eines Wireless Access Point“.

Abschnitt 10.1.2.2

Den Status der drahtlosen Zugangspunkte anzeigen

Um den Status aller drahtloser Zugangspunkte (Wireless Access Point, WAP) anzuzeigen, geben Sie Folgendes ein:

```
show interfaces wlan status access_point
```

Falls WAPs konfiguriert wurden, wird eine Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show interfaces wlan status access_point
interfaces wlan status access_point RX1400-Air
 interface     wlan-ap1
 mac           7c:ec:79:c0:8a:81
 mimo          2x2
 state         Enabled
 mode          mixed
 band          "2.4 GHz"
 channel       6
 channel width "20 MHz"
 security      "WPA2 CCMP"
 connected-client
BSSID              RX     TX          SIGNAL
-------------------------------------------------
7c:ec:79:c0:93:7c       9643    957975218       -25 dBm
```

Die Liste liefert die folgenden Informationen:

Parameter	Beschreibung
ssid	**Zusammenfassung:** Eine Zeichenkette SSID dieses WLANs.
interface	**Zusammenfassung:** Eine Zeichenkette Die von diesem WLAN verwendete Schnittstelle.
mac	**Zusammenfassung:** Eine Zeichenkette MAC-Adresse der Schnittstelle.
mimo	**Zusammenfassung:** Eine Zeichenkette MIMO-Konfiguration des Zugangspunkts.
state	**Zusammenfassung:** Eine Zeichenkette Zustand dieses Zugangspunkts.
mode	**Zusammenfassung:** Eine Zeichenkette Modus dieses WLANs.
band	**Zusammenfassung:** Eine Zeichenkette Frequenzband dieses Zugangspunkts.

Parameter	Beschreibung
channel	**Zusammenfassung:** Eine Zeichenkette Kanal dieses Zugangspunkts.
channel-width	**Zusammenfassung:** Eine Zeichenkette Breite des Kanals.
security	**Zusammenfassung:** Eine Zeichenkette Sicherheitsmodus dieses WLANs.

Falls keine WAPs konfiguriert wurden, konfigurieren Sie WAPs je nach Bedarf. Weitere Informationen finden Sie unter Abschnitt 10.1.2.4, „Hinzufügen eines Wireless Access Point“.

Abschnitt 10.1.2.3
Status der WLAN-Client-Zuordnungen anzeigen

Um den Status der WLAN-Clients, die einem bestimmten WAP (Wireless Access Point) zugeordnet sind, anzusehen, geben Sie Folgendes ein:

```
show interfaces wlan status access_point access-point connected-client
```

Erläuterung: *access-point* ist der gewünschte WAP.

Ist ein Client mit dem WAP verbunden, wird eine Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show interfaces wlan status access_point RX1400-Air connected-client
BSSID              RX           TX           SIGNAL
------------------------------------------------------
7c:ec:79:c0:93:7c       1889951798      1216926171      -64 dBm
```

Die Liste liefert die folgenden Informationen:

Parameter	Beschreibung
bssid	**Zusammenfassung:** Eine Zeichenkette Die BSSID der zugehörigen Station.
RX	**Zusammenfassung:** Eine Zeichenkette Die Anzahl vom Client empfangener Bytes.
TX	**Zusammenfassung:** Eine Zeichenkette Die Anzahl der an den Client übertragener Bytes.
signal	**Zusammenfassung:** Eine Zeichenkette Durchschnittliche Signalstärke.

Abschnitt 10.1.2.4
Hinzufügen eines Wireless Access Point

Um einen Wireless Access Point hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den Zugangspunkt hinzu, indem Sie Folgendes eingeben:

```
interface wlan wlanport 1 access-point ssids ssid
```

Erläuterung: *ssid* ist der Service Set Identifier (SSID) für den Zugangspunkt.

WICHTIG!
Es können nicht mehr als zwei WAPs gleichzeitig aktiviert werden.

3. Konfigurieren Sie die folgenden gemeinsamen Parameter, indem Sie Folgendes eingeben:

Parameter	Beschreibung
enabled	Ist die Option ausgewählt (markiert), ist der Zugangspunkt aktiviert.
band { band }	**Zusammenfassung:** { 2.4GHz, 5GHz } **Standard:** 2.4GHz Das Frequenzband.
channel { channel }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 10 Zeichen **Standard:** auto Der Kanal.
security { security }	**Zusammenfassung:** { wpa2_ccmp, wpa2_ccmp_wpa_tkip, wpa_ccmp, wpa_tkip_ccmp, wpa_tkip, wep, open } **Standard:** wpa2_ccmp_wpa_tkip Das vom WLAN unterstützte Sicherheitsprotokoll.
passphrase { passphrase }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 128 Zeichen Das Passwort für das WLAN. Das Passwort muss zwischen 8 und 63 Zeichen lang sein. Es darf Ziffern, Kleinbuchstaben, Großbuchstaben und Sonderzeichen (z. B. !@#$%^&*()_+-={}) enthalten. Verwenden Sie für erhöhte Sicherheit ein Passwort, dass mindestens 12 Zeichen lang ist und mindestens einen Großbuchstaben, einen Kleinbuchstaben und ein Sonderzeichen enthält. Dieser Parameter ist obligatorisch.

HINWEIS
Das 5,0-GHz-Frequenzband unterstützt ausschließlich SISO, das eine Kanalbreite von 20 bzw. 40 MHz unterstützen kann. Das 2,4-GHz-Frequenzband unterstützt sowohl SISO (20 MHz) als auch MIMO (40 MHz).

4. Konfigurieren Sie je nach ausgewähltem Frequenzband die folgenden zusätzlichen Parameter:

- **Bei 2,4 GHz**

Parameter	Beschreibung
mode { mode }	**Zusammenfassung:** { mixed, b-g-only, b-only, g-only } **Standard:** mixed Der Modus, der am besten zu den Clients passt, die sich mit dem WLAN verbinden.
ht-mode { ht-mode }	**Zusammenfassung:** { SISO, MIMO } **Standard:** MIMO Der MIMO-Modus.

- **Bei 5,0 GHz**

Parameter	Beschreibung
channel-width { channel-width }	**Zusammenfassung:** { 20MHz, 40MHz } **Standard:** 20MHz Die Kanalbreite.

5. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 10.1.2.5
Einen WAP (Wireless Access Point) löschen

Um einen WAP (Wireless Access Point) zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den WAP durch Eingabe von:

   ```
   no interface wlan wlanport 1 access-point ssids ssid
   ```

   Erläuterung: *ssid* ist der Service Set Identifier (SSID) für den Access Point (AP).
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 10.1.3
WLAN-Clients verwalten

Dieser Abschnitt beschreibt, wie Sie das Gerät als Client im WLAN konfigurieren können. Hierfür werden Aliase konfiguriert, die mit bestimmten Zugangspunkten verbunden sind.

INHALT

- Abschnitt 10.1.3.1, „Eine Liste der WLAN-Clients anzeigen“
- Abschnitt 10.1.3.2, „Status der WLAN-Clients anzeigen“
- Abschnitt 10.1.3.3, „Hinzufügen eines WLAN-Clients“
- Abschnitt 10.1.3.4, „Einen WLAN-Client löschen“
- Abschnitt 10.1.3.5, „Suchen nach WLAN-Clients“

Abschnitt 10.1.3.1
Eine Liste der WLAN-Clients anzeigen

Um eine Liste der WLAN-Clients anzusehen, geben Sie Folgendes ein:

```
show running-config interface wlan wlanport 1 client wireless-lans
```

```
ruggedcom# show running-config interface wlan wlanport 1 client wireless-lans | tab
                                                                          IP
                                                                          ADDRESS
WLAN ALIAS    ENABLED  SSID SECURITY       PASSWORD                       SRC
--------------------------------------------------------------------------------
WLAN-Client1  X        RX1400AP-Air--WPA2  $4$05sxb9ZekzsdhYYI0d4IDw==  static

 !
!
```

Falls keine WLAN-Clients konfiguriert wurden, fügen Sie je nach Bedarf Clients hinzu. Weitere Informationen finden Sie unter Abschnitt 10.1.3.3, „Hinzufügen eines WLAN-Clients“.

Abschnitt 10.1.3.2
Status der WLAN-Clients anzeigen

Um den Status der WLAN-Clients anzusehen, geben Sie Folgendes ein:

```
show interfaces wlan status link
```

Eine Liste ähnlich dem folgenden Beispiel wird angezeigt:

```
ruggedcom# show interfaces wlan status link
interfaces wlan status link
 interface wlan-cl1
 mac       7c:ec:79:c0:93:7c
 state     Enabled
 ssid      RX1400-Air
 frequency 2437
 signal    "-39 dBm"
```

Die Liste liefert die folgenden Informationen:

Parameter	Beschreibung
interface	**Zusammenfassung:** Eine Zeichenkette Netzwerkschnittstelle für diese Verbindung.
mac	**Zusammenfassung:** Eine Zeichenkette MAC-Adresse der Schnittstelle.
state	**Zusammenfassung:** Eine Zeichenkette Zustand dieses Verbindungszweigs.
ssid	**Zusammenfassung:** Eine Zeichenkette WLAN, mit dem dieser Client verbunden ist.
frequency	**Zusammenfassung:** Eine Zeichenkette Frequenz zur Kommunikation mit dem Zugangspunkt.
signal	**Zusammenfassung:** Eine Zeichenkette Signalstärke.

Abschnitt 10.1.3.3
Hinzufügen eines WLAN-Clients

Um einen WLAN-Client hinzuzufügen, gehen Sie wie folgt vor:

1. Durchsuchen Sie das Netzwerk nach verfügbaren WLAN-Clients. Jeder erkannte Client ist nach dem Hinzufügen wählbar. Weitere Informationen finden Sie unter Abschnitt 10.1.3.5, „Suchen nach WLAN-Clients“.
2. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
3. Fügen Sie den Client hinzu, indem Sie Folgendes eingeben:

   ```
   interface wlan wlanport 1 client wireless-lans name
   ```

   Erläuterung: *name* ist die Bezeichnung des Clients.
4. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
enabled	Ist die Option ausgewählt (markiert), ist der WLAN-Aliasname aktiviert.
ssid-security { ssid-security }	**Zusammenfassung:** Eine Zeichenkette Das WLAN, mit dem verbunden werden soll. Wählen Sie entweder ein WLAN aus der Liste oder wählen Sie "manual-setup", um ein WLAN manuell festzulegen.
password { password }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 32 Zeichen Das Passwort für das WLAN. Dieser Parameter ist obligatorisch.
ip-address-src { ip-address-src }	**Zusammenfassung:** { static, dynamic } **Standard:** dynamic Bestimmt, ob die IP-Adresse statisch oder dynamisch über DHCP oder BOOTP zugewiesen ist.
ipv6-address-src { ipv6-address-src }	**Zusammenfassung:** { static, dynamic } **Standard:** dynamic Bestimmt, ob die IP-Adresse statisch oder dynamisch über DHCPv6 zugewiesen ist.

5. Wenn *`SSID Security`* auf `manual-setup`gesetzt ist, konfigurieren Sie je nach Bedarf den/die folgenden zusätzlichen Parameter:

WICHTIG!
*Das WLAN-Passwort muss zwischen 8 und 63 Zeichen lang sein. Es darf Ziffern, Kleinbuchstaben, Großbuchstaben und Sonderzeichen (z. B. *()_+-={}[];:',<.>/?\| `~) enthalten. Verwenden Sie für erhöhte Sicherheit ein Passwort, dass mindestens 12 Zeichen lang ist und mindestens einen Großbuchstaben, einen Kleinbuchstaben und ein Sonderzeichen enthält.*

Parameter	Beschreibung
ssid { ssid }	**Zusammenfassung:** Eine Zeichenkette Die SSID für das WLAN. Dieser Parameter ist obligatorisch.
security { security }	**Zusammenfassung:** { wpa/wpa2, wep, open } **Standard:** wpa/wpa2 Das vom WLAN unterstützte Sicherheitsprotokoll.
password { password }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 32 Zeichen Das Passwort für das WLAN. Dieser Parameter ist obligatorisch.

6. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 10.1.3.4
Einen WLAN-Client löschen

Um einen WLAN-Client zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den Client durch Eingabe von:

```
no interface wlan wlanport 1 client wireless-lans name
```

Erläuterung: *name* ist der Client-Name.

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 10.1.3.5
Suchen nach WLAN-Clients

Verwenden Sie vor der Konfiguration eines WLAN-Clients für ein Gerät das Scan-Programm, um im Bereich verfügbare WLAN-Clients zu finden. Gefundene WLAN-Clients sind nach Konfiguration eines Alias für den jeweiligen Client auswählbar und können in den Ergebnissen des Scanvorgangs angezeigt werden.

Um nach verfügbaren WLAN-Clients zu suchen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass die WLAN-Schnittstelle aktiviert ist. Weitere Informationen finden Sie unter Abschnitt 10.1.1, „Aktivieren und Konfigurieren der WLAN-Schnittstelle“.
2. Stellen Sie sicher, dass alle vorhandenen WLAN-Clients deaktiviert sind. Weitere Informationen finden Sie unter Abschnitt 10.1.3.3, „Hinzufügen eines WLAN-Clients“.
3. Führen Sie das Scan-Programm aus, indem Sie Folgendes eingeben:

```
interface wlan wlanport 1 scan
```

4. [Optional] Zeigen Sie die Ergebnisse des Scanvorgangs an, indem Sie Folgendes eingeben:

```
show running-config interface wlan wlanport 1 scan-results
```

Beispiel:

```
show running-config interface wlan wlanport 1 scan-results | tab
WLAN
--------------------
RX1400AP-Air--WPA2
RuggedCom--OPEN
manual-setup

 !
!
```

Abschnitt 10.1.4
Beispiel: Konfigurieren eines WLAN mit einer Firewall

In diesem Beispiel wird gezeigt, wie WAN- und LAN-Netzwerke bei gleichzeitiger Steuerung des Datenverkehrs mit einer Firewall miteinander verbunden werden.

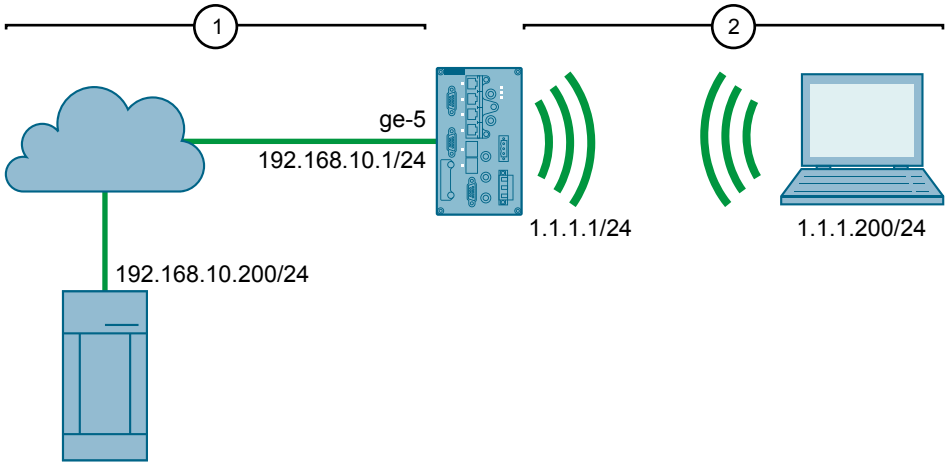


Abbildung 18: WLAN mit Firewall-Topologie

1. WAN **2.** LAN

» Schritt 1: Verbinden Sie die WAN- und LAN-Netzwerke

1. Stellen Sie sicher, dass die WLAN-Schnittstelle aktiviert ist. Weitere Informationen finden Sie unter Abschnitt 10.1.1, „Aktivieren und Konfigurieren der WLAN-Schnittstelle“.
2. Konfigurieren Sie einen drahtlosen Zugangspunkt. Weitere Informationen finden Sie unter Abschnitt 10.1.2.4, „Hinzufügen eines Wireless Access Point“.
3. Weisen Sie eine IPv4- oder IPv6-Adresse der Schnittstelle zu, die dem neuen drahtlosen Zugangspunkt zugeordnet ist. Für weitere Informationen siehe Abschnitt 7.1.3.2, „Eine IPv4-Adresse hinzufügen“ oder Abschnitt 7.1.4.2, „Eine IPv6-Adresse hinzufügen“.
4. Verbinden Sie das WAN-Netzwerk mit einem verfügbaren Switched-Ethernet-Port am Gerät.
5. Konfigurieren Sie den Port folgendermaßen:

Parameter	Wert
Switchport	{ deaktiviert }
IP-Adressquelle	static

Für weitere Informationen über das Konfigurieren eines Ports siehe Abschnitt 8.1.2, „Einen Switched-Ethernet-Port konfigurieren“.

HINWEIS
*Wenn sich ein Switched-Ethernet-Port im Direct-Routing-Modus (vs. Switch-Modus) befindet, wird eine Schnittstelle in der Form **ge-{port}** automatisch zum Menü **ip** hinzugefügt. Wenn beispielsweise der Direct-Routing-Modus für Port 5 konfiguriert wird, dann wird die Schnittstelle **ge-5** erstellt.*

6. Weisen Sie dem Switched-Ethernet-Port, der auf der WAN-Seite des Netzwerks angeschlossen ist, eine IPv4- oder IPv6-Adresse zu. Für weitere Informationen siehe Abschnitt 7.1.3.2, „Eine IPv4-Adresse hinzufügen“ oder Abschnitt 7.1.4.2, „Eine IPv6-Adresse hinzufügen“.
7. Konfigurieren Sie für jeden PC auf der WAN-Seite des Netzwerks eine IP-Adresse, die sich auf demselben Subnetz wie die für den Switched-Ethernet-Port konfigurierte IP-Adresse befindet. Beispiel:

IP-Adresse des Routers	192.168.10.1/24
IP-Adresse des PC	192.168.10.200/24

Dieser Schritt ist systemabhängig. Weitere Informationen finden Sie im Benutzerhandbuch für das OS.

8. Konfigurieren Sie für jeden PC auf der LAN-Seite des Netzwerks eine IP-Adresse und ein Standard-Gateway, die sich auf demselben Subnetz wie die für den Zugangspunkt konfigurierte IP-Adresse befinden. Beispiel:

IP-Adresse des Routers	1.1.1.1/24
IP-Adresse des PC	1.1.1.200/24
Standard-Gateway des PC	1.1.1.1

Dieser Schritt ist systemabhängig. Weitere Informationen finden Sie im Benutzerhandbuch für das OS.

9. Fügen Sie für jeden PC auf der LAN-Seite des Netzwerks eine statische Route hinzu. Zum Beispiel auf Linux-® PCs:

```
# route add 192.168.10.0 mask 255.255.255.0 1.1.1.1
```

Informationen über das Hinzufügen statischer Routen für andere Betriebssysteme finden Sie im Benutzerhandbuch für das OS.

10. Klicken Sie auf **Commit**.
11. Überprüfen Sie, dass die WAN- und LAN-Netzwerke über den Router verbunden sind, indem Sie Ping-Anfragen zwischen den PCs senden.

» Schritt 2: Konfigurieren Sie die Firewall

1. Fügen Sie eine neue Firewall hinzu (z. B. WLAN-Firewall). Weitere Informationen finden Sie unter Abschnitt 6.7.3, „Hinzufügen einer Firewall“.
2. Konfigurieren Sie eine Zone für jede Seite des Netzwerks sowie eine Zone für die Firewall. Beispiel:

Bezeichnung Zone	IP-Typ	Typ
WAN	ipv4	ipv4
LAN	ipv4	ipv4
FW	ipv4	firewall

Informationen über das Hinzufügen von Zonen finden Sie unter Abschnitt 6.7.8.2, „Eine Zone hinzufügen“.

3. Fügen Sie Schnittstellen für den Switched-Ethernet-Port, den Zugangspunkt und das Gerät hinzu. Stellen Sie sicher, dass der Switched-Ethernet-Port der WAN-Zone zugeordnet ist und dass andere Schnittstellen der LAN-Zone zugeordnet sind. Beispiel:

Interface	Vordefinierte Zone
ge-5	WAN
wlan-ap1	LAN
switch.0001	LAN

Informationen über das Hinzufügen einer Schnittstelle und das Zuordnen dieser Schnittstelle zu einer vordefinierten Zone finden Sie unter Abschnitt 6.7.9.2, „Hinzufügen einer Schnittstelle“ und Abschnitt 6.7.9.3, „Eine Schnittstelle zu einer Zone zuweisen“.

4. Fügen Sie Grundregeln hinzu, um den Datenverkehr zwischen den Netzwerken zu steuern. Beispiel:

Bezeichnung	Quellzone	Zielzone	Grundregel
Grundregel1	WAN	LAN	ablehnen
Grundregel2	WAN	FW	akzeptieren
Grundregel3	LAN	WAN	akzeptieren
Grundregel4	LAN	FW	akzeptieren
Grundregel5	FW	LAN	akzeptieren
Grundregel6	FW	WAN	akzeptieren

   Weitere Informationen über das Hinzufügen von Grundregeln finden Sie in Abschnitt 6.7.11.2, „Eine Regel hinzufügen“.
5. Validieren Sie die Firewall-Konfiguration. Weitere Informationen finden Sie unter Abschnitt 6.7.15, „Eine Firewall-Konfiguration überprüfen“.
6. Aktivieren Sie die Firewall. Weitere Informationen finden Sie unter Abschnitt 6.7.16, „Eine Firewall aktivieren/deaktivieren“.
7. Wählen Sie die neue Firewall als Arbeitskonfiguration aus. Weitere Informationen finden Sie unter Abschnitt 6.7.5, „Betrieb mit mehreren Firewallkonfigurationen“.
8. Klicken Sie auf **Commit**.
9. Überprüfen Sie, dass die WAN- und LAN-Netzwerke über den Router verbunden sind, indem Sie Ping-Anfragen zwischen den PCs senden.

Abschnitt 10.2

Mobilfunkmodem-Schnittstellen verwalten

Dieser Abschnitt beschreibt, wie Sie eine Schnittstelle zu einem 4G-LTE-Mobilfunknetz konfigurieren und die GPS-Fähigkeiten des Geräts aktivieren können.

INHALT

- Abschnitt 10.2.1, „Dual-SIM-Karten aktivieren“
- Abschnitt 10.2.2, „Eine Liste der Mobilfunkmodem-Schnittstellen anzeigen“
- Abschnitt 10.2.3, „Anzeigen des Status einer Mobilfunkmodem-Schnittstelle“
- Abschnitt 10.2.4, „Statistiken zu PPP-Schnittstellen anzeigen“
- Abschnitt 10.2.5, „Eine Mobilfunkmodem-Schnittstelle konfigurieren“

Abschnitt 10.2.1

Dual-SIM-Karten aktivieren

RUGGEDCOM RX1400 unterstützt Dual-Micro-SIM-Karten für das LTE-Modem, um einen Failover-Mechanismus bereitzustellen, wenn eine der SIM-Karten die Verbindung zum Netzwerk verliert.

Um beide Micro-SIM-Karten zu aktivieren, gehen Sie wie folgt vor:

1. Vergewissern Sie sich, dass beide Micro-SIM-Karten installiert sind. Ausführliche Informationen hierzu finden Sie im *RUGGEDCOM RX1400 Installationsleitfaden*.
2. Konfigurieren Sie ein GSM-Profil für jede Micro-SIM-Karte und achten Sie darauf, dass die andere Karte jeweils als Failover-Profil eingerichtet ist. Weitere Informationen finden Sie unter Abschnitt 10.5.2, „Hinzufügen eines GSM-Profils“.
3. Konfigurieren Sie die Mobilfunkschnittstelle für die Verbindung mit dem Mobilfunknetz über das primäre Profil. Weitere Informationen finden Sie unter Abschnitt 10.4, „Herstellen einer Verbindung als PPP-Client“.

Abschnitt 10.2.2
Eine Liste der Mobilfunkmodem-Schnittstellen anzeigen

Um eine Liste der Mobilfunkmodem-Schnittstellen anzusehen, geben Sie Folgendes ein:

```
show running-config interface cellmodem
```

Eine Tabelle oder Liste ähnlich dem folgenden Beispiel wird angezeigt:

```
ruggedcom# show running-config interface cellmodem
interface
 cellmodem celport 1
  enabled
  no alias
  lte ppp-client connect-to profile1
 !
!
```

Abschnitt 10.2.3
Anzeigen des Status einer Mobilfunkmodem-Schnittstelle

Um den Status der Mobilfunkmodem-Schnittstelle anzuzeigen, geben Sie Folgendes ein:

```
show interfaces cellmodem port lte
```

Erläuterung:

- *port* ist die Portnummer für das Modul

Eine Tabelle oder Liste ähnlich dem folgenden Beispiel wird angezeigt:

```
ruggedcom# show interfaces cellmodem cel-1 cdma NETWORK RSSI NETWORK NETWORK NETWORK
 PHONE IFNAME TYPE SUPPORTED ESN ECIO INDICATOR OPERATOR IN USE STATUS NUMBER
 ------------------------------------------------------------------------------- cel-1 cdma 0 0
 Unknown
```

Diese Tabelleoder Liste liefert die folgenden Informationen:

Parameter	Beschreibung
state	**Zusammenfassung:** { not set, up, down, testing, unknown, dormant, notPresent, lowerLayerDown } Der Link-Status des Ports. Dieser Parameter ist obligatorisch.
media	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 31 Zeichen Die drahtlose Datenkommunikationstechnologie, mit der das Modem kompatibel ist{ GSM/HSPA, CDMA/EVDO, LTE }.

Parameter	Beschreibung
	Dieser Parameter ist obligatorisch.
admin-state	**Zusammenfassung:** { not set, up, down, testing, unknown, dormant, notPresent, lowerLayerDown } Der Verwaltungszustand des Ports. Dieser Parameter ist obligatorisch.

Abschnitt 10.2.4

Statistiken zu PPP-Schnittstellen anzeigen

Um die Statistiken für die PPP-Schnittstelle anzuzeigen, geben Sie Folgendes ein:

```
show interfaces cellmodem ppp-connections
```

Eine Tabelle oder Liste ähnlich dem folgenden Beispiel wird angezeigt:

```
ruggedcom# show interfaces cellmodem ppp-connections
             CONNECTION    LOCAL  REMOTE  TX     RX
IFNAME  TYPE  STATUS        IP     IP      BYTES  BYTES  MTU
-------------------------------------------------------------
cel-1   lte   Disconnected                0      0      0
```

Diese Tabelle oder Liste liefert die folgenden Informationen:

Parameter	Beschreibung
connection-status	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 128 Zeichen PPP-Verbindungsstatus Dieser Parameter ist obligatorisch.
local-ip	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 32 Zeichen Die dem Modem vom entfernten Server zugewiesene IP-Adresse Dieser Parameter ist obligatorisch.
remote-ip	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 32 Zeichen Die IP-Adresse des entfernten Servers Dieser Parameter ist obligatorisch.
tx-bytes	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die über das Modem übertragenen Bytes Dieser Parameter ist obligatorisch.
rx-bytes	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die vom Modem empfangenen Bytes Dieser Parameter ist obligatorisch.
mtu	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl MTU (en: Maximum Transmission Unit, maximale Übertragungseinheit)-Wert an der PPP-Schnittstelle Dieser Parameter ist obligatorisch.

Abschnitt 10.2.5
Eine Mobilfunkmodem-Schnittstelle konfigurieren

Um eine Mobilfunkmodem-Schnittstelle zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***interface » cellmodem » {interface}***, wobei *{interface}* die Mobilfunkmodem-Schnittstelle ist.
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
enabled	**Zusammenfassung:** { true, false } **Standard:** false Bietet die Option, diese Schnittstelle zu aktivieren oder zu deaktivieren. Wenn die Option nicht markiert ist (d. h. deaktiviert), verhindert die Schnittstelle, dass Frames an dieser Schnittstelle gesendet oder empfangen werden.
link-alarms	**Zusammenfassung:** { true, false } **Standard:** true Das Deaktivieren von Link-Alarmen („link-alarms") verhindert, dass Alarme und "LinkUp"- und "LinkDown"-SNMP-Traps für diese Schnittstelle versendet werden. Link-Alarme können für das gesamte System auch unter "admin / alarm-cfg" verwaltet werden.
alias { alias }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 64 Zeichen Der SNMP-Aliasname der Schnittstelle.

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 10.3
AT-Befehle ausführen

Um AT-Befehle (Hayes-Befehle) an das Mobilfunkmodem zu senden, geben Sie Folgendes ein:

```
interfaces cellmodem cel-1 lte at command command
```

Erläuterung: *`command`* ist der AT-Befehl

Abschnitt 10.4
Herstellen einer Verbindung als PPP-Client

Um eine Verbindung mit einem Mobilfunknetz als PPP-Client herzustellen bzw. zu trennen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Stellen Sie sicher, dass die Schnittstelle des Mobilfunkmodems konfiguriert wurde. Weitere Informationen finden Sie unter Abschnitt 10.2.5, „Eine Mobilfunkmodem-Schnittstelle konfigurieren".
3. Stellen Sie sicher, dass ein geeignetes Mobilfunkmodem-Profil konfiguriert wurde. Weitere Informationen finden Sie unter Abschnitt 10.5, „Mobilfunkmodem-Profile verwalten".
4. Stellen Sie sicher, dass für den Modemtyp bei einem Serviceanbieter ein Konto aktiviert wurde.

5. Stellen Sie vor dem Herstellen der Verbindung sicher, dass die Antennen ordnungsgemäß mit dem Gerät verbunden wurden. Ausführliche Informationen hierzu finden Sie im *RUGGEDCOM RX1400 Installationsleitfaden*.
6. Stecken Sie eine SIM-Karte in das Mobilfunkmodemmodul.
7. Wählen Sie das beim Herstellen einer Verbindung zum Drahtlosnetzwerk zu verwendende Mobilfunkmodem-Profil, indem Sie Folgendes eingeben:

   ```
   interface cellmodem celport 1 lte ppp-client connect-to profile
   ```

   Erläuterung:

   - *profile* ist das Mobilfunkmodem-Profil.
8. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 10.5
Mobilfunkmodem-Profile verwalten

GSM-Profile (Global System for Mobile Communications) müssen konfiguriert werden, bevor HSPA-Daten verfügbar sind.

INHALT

- Abschnitt 10.5.1, „Eine Liste der GSM-Profile anzeigen“
- Abschnitt 10.5.2, „Hinzufügen eines GSM-Profils“
- Abschnitt 10.5.3, „Ein GSM-Profil löschen“

Abschnitt 10.5.1
Eine Liste der GSM-Profile anzeigen

Um eine Liste der GSM-Profile anzuzeigen, geben Sie Folgendes ein:

```
show running-config global cellular profiles gsm
```

Falls Profile konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config global cellular profiles gsm | tab
                                                 USE                          DIAL    DISCONNECT
 FAILOVER
                    APN   DIAL                    PEER                         ON      IDLE        ON
NAME  APN           TYPE  STRING    SIM  PROFILE  DNS   USERNAME  PASSWORD     DEMAND  TIMEOUT     DEMAND
   MTU   AUTHENTICATION
-------------------------------------------------------------------------------------------------------------
gsm1  apn.gsm2.net  ipv4  *99***1#  1    -        -     N/A       N/A          -       0           -
   1500  none
gsm2  apn.gsm2.net  ipv4  *99***1#  2    gsm1     -     N/A       N/A          -       0           -
   1500  none

!
```

Falls keine Profile konfiguriert wurden, fügen Sie je nach Bedarf Profile hinzu. Weitere Informationen finden Sie unter Abschnitt 10.5.2, „Hinzufügen eines GSM-Profils“.

Abschnitt 10.5.2
Hinzufügen eines GSM-Profils

Um ein GSM-Profil für die Mobilfunkmodem-Schnittstelle hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie die Einschränkung hinzu, indem Sie Folgendes eingeben:

```
global cellular profiles gsm name
```

   Erläuterung:

   - *name* ist die Bezeichnung des Profils

3. Konfigurieren Sie das Mobilfunknetz, indem Sie die folgenden Befehle eingeben:

Parameter	Beschreibung
apn { apn }	**Zusammenfassung:** Eine Zeichenkette **Standard:** none Der Name des Drahtlosnetzwerk-Zugangspunkts.
apn-type { apn-type }	**Zusammenfassung:** { ipv4, ipv6, ipv4v6 } **Standard:** ipv4 Den für die Anbindung an PDN verwendeten APN-Typ festlegen
dial-string { dial-string }	**Zusammenfassung:** Eine Zeichenkette **Standard:** *99***1# Ein vom drahtlosen Provider gegebener Wählstring zum Verbinden mit dem Zugangspunktnamen.
sim { sim }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 1 und 2 **Standard:** 1 Den von diesem Profil zu verwendenden SIM-Index festlegen
peer { peer }	**Zusammenfassung:** Eine Zeichenkette mit 7 bis 15 Zeichen oder eine Zeichenkette mit 6 bis 40 Zeichen Die Peer-Adresse zum Ausschalten der Adresse des Trägers

4. Wählen Sie das zu verwendende Failover-Profil, indem Sie den folgenden Befehl eingeben:

Parameter	Beschreibung
profile { profile }	**Zusammenfassung:** Eine Zeichenkette Das Mobilfunkverbindungsprofil festlegen

5. Konfigurieren Sie die GSM-PPP-Einstellungen, indem Sie die folgenden Befehle eingeben:

Parameter	Beschreibung
use-peer-dns	Aktiviert die vom PPP-Server empfohlenen DNS-Server-Einträge. Aktiviert diese Option, sofern Sie nicht über einen eigenen Name-Server verfügen.
username { username }	**Zusammenfassung:** Eine Zeichenkette **Standard:** N/A Die Benutzer-ID zum Verbinden mit dem entfernten Server.
password { password }	**Zusammenfassung:** Eine Zeichenkette **Standard:** N/A Das vom entfernten Server zu authentifizierende Passwort.

Parameter	Beschreibung
dial-on-demand	Aktiviert "Dial-on-Demand" für diese Verbindung. Der Aufbau der PPP-Verbindung wird so lange hinausgezögert, bis Daten zur Übertragung über die Schnittstelle vorhanden sind. Falls "Dial-on-Demand" konfiguriert ist, kann kein "Failover-on-Demand" konfiguriert sein. **HINWEIS** *Falls "Dial-on-Demand" konfiguriert ist, kann kein "Failover-on-Demand" konfiguriert sein.*
disconnect-idle-timeout { disconnect-idle-timeout }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl **Standard:** 0 Die Wartezeit in Sekunden vor dem Trennen vom PPP, falls kein Verkehr auf der Verbindung ist. Diese Option ist nur verfügbar, wenn "Dial-on-Demand" aktiviert ist.
failover-on-demand	Aktiviert Verbindungs-"Failover on-Demand" an diesem Gerät. Der PPP-Verbindungsaufbau an diesem Gerät wird vom Verbindungs-Failover gesteuert. Ist ein Verbindungs-"Failover on-Demand" konfiguriert, kann kein "Dial-on-Demand" konfiguriert werden. **HINWEIS** *Ist ein Verbindungs-"Failover on-Demand" konfiguriert, kann kein "Dial-on-Demand" konfiguriert werden.*
mtu { mtu }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 128 und 1500 **Standard:** 1500 MTU (en: Maximum Transmission Unit, maximale Übertragungseinheit)-Wert an einer PPP-Schnittstelle.
authentication { authentication }	**Zusammenfassung:** { none, chap, pap } **Standard:** none Das für den Aufbau einer Mobilfunkdatenverbindung verwendete Authentifizierungsprotokoll

6. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 10.5.3
Ein GSM-Profil löschen

Um ein GSM-Profil zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den ausgewählten Schlüssel durch Eingabe von:

```
no global cellular profiles gsm name
```

Erläuterung:

- *`name`* ist der Name des Profils

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 10.6

Das LTE-Modem verwalten

Dieser Abschnitt beschreibt, wie Sie das LTE-Modem verwalten können.

INHALT

- Abschnitt 10.6.1, „Aktivieren/Deaktivieren des LTE-Modems“
- Abschnitt 10.6.2, „LTE-Modem konfigurieren“
- Abschnitt 10.6.3, „Das Mobilfunkmodem zurücksetzen“
- Abschnitt 10.6.4, „Aktivieren/Deaktivieren von GPS“
- Abschnitt 10.6.5, „NMEA-GPS-Datenströme aktivieren und konfigurieren“
- Abschnitt 10.6.6, „Ändern der aktiven SIM-Karte“
- Abschnitt 10.6.7, „Firmware-Updates verwalten“

Abschnitt 10.6.1

Aktivieren/Deaktivieren des LTE-Modems

Das LTE-Modem kann über den RUGGEDCOM ROX II deaktiviert werden.

» Aktivieren

Um das LTE-Modem zu aktivieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Aktivieren Sie das LTE-Modem, indem Sie Folgendes eingeben:

```
interface cellmodem celport 1 enabled
```

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

» Deaktivieren

Um das LTE-Modem zu deaktivieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Deaktivieren Sie das LTE-Modem, indem Sie Folgendes eingeben:

```
no interface cellmodem celport 1 enabled
```

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 10.6.2
LTE-Modem konfigurieren

Um das LTE-Modem zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Aktivieren Sie das LTE-Modem. Für weitere Informationen siehe Abschnitt 10.6.1, „Aktivieren/Deaktivieren des LTE-Modems“.
3. Navigieren Sie zu ***interface » cellmodem » celport/1 » lte*** .
4. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
failover-timer { failover-timer }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 1 und 10 **Standard:** 2 Den Timer bei SIM-Karten-Failover in Minuten festlegen
max-try { max-try }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 0 und 65535 **Standard:** 0 Geben Sie die maximale Anzahl der Wiederholversuche bei SIM-Karten-Failover an. 0 steht für unendliche Wiederholversuche

5. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.
6. [Optional] Aktivieren Sie GPS. Für weitere Informationen siehe Abschnitt 10.6.4, „Aktivieren/Deaktivieren von GPS“.

Abschnitt 10.6.3
Das Mobilfunkmodem zurücksetzen

Um ein Mobilfunkmodem zurückzusetzen, geben Sie Folgendes ein:

```
interfaces cellmodem cel-1 lte reset
```

Erläuterung:

Abschnitt 10.6.4
Aktivieren/Deaktivieren von GPS

Bei aktiviertem GPS können Benutzer den aktuellen Standort des Geräts einsehen. Sofern aktiviert, kann der RUGGEDCOM ROX II auch einen NMEA-GPS-Datenstrom über TCP an einen Server senden, der eine GPS-Anwendung hostet.

Um GPS auf dem Mobilfunkmodem zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Aktivieren oder deaktivieren Sie GPS, indem Sie Folgendes eingeben:

   Aktivieren von GPS

```
interface cellmodem celport 1 lte gps enabled
```

Deaktivieren von GPS

```
no interface cellmodem celport 1 lte gps enabled
```

3. [Optional] Aktivieren oder deaktivieren Sie NMEA GPS-Datenströme. Weitere Informationen finden Sie unter Abschnitt 10.6.5, „NMEA-GPS-Datenströme aktivieren und konfigurieren“.
4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 10.6.5

NMEA-GPS-Datenströme aktivieren und konfigurieren

Wenn GPS aktiviert ist, kann der RUGGEDCOM ROX II einen NMEA-GPS-Datenstrom über TCP an einen Server senden, der eine GPS-Anwendung hostet. Diese Funktion kann unabhängig von der LTE-Modemkonfiguration aktiviert oder deaktiviert werden.

Um die NMEA-GPS-Datenströme zu aktivieren und zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Geben Sie Folgendes ein:

```
interface cellmodem celport 1 lte gps nmea
```

Erläuterung:

- *`interface`* ist die Schnittstelle des Mobilfunkmodems

3. Konfigurieren Sie je nach Bedarf die folgenden Parameter:

Parameter	Beschreibung
enabled	Aktiviert NMEA-Datenstrom **HINWEIS** *Vor Aktivieren des NMEA-Datenstroms muss GPS aktiviert sein*
listen-ip { listen-ip }	**Zusammenfassung:** Eine Zeichenkette **Standard:** 0.0.0.0 Die IP-Adresse, an der das Gerät Anfragen des entfernten Hosts empfängt.
local-port { local-port }	**Zusammenfassung:** Eine vorzeichenlose 16-Bit-Ganzzahl zwischen 0 und 65535 **Standard:** 10110 Der Port, an dem das Gerät Anfragen des entfernten Hosts empfängt.
extra-ip-ports { extra-ip-ports }	**Zusammenfassung:** Eine Zeichenkette Das Gerät empfängt auch an diesen IP-Adressen. Fügen Sie bei Port-Werten ':#' hinzu, um die nicht voreingestellten Port-Werte einzustellen (d. h. xxx.xxx.xxx.xxx:19343 [::]:16000). Bei Verwendung der Standardadresse legen Sie keine empfangende Adresse mit dem gleichen Port fest.
max-sessions { max-sessions }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 1 und 32 **Standard:** 10 Die maximale Anzahl gleichzeitiger TCP/IP-Sitzungen.

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 10.6.6
Ändern der aktiven SIM-Karte

Wenn zwei SIM-Karten installiert sind, dann ist die SIM-Karte in Steckplatz 1 standardmäßig die primäre (bzw. aktive) Karte. Die Karte in Steckplatz 2 dient als Backup-Karte, falls die primäre Karte die Verbindung zum Netzwerk verliert.

Um manuell umzuschalten, welche Karte die aktive SIM-Karte sein soll, gehen Sie wie folgt vor:

1. Um die SIM-Karten umzuschalten, geben Sie Folgendes ein:

   ```
   interfaces cellmodem cel-1 lte force-switch-profile
   ```

2. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Um zu überprüfen, ob die SIM-Karten erfolgreich umgeschaltet wurden, geben Sie Folgendes ein:

```
show interfaces cellmodem cel-1 lte
```

Eine Liste ähnlich dem folgenden Beispiel wird angezeigt:

```
ruggedcom# show interfaces cellmodem cel-1 lte
interfaces cellmodem cel-1 lte
 lte
  network supported GSM,GPRS,EDGE,UMTS,HSDPA/HSUPA,HSPA+,LTE
  imei              359225052306750
  radio             on
  rssi indicator    -73
  network operator  TELUS
  network in use    LTE
  network status    "Registered to Home network"
  sim               8912230100043535630(Sim1)
  active profile    Profile2
  gps
   mode standalone
```

Die aktuell aktive SIM-Karte wird unter **Active Profile** aufgeführt.

Abschnitt 10.6.7
Firmware-Updates verwalten

Firmware-Upgrades für das LTE-Modem sind entweder direkt über das MicroSD/microSDHC-Flashlaufwerk oder drahtlos über einen entfernten HTTP/HTTPS-Server möglich.

Wird ein Upgrade über die drahtlose Verbindung ausgeführt, stellt RUGGEDCOM ROX II die Verbindung zum entfernten Server her und holt dann die neue Firmware-Version ab. Firmware-Updates sind entweder auf Anforderung oder automatisch, je nach Wunsch des Benutzers, möglich.

Bei einem Firmware-Update führt RUGGEDCOM ROX II die folgenden Schritte aus:

1. Er stellt die Verbindung zum MicroSD/microSDHC-Flashlaufwerk oder zum entfernten Server her und überprüft die Firmware-Version
2. Er lädt die neue Firmware herunter
3. Er prüft die neue Firmware daraufhin, ob sie für das Modem gültig ist
4. Er lädt die neue Firmware in das Modem
5. Er protokolliert alle Firmware-Updates und Aktionen im Systemprotokoll (Syslog)

6. Er schaltet das Modem wieder in den Normalbetrieb

INHALT

- Abschnitt 10.6.7.1, „Den Firmware-Update-Status anzeigen“
- Abschnitt 10.6.7.2, „Konfigurieren des Firmware-Update-Modus und der -Quelle“
- Abschnitt 10.6.7.3, „Firmware-Update durchführen“

Abschnitt 10.6.7.1

Den Firmware-Update-Status anzeigen

Um den Status des Firmware-Updates anzusehen, geben Sie Folgendes ein:

```
show interfaces cellmodem cel-1 firmware-update
```

Erläuterung:

- *interface* ist die Schnittstelle des Mobilfunkmodems.

Diese Tabelle enthält folgende Informationen:

Parameter	Beschreibung
current-version	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 64 Zeichen Die aktuelle Firmware-Version Dieser Parameter ist obligatorisch.
status-message	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 128 Zeichen Zusätzliche Einzelheiten zum Status des Updates.
last-update-attempt	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 64 Zeichen Datum und Uhrzeit der Fertigstellung des letzten Update-Versuchs.
last-update-result	**Zusammenfassung:** { N/A, Successful, Failed } Zeigt an, ob das letzte Firmware-Update erfolgreich abgeschlossen wurde.

Abschnitt 10.6.7.2

Konfigurieren des Firmware-Update-Modus und der -Quelle

Das Verfahren, bei dem der RUGGEDCOM ROX II Firmware-Updates erkennt und lädt, ist vom Benutzer konfigurierbar. Die Quelle kann auch so konfiguriert werden, dass sie auf einen dezentralen Upgrade-Server oder einen lokalen microSD/microSDHC-Flash-Speicher ausgerichtet ist.

Um ein Upgrade des Firmware-Update-Modus und der -Quelle auszuführen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass der Upgrade-Server konfiguriert ist und die neueste Firmware-Version hinzugefügt wurde. Weitere Informationen finden Sie unter Abschnitt 4.15.2, „Einrichten eines Upgrade-Servers“.
2. Stellen Sie sicher, dass die Mobilfunkmodem-Schnittstelle aktiviert ist. Weitere Informationen finden Sie unter Abschnitt 10.2.5, „Eine Mobilfunkmodem-Schnittstelle konfigurieren“.
3. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
4. Navigieren Sie zu ***interface » cellmodem » {interface} » lte » firmware-upgrade***, wobei *{interface}* die Mobilfunkmodem-Schnittstelle ist.

5. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
repository-url { repository-url }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 256 Zeichen Die URL der Firmware zum Herunterladen. Die URL HTTP, HTTPS, USB und SD werden unterstützt. Zum Aktualisieren von einem USB-Flash-Laufwerk oder einer microSD-Karte (sofern zutreffend) ist das URL-Format "usb://device-name/path-to-file-on-system" bzw. "sd://device-name/path-to-file-on-system". Um den Gerätenamen zu bestimmen, legen Sie Ihr Speichermedium ein und navigieren Sie zu "chassis", "storage", "removable" (WebUI) oder geben Sie "show chassis" ein. Bei allen anderen Protokollen ist das Format: "protocol://host:port/path-to-file". Bei Verwendung des für das Protokoll voreingestellten Ports, lassen Sie ":port" weg.
username { username }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 64 Zeichen Der zum Verbinden mit dem Upgrade-Server erforderliche Benutzername.
password { password }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 1024 Zeichen Das Passwort zum Benutzernamen.
mode { mode }	**Zusammenfassung:** { manual-check-and-update, auto-check-manual-update, auto-check-and-update } **Standard:** manual-check-and-update Der Aktualisierungsmodus. Mögliche Optionen sind: * manual-check-and-update - FOTA prüft und installiert die Firmware, wenn der Benutzer dies veranlasst * auto-check-manual-update - FOTA prüft automatisch auf neue Firmware und installiert Updates, wenn der Benutzer dies veranlasst * auto-check-and-update - FOTA prüft automatisch auf neue Firmware und installiert Updates
interval { interval }	**Zusammenfassung:** Eine vorzeichenlose 16-Bit-Ganzzahl zwischen 1 und 365 **Standard:** 90 Die Anzahl der Tage, die gewartet werden muss, bevor automatisch auf neue Firmware geprüft wird.

6. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 10.6.7.3
Firmware-Update durchführen

Um manuell ein Firmware-Update zu starten, gehen Sie wie folgt vor:



HINWEIS
Falls das Upgrade nicht möglich ist, siehe Abschnitt 19.5, „Fehlerbehebung bei Firmware-Updates“.

1. Stellen Sie sicher, dass der Modus des Firmware-Updates konfiguriert ist. Weitere Informationen finden Sie unter Abschnitt 10.6.7.2, „Konfigurieren des Firmware-Update-Modus und der -Quelle“.
2. Wenn Sie das Gerät über USB/MicroSD aktualisieren, legen Sie das Speichermedium in das Gerät ein.
3. Führen Sie das Firmware-Update durch, indem Sie Folgendes eingeben:

```
interfaces cellmodem interface firmware-update
```

Erläuterung:

- *interface* ist die Schnittstelle des Mobilfunkmodems.

11 Tunnel und VPNs

In diesem Kapitel wird beschrieben, wie Sie Tunnel und Virtual Private Networks (VPN) konfigurieren können.

INHALT

- Abschnitt 11.1, „Verwalten von virtuellen Switches“
- Abschnitt 11.2, „Den Layer-2-Tunnel-Daemon verwalten“
- Abschnitt 11.3, „L2TP-Tunnel verwalten“
- Abschnitt 11.4, „L2TPv3-Tunnel verwalten“
- Abschnitt 11.5, „Verwalten von GOOSE-Tunneln“
- Abschnitt 11.6, „Generische Tunnel verwalten“
- Abschnitt 11.7, „GRE (Generic Routing Encapsulation)-Tunnel verwalten“
- Abschnitt 11.8, „IPsec-Tunnel verwalten“
- Abschnitt 11.9, „6in4- und 4in6-Tunnel verwalten“
- Abschnitt 11.10, „DMVPN verwalten“

Abschnitt 11.1

Verwalten von virtuellen Switches

Virtuelle Switches überbrücken verschiedene Netzwerksegmente in einer Art und Weise, die unabhängig von bestimmten Protokollen ist.

Der Netzwerkdatenverkehr zwischen den Segmenten wird unabhängig von den im Paket festgelegten IP- und MAC-Adressen weitergeleitet. In einem virtuellen Switch erfolgt die Weiterleitung in Layer 2 und erlaubt, den gesamten Netzwerkverkehr, einschließlich Layer-2-Multicast- (d.h. GOOSE, ISO), IP Multicast-, Unicast- und Broadcast-Nachrichten, ohne Änderungen durch den Tunnel des virtuellen Switch zu leiten.

Ein virtueller Switch kann insbesondere für das GOOSE Messaging nützlich sein, wenn Sender und Empfänger über ein routingfähiges IP-Netzwerk kommunizieren müssen. Da es keine IP-Kapselung für den durch den virtuellen Switch geführten Layer-2-Verkehr gibt, wird die Latenz für den Verkehr zwischen den Endgeräten minimiert.

Der virtuelle Switch wird auf dem Gerät als virtuelle Ethernet-Schnittstelle über einer physischen Schnittstelle (d.h. Ethernet-Port) zwischen zwei Routern angezeigt. Die beiden Router können sich physisch an verschiedenen Standorten befinden.

In einem Router können mehrere Instanzen virtueller Switches vorhanden sein. Jede Instanz kann zwei oder mehr Schnittstellen haben, jedoch kann eine Schnittstelle nur ein Mitglied einer Instanz eines virtuellen Switch sein.

Eine Schnittstelle des virtuellen Switch in einem Router kann eine routingfähige Schnittstelle sein, wenn eine IP-Adresse entweder statisch oder über DHCP zugewiesen wird. Die der Schnittstelle des virtuellen Switch zugewiesene Netzwerkadresse kann in das dynamische Routing-Protokoll aufgenommen werden. Die Schnittstelle

kann auch ein Routing-Update aufrufen. Die dem virtuellen Switch zugewiesene IP-Adresse kann als Standard-Gateway für die Endgeräte verwendet werden, die mit der Schnittstelle des virtuellen Switch verbunden sind. Netzwerkdienste (z. B. SSH, DHCP, NTP, VRRP usw.) können so konfiguriert werden, dass sie an der Schnittstelle des virtuellen Switch ausgeführt werden.

Der Netzwerkdatenverkehr kann für ausgewählte Schnittstellen des virtuellen Switch in Abhängigkeit der MAC-Zieladresse, MAC-Quelladresse und/oder des Protokolls (z. B. iso, arp, ipv4, ipv6 usw.) gefiltert werden. Erfüllt ein Paket die Filterkriterien, wird es zum entsprechenden Ziel geroutet. Andernfalls wird es verworfen.

Achten Sie bei der Konfiguration eines virtuellen Switch auf Folgendes:

- Gehen Sie beim Hinzufügen einer (einem Switch-Port an einem vorhandenen Line-Modul zugewiesenen) VLAN-Schnittstelle in einem virtuellen Switch sorgfältig vor. Der VLAN-Tag an einem markierten (getaggten) Frame, der an der VLAN-Schnittstelle eines Switch-Ports empfangen wurde, darf nicht beibehalten werden, wenn der Verkehr über eine routingfähige Schnittstelle (d.h. cel1 oder switch.0001), die auch Teil derselben Instanz des virtuellen Switch ist, in die ausgehende Richtung geleitet wird. Ein VLAN-Tag wird jedoch beibehalten, wenn markierter Verkehr an einer routingfähigen Schnittstelle empfangen wird.
- Einer Schnittstelle zugewiesene IP-Adressen werden inaktiv und ausgeblendet, wenn die Schnittstelle zum virtuellen Switch hinzugefügt wird. Die Adresse an der Schnittstelle wird reaktiviert, nachdem die Schnittstelle aus dem virtuellen Switch entfernt wurde.
- Gehen Sie beim Hinzufügen einer Schnittstelle zum virtuellen Switch vorsichtig vor. Netzwerkdienste, die an den einzelnen Schnittstellen ausgeführt werden, müssen nach dem Hinzufügen der Schnittstelle zum virtuellen Switch neu konfiguriert werden. Wenn ein auf switch.0001 laufender DHCP-Server beispielsweise anschließend zu einem Mitglied des virtuellen Switch vsw-1 gemacht wird, muss die DHCP-Konfiguration so geändert werden, dass sie auf vsw-1 verweist.
- Der virtuelle Switch wird in der RUGGEDCOM ROX II-Software implementiert. Aufgrund dessen wird eine CPU-Ressource zum Weiterleiten des Broadcast-, Multicast- und Unicast-Datenverkehrs benötigt.
- Wenn der Router als Firewall läuft, muss der Parameter **routeback** unter ***firewall » fwconfig » fwinterface*** für die Schnittstelle des virtuellen Switch aktiviert werden. Weitere Informationen finden Sie unter Abschnitt 6.7.9, „Schnittstellen verwalten“.

INHALT

- Abschnitt 11.1.1, „Eine Liste virtueller Switches anzeigen“
- Abschnitt 11.1.2, „Hinzufügen eines virtuellen Switch“
- Abschnitt 11.1.3, „Einen virtuellen Switch löschen“
- Abschnitt 11.1.4, „Schnittstellen für virtuelle Switches verwalten“
- Abschnitt 11.1.5, „Verkehr über einen virtuellen Switch filtern“
- Abschnitt 11.1.6, „Filterregeln verwalten“
- Abschnitt 11.1.7, „In/Out-Schnittstellen verwalten“
- Abschnitt 11.1.8, „VLANs für virtuelle Switches verwalten“

Abschnitt 11.1.1

Eine Liste virtueller Switches anzeigen

Um eine Liste der virtuellen Switches anzusehen, geben Sie Folgendes ein:

```
show running-config interface virtualswitch
```

Falls virtuelle Switches konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config interface virtualswitch
interface
 virtualswitch vs1
  retain-ip
  no alias
  no proxyarp
  interface fe-cm-1
  !
 !
!
```

Falls keine virtuellen Switches konfiguriert wurden, fügen Sie je nach Bedarf Switches hinzu. Weitere Informationen finden Sie unter Abschnitt 11.1.2, „Hinzufügen eines virtuellen Switch“.

Abschnitt 11.1.2

Hinzufügen eines virtuellen Switch

Um einen virtuellen Switch hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den virtuellen Switch hinzu, indem Sie Folgendes eingeben:

   ```
   interface virtualswitch name
   ```

   Erläuterung:

   - *name* ist die dem virtuellen Switch zugeordnete Bezeichnung
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
enabled	**Zusammenfassung:** { true, false } **Standard:** true Aktiviert diese Schnittstelle.
retain-ip	**Zusammenfassung:** { true, false } **Standard:** false IP an Bridge-Gerät speichern
forward-delay { forward-delay }	**Zusammenfassung:** Vorzeichenlose 8-Bit-Ganzzahl **Standard:** 15 Verzögerung (in Sekunden) des empfangenden und lernenden Zustands, bevor der weiterleitende Zustand eintritt.
alias { alias }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 64 Zeichen Der SNMP-Aliasname der Schnittstelle.
ip-address-src { ip-address-src }	**Zusammenfassung:** { static, dynamic } **Standard:** static Zeigt an, ob die IP-Adresse statisch oder dynamisch über DHCP oder BOOTP zugewiesen ist.
ipv6-address-src { ipv6-address-src }	**Zusammenfassung:** { static, dynamic } **Standard:** static Zeigt an, ob die IPv6-Adresse statisch oder dynamisch über DHCPv6 zugewiesen ist.

Parameter	Beschreibung
proxyarp	Aktiviert/deaktiviert, dass der Port auf ARP-Anfragen für andere Hosts als sich selbst antwortet

4. Fügen Sie eine oder mehrere Schnittstellen zum virtuellen Switch hinzu. Weitere Informationen finden Sie unter Abschnitt 11.1.4.2, „Hinzufügen einer Schnittstelle des virtuellen Switch“.
5. [Optional] Weisen Sie dem virtuellen Switch ein oder mehrere VLANs zu. Weitere Informationen finden Sie unter Abschnitt 11.1.8.2, „Ein VLAN auf Basis eines virtuellen Switch hinzufügen“.
6. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.1.3
Einen virtuellen Switch löschen

Um einen virtuellen Switch zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den ausgewählten virtuellen Switch durch Eingabe von:

   ```
   no interface virtualswitch name
   ```

   Erläuterung:

   - *`name`* ist die dem virtuellen Switch zugeordnete Bezeichnung
3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.1.4
Schnittstellen für virtuelle Switches verwalten

Dieser Abschnitt beschreibt, wie Sie Schnittstellen für virtuelle Switches konfigurieren und verwalten können.

INHALT

- Abschnitt 11.1.4.1, „Eine Liste von Schnittstellen für virtuelle Switches anzeigen“
- Abschnitt 11.1.4.2, „Hinzufügen einer Schnittstelle des virtuellen Switch“
- Abschnitt 11.1.4.3, „Eine Schnittstelle des virtuellen Switch löschen“

Abschnitt 11.1.4.1
Eine Liste von Schnittstellen für virtuelle Switches anzeigen

Um eine Liste von Schnittstellen für virtuelle Switches anzusehen, geben Sie Folgendes ein:

```
show running-config interface virtualswitch name interface
```

Erläuterung:

- *`name`* ist die dem virtuellen Switch zugeordnete Bezeichnung

Falls Schnittstellen für virtuelle Switches konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config interface virtualswitch vs1 interface | tab
NAME
-----------------
switch.0100


 !
!
```

Falls keine Schnittstellen für virtuelle Switches konfiguriert wurden, fügen Sie je nach Bedarf Schnittstellen hinzu. Weitere Informationen finden Sie unter Abschnitt 11.1.4.2, „Hinzufügen einer Schnittstelle des virtuellen Switch“.

Abschnitt 11.1.4.2

Hinzufügen einer Schnittstelle des virtuellen Switch

Um eine Schnittstelle des virtuellen Switch hinzuzufügen, gehen Sie wie folgt vor:

WICHTIG!
Es sind mindestens zwei Schnittstellen für eine Bridge eines virtuellen Switch erforderlich.

ACHTUNG!
Zugriffsrisiko – Gefahr einer Unterbrechung des Zugriffs. Wählen Sie nicht die Schnittstelle, die für den Zugriff auf die Web-Schnittstelle verwendet wird. Aktive Web-Sitzungen gehen verloren und die Web-Schnittstelle ist dann solange nicht erreichbar, bis der virtuelle Switch deaktiviert ist.

HINWEIS
*Die Schnittstelle **wlan-cl1** wird nicht als Schnittstelle des virtuellen Switch unterstützt.*

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie eine Schnittstelle zum virtuellen Switch hinzu, indem Sie Folgendes eingeben:

   ```
   interface virtualswitch name interface interface
   ```

   Erläuterung:

   - *name* ist die dem virtuellen Switch zugeordnete Bezeichnung
   - *interface* ist die der Schnittstelle zugewiesene Bezeichnung

   Auf die neue Schnittstelle kann nun zugegriffen werden, indem Sie Folgendes eingeben:

   ```
   ip vsw-name
   ```

   Der neue virtuelle Switch ist nun im Menü **ip** mit dem Präfix *vsw-* (d. h. vsw-vs1, vsw-vs2 usw.) sichtbar.
3. Weisen Sie der Schnittstelle eine IPv4- oder IPv6-Adresse zu. Weitere Informationen finden Sie in Abschnitt 7.1.3.2, „Eine IPv4-Adresse hinzufügen“ oder Abschnitt 7.1.4.2, „Eine IPv6-Adresse hinzufügen“.
4. Weisen Sie bei Bedarf der Schnittstelle des virtuellen Switch ein oder mehrere VLANs zu. Weitere Informationen finden Sie unter Abschnitt 11.1.8.2, „Ein VLAN auf Basis eines virtuellen Switch hinzufügen“.
5. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.1.4.3
Eine Schnittstelle des virtuellen Switch löschen

Um eine Schnittstelle des virtuellen Switch zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die Schnittstelle des virtuellen Switch, indem Sie Folgendes eingeben:

   ```
   no interface virtualswitch name interface interface
   ```

   Erläuterung:

   - *name* ist die dem virtuellen Switch zugeordnete Bezeichnung
   - *interface* ist die der Schnittstelle zugewiesene Bezeichnung
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.1.5
Verkehr über einen virtuellen Switch filtern

Pakete, die über einen virtuellen Switch übertragen werden, können nach MAC-Quelladresse, MAC-Zieladresse und/oder Protokoll (z. B. iso, arp, ipv4, ipv6 usw.) gefiltert werden. Die Filterregeln werden separat festgelegt und können je nach Bedarf für jeden virtuellen Switch einzeln angewandt werden. Beispielsweise kann ein einzelner Filter Verkehr zu einer bestimmten MAC-Adresse, der über fe-cm-1 eingeht, erkennen und an switch-001 umleiten. Gleichzeitig kann er andere Verkehrstypen erkennen und ablehnen.

INHALT

- Abschnitt 11.1.5.1, „Aktivieren/Deaktivieren der Filterung für virtuelle Switches“
- Abschnitt 11.1.5.2, „Eine Liste von Filtern für virtuelle Switches anzeigen“
- Abschnitt 11.1.5.3, „Hinzufügen eines Filters für den virtuellen Switch“
- Abschnitt 11.1.5.4, „Einen Filter des virtuellen Switch löschen“

Abschnitt 11.1.5.1
Aktivieren/Deaktivieren der Filterung für virtuelle Switches

Um die Filterung für virtuelle Switches zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Aktivieren oder deaktivieren Sie die Filterung für virtuelle Switches, indem Sie Folgendes eingeben:

   Aktivieren der Filterung für virtuelle Switches

   ```
   security virtualswitch-filter enabled
   ```

   Deaktivieren der Filterung für virtuelle Switches

   ```
   no security virtualswitch-filter enabled
   ```
3. Sofern aktiviert, aktivieren Sie **Retain IP on Bridge Device** für die relevanten virtuellen Switches. Diese Funktion aktiviert/deaktiviert die Fähigkeit des Switch, sich die IP-Adresse einer Ethernet-Schnittstelle zu merken, wenn diese zum Bridge-Gerät hinzugefügt wird. Im aktivierten Zustand wird die IP-Adresse

gespeichert, und auf den Router kann dezentral über die Ethernet-Schnittstelle zugegriffen werden. Im deaktivierten Zustand muss die IP-Adresse dem Bridge-Gerät zugewiesen werden, um dezentral auf den Router zuzugreifen.

Weitere Informationen über das Aktivieren/Deaktivieren der Funktion **Retain IP on Bridge Device** finden Sie in Abschnitt 11.1.2, „Hinzufügen eines virtuellen Switch“.

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.1.5.2
Eine Liste von Filtern für virtuelle Switches anzeigen

Um eine Liste von Filtern für virtuelle Switches anzusehen, geben Sie Folgendes ein:

```
show running-config security virtualswitch-filter virtualswitch
```

Falls Filter konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config security virtualswitch-filter virtualswitch | tab
IF
NAME  NAME   ROUTE  NAME         NAME
-----------------------------------------------
vs1
      arp    X
      ipv4   X
      ipv6   -
                    switch.0010
                                 switch.0020
      iso    -
                    switch.0010
                                 switch.0020
      goose  -
                    switch.0010
                                 switch.0020

 !
!
```

Falls keine Filter für virtuelle Switches konfiguriert wurden, fügen Sie je nach Bedarf Filter hinzu. Weitere Informationen finden Sie unter Abschnitt 11.1.5.3, „Hinzufügen eines Filters für den virtuellen Switch“.

Abschnitt 11.1.5.3
Hinzufügen eines Filters für den virtuellen Switch

Um einen Filter für den virtuellen Switch hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Stellen Sie sicher, dass einer oder mehrere virtuelle Switches konfiguriert sind. Weitere Informationen finden Sie unter Abschnitt 11.1.2, „Hinzufügen eines virtuellen Switch“.
3. Fügen Sie den Filter für den virtuellen Switch hinzu, indem Sie Folgendes eingeben:

   ```
   security virtualswitch-filter virtualswitch interface
   ```

   Erläuterung:

   - *`interface`* ist eine Schnittstelle des virtuellen Switch

4. Konfigurieren Sie eine oder mehrere Regeln, die bei der Filterung verwendet werden. Weitere Informationen finden Sie unter Abschnitt 11.1.6.3, „Eine Regel hinzufügen“.
5. Fügen Sie die gewünschten Regeln zum Filter für den virtuellen Switch hinzu. Weitere Informationen finden Sie unter Abschnitt 11.1.6.4, „Eine Regel zum Filter des virtuellen Switch hinzufügen“.
6. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.1.5.4
Einen Filter des virtuellen Switch löschen

Um einen Filter des virtuellen Switch zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den Filter für den virtuellen Switch durch Eingabe von:

   ```
   no security virtualswitch-filter virtualswitch name
   ```

   Erläuterung:

   - *`name`* ist die Bezeichnung des Filters für den virtuellen Switch
3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.1.6
Filterregeln verwalten

Ein virtueller Switch-Filter kann ein oder mehrere Regeln auf den Verkehr, der über einen virtuellen Switch läuft, anwenden.

INHALT

- Abschnitt 11.1.6.1, „Eine Liste der Regeln anzeigen“
- Abschnitt 11.1.6.2, „Eine Liste von Regeln zum Filter des virtuellen Switch anzeigen“
- Abschnitt 11.1.6.3, „Eine Regel hinzufügen“
- Abschnitt 11.1.6.4, „Eine Regel zum Filter des virtuellen Switch hinzufügen“
- Abschnitt 11.1.6.5, „Eine Regel löschen“
- Abschnitt 11.1.6.6, „Eine Regel aus einem Filter des virtuellen Switches löschen“

Abschnitt 11.1.6.1
Eine Liste der Regeln anzeigen

Um eine Liste der Regeln anzusehen, die von einem Filter für virtuelle Switches verwendet werden können, geben Sie Folgendes ein:

```
show running-config security virtualswitch-filter rules
```

Falls Regeln konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config security virtualswitch-filter rules | tab
NAME   ACTION  SRCMAC             DSTMAC             PROTO
-------------------------------------------------------------
arp    accept  -                  -                  arp
goose  accept  00:00:00:00:11:11  01:0c:cd:01:00:33  0x88b8
ipv4   accept  00:00:00:00:00:01  00:00:00:00:00:02  ipv4
ipv6   accept  -                  -                  ipv6
iso    accept  -                  -                  iso

 !
!
```

Falls keine Regeln konfiguriert wurden, fügen Sie je nach Bedarf Regeln hinzu. Weitere Informationen finden Sie unter Abschnitt 11.1.6.3, „Eine Regel hinzufügen“.

Abschnitt 11.1.6.2

Eine Liste von Regeln zum Filter des virtuellen Switch anzeigen

Um eine Liste von Regeln zum Filter des virtuellen Switch anzuzeigen, geben Sie Folgendes ein:

```
show running-config security virtualswitch-filter virtualswitch name rule
```

Erläuterung:

- *name* ist die Bezeichnung des Filters für den virtuellen Switch

Falls Regeln zugewiesen wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config security virtualswitch-filter virtualswitch vs1 rule | tab
NAME   ROUTE  NAME         NAME
---------------------------------------
arp    X
ipv4   X
ipv6   -
               switch.0010
                            switch.0020
iso    -
               switch.0010
                            switch.0020
goose  -
               switch.0010
                            switch.0020

  !
 !
!
```

Falls keine Regeln zugewiesen wurden, weisen Sie diese nach Bedarf zu. Weitere Informationen finden Sie unter Abschnitt 11.1.6.4, „Eine Regel zum Filter des virtuellen Switch hinzufügen“.

Abschnitt 11.1.6.3

Eine Regel hinzufügen

Um eine Regel hinzuzufügen, die von einem Filter des virtuellen Switch verwendet werden kann, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.

2. Stellen Sie sicher, dass einer oder mehrere virtuelle Switches konfiguriert sind. Weitere Informationen finden Sie unter Abschnitt 11.1.2, „Hinzufügen eines virtuellen Switch“.
3. Fügen Sie den Filter für den virtuellen Switch hinzu, indem Sie Folgendes eingeben:

```
security virtualswitch-filter rules rule
```

Erläuterung:

- *rule* ist die Bezeichnung der Regel

4. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
action { action }	**Zusammenfassung:** { accept, drop } **Standard:** accept Der Vorgang, wenn ein eingehendes Frame den Kriterien entspricht.
srcmac { srcmac }	**Zusammenfassung:** Eine Zeichenkette mit 17 Zeichen Die für eingehende Frames erforderliche MAC-Quelladresse.
dstmac { dstmac }	**Zusammenfassung:** Eine Zeichenkette mit 17 Zeichen Die für eingehende Frames erforderliche MAC-Zieladresse.
proto { proto }	**Zusammenfassung:** { iso, arp, ipv4, ipv6 } oder eine Zeichenkette Das vordefinierte Protokoll oder 6-stellige Zeichenkette (wie 0x88A2) zum Erstellen von Frames. Dieser Parameter ist obligatorisch.

5. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.
6. Fügen Sie die Regel zum Filter des virtuellen Switch hinzu. Weitere Informationen finden Sie unter Abschnitt 11.1.6.4, „Eine Regel zum Filter des virtuellen Switch hinzufügen“.

Abschnitt 11.1.6.4

Eine Regel zum Filter des virtuellen Switch hinzufügen

Um eine Regel zum Filter des virtuellen Switch hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie die Regel hinzu, indem Sie Folgendes eingeben:

```
security virtualswitch-filter virtualswitch name rule rule
```

Erläuterung:

- *name* ist die Bezeichnung des Filters für den virtuellen Switch
- *rule* ist die Bezeichnung der Regel

3. Konfigurieren Sie das IN/OUT-Interface für die Regel. Für weitere Informationen siehe Abschnitt 11.1.7.2, „Ein IN/OUT-Interface hinzufügen“.
4. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.1.6.5
Eine Regel löschen

Um eine Regel für die Filterung des virtuellen Switch-Verkehrs zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die Regel durch Eingabe von:

   ```
   no security virtualswitch-filter rules rule
   ```

   Erläuterung:

   - *rule* ist die Bezeichnung der Regel
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.1.6.6
Eine Regel aus einem Filter des virtuellen Switches löschen

Um eine Regel aus einem Filter des virtuellen Switches zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den Filter, indem Sie Folgendes eingeben:

   ```
   no security virtualswitch-filter virtualswitch name rule rule
   ```

   Erläuterung:

   - *name* ist die Bezeichnung des Filters für den virtuellen Switch
   - *rule* ist die Bezeichnung der Regel
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.1.7
In/Out-Schnittstellen verwalten

In/Out-Schnittstellen für virtuelle Switch-Filter stellen die Schnittstelle dar, die durch den Filter (*in*-Schnittstelle) überwacht wird, und die Ziel-Schnittstelle (*out*-Schnittstelle) für den Netzwerkverkehr, der die Filterkriterien erfüllt.

INHALT

- Abschnitt 11.1.7.1, „Eine Liste der IN/OUT-Interfaces anzeigen“
- Abschnitt 11.1.7.2, „Ein IN/OUT-Interface hinzufügen“
- Abschnitt 11.1.7.3, „Ein IN/OUT-Interface löschen“

Abschnitt 11.1.7.1
Eine Liste der IN/OUT-Interfaces anzeigen

Um eine Liste der IN/OUT-Interfaces, die von einem Filter für virtuelle Switches verwendet werden können, anzuzeigen, geben Sie Folgendes ein:

```
show running-config security virtualswitch-filter virtualswitch name rule rule [ in-interface | out-interface ]
```

Erläuterung:

- *name* ist die Bezeichnung des Filters für den virtuellen Switch
- *rule* ist die Bezeichnung der Regel

Falls IN/OUT-Interfaces konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config security virtualswitch-filter virtualswitch vs1 rule in-interface | tab
NAME   NAME
--------------------
ipv6
       switch.0010
iso
       switch.0010
goose
       switch.0010

  !
 !
!
```

Falls keine IN/OUT-Interfaces konfiguriert wurden, fügen Sie je nach Bedarf Interfaces hinzu. Für weitere Informationen siehe Abschnitt 11.1.7.2, „Ein IN/OUT-Interface hinzufügen“.

Abschnitt 11.1.7.2
Ein IN/OUT-Interface hinzufügen

Um ein IN/OUT-Interface hinzufügen, das von einem Filter des virtuellen Switch verwendet werden kann, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie das IN/OUT-Interface hinzu, indem Sie Folgendes eingeben:

   ```
   security virtualswitch-filter virtualswitch name rule rule [ in-interface | out-interface ] interface
   ```

   Erläuterung:

   - *name* ist die Bezeichnung des Filters für den virtuellen Switch
   - *rule* ist die Bezeichnung der Regel
   - *interface* ist die Bezeichnung der Schnittstelle
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.1.7.3
Ein IN/OUT-Interface löschen

Um ein IN/OUT-Interface zu löschen, das von einem Filter des virtuellen Switch verwendet werden kann, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie das Interface, indem Sie Folgendes eingeben:

   ```
   no security virtualswitch-filter virtualswitch name rule rule [ in-interface | out-interface ]
   interface
   ```

   Erläuterung:

   - *name* ist die Bezeichnung des Filters für den virtuellen Switch
   - *rule* ist die Bezeichnung der Regel
   - *interface* ist die Bezeichnung der Schnittstelle
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.1.8
VLANs für virtuelle Switches verwalten

Dieser Abschnitt beschreibt, wie Sie VLANs für virtuelle Switches konfigurieren und verwalten können.

INHALT

- Abschnitt 11.1.8.1, „Eine Liste von VLANs für virtuelle Switches anzeigen“
- Abschnitt 11.1.8.2, „Ein VLAN auf Basis eines virtuellen Switch hinzufügen“
- Abschnitt 11.1.8.3, „Ein VLAN auf Basis von virtuellen Switches löschen“

Abschnitt 11.1.8.1
Eine Liste von VLANs für virtuelle Switches anzeigen

Um eine Liste von VLANs für virtuelle Switches anzusehen, geben Sie Folgendes ein:

```
show running-config interface virtualswitch id vlan
```

Erläuterung:

- *id* ist die dem virtuellen Switch zugeordnete ID

Falls VLANs konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config interface virtualswitch 1 vlan | tab
     IP
     ADDRESS
VID  SRC      QOS  INGRESS  MARK
---------------------------------
100  static

 !
!
```

Falls keine VLANs für virtuelle Switches konfiguriert wurden, fügen Sie je nach Bedarf VLANs hinzu. Weitere Informationen finden Sie unter Abschnitt 11.1.8.2, „Ein VLAN auf Basis eines virtuellen Switch hinzufügen“.

Abschnitt 11.1.8.2
Ein VLAN auf Basis eines virtuellen Switch hinzufügen

Um ein VLAN auf Basis eines virtuellen Switch hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie das VLAN hinzu, indem Sie Folgendes eingeben:

```
interface virtualswitch id vlan vlan-id
```

   Erläuterung:

   - *id* ist die dem virtuellen Switch zugeordnete ID
   - *vlan-id* ist die dem VLAN zugewiesene ID

3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
ip-address-src { ip-address-src }	**Zusammenfassung:** { static, dynamic } **Standard:** static Zeigt an, ob die IP-Adresse statisch oder dynamisch über DHCP oder BOOTP zugewiesen ist.
ipv6-address-src { ipv6-address-src }	**Zusammenfassung:** { static, dynamic } **Standard:** static Zeigt an, ob die IPv6-Adresse statisch oder dynamisch über DHCPv6 zugewiesen ist.

4. [Optional] Fügen Sie eine QoS-Map hinzu. Für weitere Informationen siehe Abschnitt 15.2.7.2, „Hinzufügen einer QoS-Map“.
5. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.1.8.3
Ein VLAN auf Basis von virtuellen Switches löschen

Um ein VLAN auf Basis von virtuellen Switches zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie das gewählte VLAN, indem Sie Folgendes eingeben:

```
no interface virtualswitch id vlan vlan-id
```

   Erläuterung:

   - *id* ist die dem virtuellen Switch zugeordnete ID
   - *vlan-id* ist die dem VLAN zugewiesene ID

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.2

Den Layer-2-Tunnel-Daemon verwalten

RUGGEDCOM ROX II kann den Bereich der Dienste, die ausschließlich über Layer-2-Protokolle kommunizieren (d. h. auf Ethernet-Ebene) durch Tunneling über geroutete IP-Netzwerke erweitern. Der Layer-2-Tunnel-Daemon unterstützt das IEC61850 GOOSE-Protokoll ebenso wie einen generischen Mechanismus für das Tunneling nach Ethernet-Typ.

INHALT

- Abschnitt 11.2.1, „RTT-Statistiken anzeigen“
- Abschnitt 11.2.2, „Konfigurieren des Layer-2-Tunnel-Daemon“

Abschnitt 11.2.1

RTT-Statistiken anzeigen

Die Statistiken zur Hin- und Rücklaufzeit (Round Trip Time, RTT) geben die erfasste Hin- und Rücklaufzeit zu jedem entfernten Daemon wieder. Es werden die minimale, durchschnittliche, maximale und die Standardabweichung der Zeiten dargestellt. Einträge mit großen Unterschieden zwischen den Parametern `transmitted` und `received` weisen auf mögliche Probleme hin.

Um die RTT-Statistiken anzuzeigen, geben Sie Folgendes ein:

HINWEIS
RTT-Statistiken sind nur verfügbar, wenn IP-Adressen des entfernten Daemons für generische Tunnel konfiguriert sind. Weitere Informationen über IP-Adressen des entfernten Daemons finden Sie unter Abschnitt 11.6.5, „IP-Adressen entfernter Daemons für generische Tunnel verwalten“.

```
show tunnel l2tunneld status round-trip-time
```

Eine Tabelle oder Liste ähnlich dem folgenden Beispiel wird angezeigt:

```
ruggedcom# show tunnel l2tunneld status round-trip-time
                                    MINIMUM   AVERAGE   MAXIMUM
REMOTE IP    TRANSMITTED  RECEIVED  RTT       RTT       RTT       DEVIATION
-------------------------------------------------------------------------------
192.168.5.1  45           42        0.277000  0.917000  3.735000  0.556000
```

Diese Tabelle oder Liste liefert die folgenden Informationen:

Parameter	Beschreibung
remote-ip	**Zusammenfassung:** Eine Zeichenkette mit 7 bis 15 Zeichen Die IP-Adresse des entfernten Dämon. Dieser Parameter ist obligatorisch.
transmitted	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl der durch den Tunnel übertragenen Beacon-Frames. Dieser Parameter ist obligatorisch.
received	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl der durch den Tunnel empfangenen Beacon-Frames. Dieser Parameter ist obligatorisch.

Parameter	Beschreibung
minimum-rtt	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 32 Zeichen Die minimale Hin- und Rücklaufzeit des Beacon. Dieser Parameter ist obligatorisch.
average-rtt	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 32 Zeichen Die durchschnittliche Hin- und Rücklaufzeit des Beacon. Dieser Parameter ist obligatorisch.
maximum-rtt	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 32 Zeichen Die maximale Hin- und Rücklaufzeit des Beacon. Dieser Parameter ist obligatorisch.
deviation	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 32 Zeichen Die Standardabweichung. Dieser Parameter ist obligatorisch.

Abschnitt 11.2.2

Konfigurieren des Layer-2-Tunnel-Daemon

Um den Layer-2-Tunnel-Daemon zu konfigurieren, gehen Sie wie folgt vor:

WICHTIG!
Stellen Sie sicher, dass zwischen dem LAN der Unterstation und anderen LANs, die GOOSE-Frames an das LAN weiterleiten könnten, keine Verkehrsschleifen existieren. Verwenden Sie kein GOOSE-Gateway zwischen bereits verbundenen Unterstationen. Der GOOSE-Daemon gibt Pakete an das Netzwerk mit einem integrierten Time-To-Live-(TTL)-Zähler aus, der mit jeder Übertragung herunterzählt. Dadurch wird eine unendliche Paketschleife verhindert; eine übermäßige Netzwerknutzung wird hingegen nicht verhindert.

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***tunnel » l2tunneld*** und konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
enabled	Aktiviert den Layer-2-Protokollserver.
udp-port { udp-port }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 1 und 65535 **Standard:** 1311 Der UDP-Port zur Kommunikation mit dem anderen Dämon.
beacon-interval { beacon-interval }	**Zusammenfassung:** { off } oder eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 10 und 3600 **Standard:** 60 Die Hin- und Rücklaufzeit (RTT) der gesendeten Nachricht

3. Fügen Sie bei Bedarf GOOSE- oder generische Tunnel hinzu. Weitere Informationen finden Sie in Abschnitt 11.5.3, „Einen GOOSE-Tunnel hinzufügen“ oder Abschnitt 11.6.3, „Hinzufügen eines generischen Tunnels“.
4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.3

L2TP-Tunnel verwalten

Das Layer-2-Tunneling-Protocol (L2TP) wird hauptsächlich für das Tunneln von Point-to-Point-Protocol-(PPP)-Paketen durch ein IP-Netzwerk verwendet, obwohl es auch andere Layer-2-Protokolle tunneln kann.

RUGGEDCOM ROX II verwendet L2TPD zusammen mit Libreswan und PPP, um die Herstellung einer sicheren, privaten Verbindung mit dem Router über den Microsoft Windows VPN/L2TP-Client zu ermöglichen.

WICHTIG!
L2TPD hört am UDP-Port 1701. Ist eine Firewall aktiviert, so muss sie so konfiguriert werden, dass Verbindungen mit L2TPD nur über IPsec möglich sind. Direkte Verbindungen mit L2TPD müssen verhindert werden.

INHALT

- Abschnitt 11.3.1, „Konfigurieren von L2TP-Tunneln“
- Abschnitt 11.3.2, „DNS-Server konfigurieren“
- Abschnitt 11.3.3, „PPP-Optionen konfigurieren“
- Abschnitt 11.3.4, „WINS-Server konfigurieren“

Abschnitt 11.3.1

Konfigurieren von L2TP-Tunneln

Um L2TP-Tunnel zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***tunnel » l2tp*** und konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
enabled	Aktiviert L2TP. **HINWEIS** *Das Aktivieren von L2TP erfordert, dass "l2tpv3/dynamic/enabled" und "l2tpv3/dynamic/mode" auf Ins eingestellt sind*
local-ip { local-ip }	**Zusammenfassung:** Eine Zeichenkette mit 7 bis 15 Zeichen Die lokale IP-Adresse. Bei Einstellung verwenden alle L2TP-Schnittstellen (l2tp-ppp-0, l2tp-ppp-1, usw.) dieselbe IP-Adresse. Um verschiedene lokale IP-Adressen (aus einem IP-Pool) für verschiedene L2TP-Schnittstellen zu verwenden, lassen Sie diesen Parameter leer.
first-ip { first-ip }	**Zusammenfassung:** Eine Zeichenkette mit 7 bis 15 Zeichen Die erste Adresse im IP-Adress-Pool. Ist "local-ip" nicht eingestellt, werden sowohl lokale als auch entfernte IP-Adressen aus diesem Pool genommen.
max-connection { max-connection }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 1 und 10 Die maximale Anzahl an Verbindungen.
closing-wait-timeout { closing-wait-timeout }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 5 und 120 **Standard:** 60

Parameter	Beschreibung
	Die Anzahl an Sekunden Wartezeit, bevor der Tunnel gesäubert wird, nachdem der Tunnel in den Status "closing-wait" wechselt.

3. Konfigurieren Sie Domain Name System (DNS)- oder Windows Internet Name Service (WINS)-Server. Weitere Informationen finden Sie unter Abschnitt 11.3.2, „DNS-Server konfigurieren“ oder Abschnitt 11.3.4, „WINS-Server konfigurieren“.
4. Konfigurieren Sie L2TP-Tunnel für Point-to-Point-Protocol-(PPP)-Sitzungen. Weitere Informationen finden Sie unter Abschnitt 11.3.3, „PPP-Optionen konfigurieren“.
5. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.3.2
DNS-Server konfigurieren

Um redundante Domain-Name-System-(DNS-)Server für L2TP-Tunnel zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Zum Konfigurieren der primären und sekundären DNS-Server geben Sie Folgendes ein:

```
tunnel l2tp dns-server primary primary-ip secondary secondary-ip
```

   Erläuterung:

   - *`primary-ip`* ist die IP-Adresse des primären DNS-Servers
   - *`secondary-ip`* ist die IP-Adresse des sekundären DNS-Servers

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.3.3
PPP-Optionen konfigurieren

Um L2TP-Tunnel für PPP-(Point-to-Point-Protocol)-Sitzungen zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***tunnel » l2tp » ppp*** und konfigurieren Sie den/die folgenden Parameter nach Bedarf:

   HINWEIS
   *Ist **Authorize Locally** nicht aktiviert, verwendet L2TP die RADIUS-Authentifizierung. Weitere Informationen zum Konfigurieren der RADIUS-Authentifizierung für die PPP-Dienste finden Sie unter Abschnitt 6.5.3.2, „Eine RADIUS-Authentifizierung für PPP-Services konfigurieren“.*

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.3.4

WINS-Server konfigurieren

Um redundante Domain-Name-System-(WINS)-Server für L2TP-Tunnel zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Zum Konfigurieren der primären und sekundären WINS-Server geben Sie Folgendes ein:

   ```
   tunnel l2tp WINS-server primary primary-ip secondary secondary-ip
   ```

   Erläuterung:

   - *primary-ip* ist die IP-Adresse des primären WINS-Servers
   - *secondary-ip* ist die IP-Adresse des sekundären WINS-Servers
3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.4

L2TPv3-Tunnel verwalten

L2TPv3 (Layer 2 Tunneling Protocol Version 3) bietet einen Pseudowire-Service, der Multiprotokoll-Layer-2-Verkehr über IP-Netzwerke kapselt. Im Gegensatz zu L2TP gibt es keine Einschränkungen für die Layer-2-Datenformate, die übertragen oder empfangen werden können.

L2TPv3 ist eine vereinfachte Alternative zu MPLS (Multiprotocol Label Switching) mit einer verbesserten Leistung (z. B. hohe Datenpaketrate und geringer CPU-Verbrauch) über L2TP und IP-Netzwerk.

Es gibt zwei Arten von L2TPv3-Tunneln:

- **Statisch**
  Ein statischer L2TPv3-Tunnel ist eine feste Verbindung zwischen zwei Provider Edge (PE)-Geräten, bei der die Sitzungs-IDs und Cookies auf beiden Geräten festgelegt werden. Auf diese Weise können die Geräte den Layer-2-Verkehr weiterleiten, sobald sich die Sitzung mit dem Anschlusskreis verbindet.
- **Dynamisch**
  Ein dynamischer LTPv3-Tunnel erstellt Sitzungen basierend auf dem dynamischen Austausch von Steuernachrichten zwischen den PE-Geräten, um die Art des Layer-2-Verkehrs zu bestimmen, der geroutet werden muss. Sitzungs-IDs und Cookies werden von den Geräten selbst für jede Sitzung generiert. Dadurch kann L2TPv3 bei einem Netzwerkausfall Sitzungen automatisch wieder aufbauen.

WICHTIG!
RUGGEDCOM ROX II unterstützt maximal 128 Tunnel-Sitzungen, die wiederum jeweils maximal 128 VLANs unterstützen.

INHALT

- Abschnitt 11.4.1, „L2TPv3-Tunnelszenarien“
- Abschnitt 11.4.2, „Einen L2TPv3-Tunnel erstellen“
- Abschnitt 11.4.3, „Statische L2TPv3-Tunnel verwalten“
- Abschnitt 11.4.4, „Dynamische L2TPv3-Tunnel verwalten“
- Abschnitt 11.4.5, „Sitzungen für L2TPv3-Tunnel verwalten“

- Abschnitt 11.4.6, „VLANs für L2TPv3-Tunnel verwalten“

Abschnitt 11.4.1

L2TPv3-Tunnelszenarien

Im Folgenden sind einige Möglichkeiten dargestellt, wie L2TPv3-Tunnel eingerichtet werden können.

L2TPv3-Basistunnel

In der folgenden Topologie wird ein L2TPv3-Tunnel zwischen den Routern R1 und R2 über eine WAN-Schnittstelle errichtet. Die Tunnel-Schnittstelle erhält auf beiden Geräten eine IPv4-Adresse. Der von R1 geroutete Datenverkehr wird in einem L2TPv3-Header gekapselt und von R2 entkapselt. Umgekehrt ist es möglich, den Verkehr von R2 aus zu leiten.

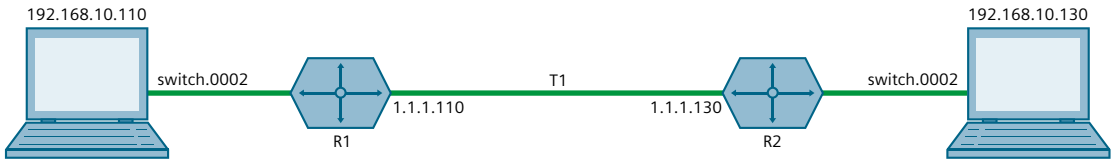


Abbildung 19: L2TPv3-Basistunnel

Mehrfache Sitzungen

In der folgenden Topologie wurden mithilfe von Sitzungen getrennte Bridges zwischen den Routern R1 und R2 errichtet. Der über den virtuellen Switch switch.0002 gesendete Verkehr passiert den l2t-1-1-Tunnel. Der über den virtuellen Switch switch.0003 gesendete Verkehr passiert den l2t-1-2-Tunnel.

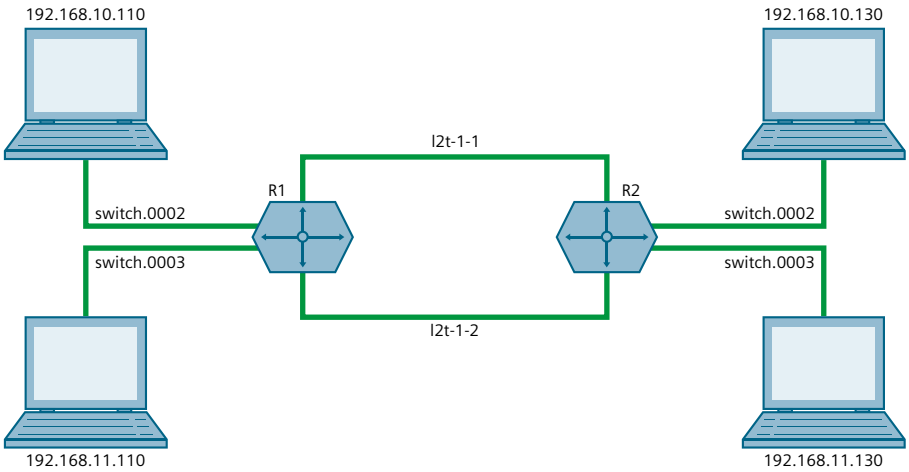


Abbildung 20: Mehrere LAN-Erweiterungen über einen einzelnen L2TPv3-Tunnel

L2TPv3-Mehrfachtunnel

In der folgenden Topologie werden zwei L2TPv3-Tunnel konfiguriert: der eine von Router R1 an R2 und der andere von R1 an R3. Jeder wird durch den virtuellen Switch switch.0002 in eine Bridge umgewandelt.

Der von 192.158.10.110 an 192.168.10.130 gesendete Verkehr passiert die l2t-1-1-Bridge und umgekehrt.

Der von 192.158.10.110 an 192.168.11.110 gesendete Verkehr passiert die l2t-2-1-Bridge und umgekehrt.

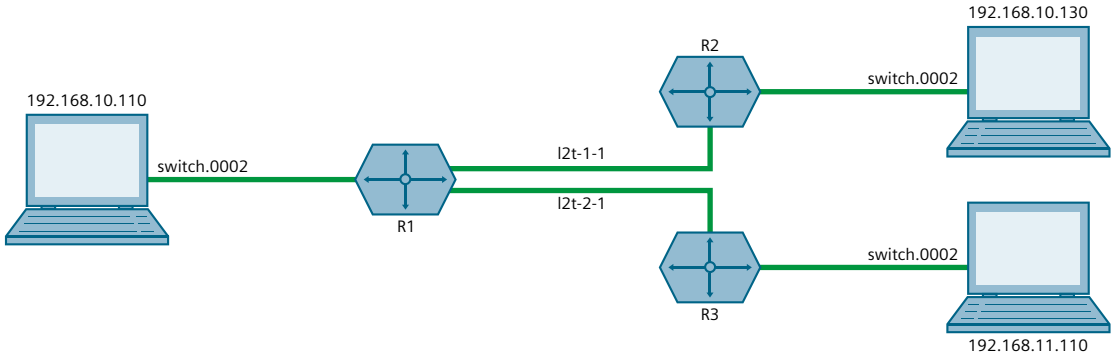


Abbildung 21: Mehrere LAN-Erweiterungen über mehrere L2TPv3-Tunnel

Abschnitt 11.4.2

Einen L2TPv3-Tunnel erstellen

Um einen L2TPv3-Tunnel mit einem anderen Provider Edge (PE)-Gerät zu erstellen, gehen Sie wie folgt vor:

1. **Legen Sie die Schnittstelle des L2TPv3-Tunnels an**

   Eine L2TPv3-Tunnel-Schnittstelle wird automatisch von RUGGEDCOM ROX II immer dann angelegt, wenn eine Sitzung definiert wird. Die Schnittstelle wird im Menü unter **ip** aufgelistet und folgt den folgenden Vorgaben zur Benennung:

   ```
   l2t-{tunnel-name}-{session-name}
   ```

   Beispiel:

   ```
   l2t-1-2
   ```

   Ist der Sitzung eine VLAN-ID zugewiesen, wird eine zusätzliche Schnittstelle in folgendem Format generiert:

   ```
   l2t-{tunnel-name}-{session-name}.{vlan-id}
   ```

   Beispiel:

   ```
   l2t-1-2.0004
   ```

   Um eine Tunnel-Schnittstelle anzulegen, beginnen Sie damit, einen statischen oder dynamischen L2TPv3-Tunnel hinzuzufügen. Für weitere Informationen siehe Abschnitt 11.4.3.3, „Hinzufügen eines statischen L2TPv3-Tunnels“ oder Abschnitt 11.4.4.3, „Hinzufügen eines dynamischen L2TPv3-Tunnels“.

2. **Erstellen Sie einen virtuellen Switch oder weisen Sie eine IP-Adresse zu.**

   Die L2TPv3-Tunnel-Schnittstelle ist eine Ethernet-ähnliche Schnittstelle. Als solche kann sie zu einem virtuellen Switch hinzugefügt werden, um eine Bridge zu bilden, oder einer IP-Adresse zugewiesen werden, um den Layer-3-Verkehr zu leiten.

   Informationen, wie Sie eine L2TPv3-Tunnel-Schnittstelle zu einem virtuellen Switch hinzufügen, finden Sie unter Abschnitt 11.1.4.2, „Hinzufügen einer Schnittstelle des virtuellen Switch“.

   Informationen, wie Sie der L2TPv3-Tunnel-Schnittstelle eine IP-Adresse zuweisen, finden Sie entweder unter Abschnitt 7.1.3, „IPv4-Adressen verwalten“ oder unter Abschnitt 7.1.4, „IPv6-Adressen verwalten“.

Abschnitt 11.4.3
Statische L2TPv3-Tunnel verwalten

Konfigurieren Sie statische L2TPv3-Tunnel für die manuelle Steuerung von Tunnel- und Sitzungsparametern an beiden Enden der Bridge. Diese festen Tunnel werden als *nicht gemanagt* bezeichnet.

INHALT

- Abschnitt 11.4.3.1, „Statische L2TPv3-Tunnel aktivieren/deaktivieren“
- Abschnitt 11.4.3.2, „Eine Liste der statischen L2TPv3-Tunnel anzeigen“
- Abschnitt 11.4.3.3, „Hinzufügen eines statischen L2TPv3-Tunnels“
- Abschnitt 11.4.3.4, „Einen statischen L2TPv3-Tunnel löschen“

Abschnitt 11.4.3.1
Statische L2TPv3-Tunnel aktivieren/deaktivieren

Um statische L2TPv3-Tunnel zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Aktivieren oder deaktivieren Sie statische L2TPv3-Tunnel, indem Sie Folgendes eingeben:

   Zum Aktivieren der Tunnel

   ```
   tunnel l2tpv3 static enabled
   ```

   Zum Deaktivieren der Tunnel

   ```
   no tunnel l2tpv3 static enabled
   ```

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.4.3.2
Eine Liste der statischen L2TPv3-Tunnel anzeigen

Um eine Liste der statischen L2TPv3-Tunnel anzusehen, geben Sie Folgendes ein:

```
show running-config tunnel l2tpv3 static tunnel
```

Falls Tunnel konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config tunnel l2tpv3 static tunnel
tunnel
 l2tpv3 static tunnel 1
  tunnel-id        1
  remote-tunnel-id 2
  transport-encap  udp
  local-ip         192.168.0.10
  local-port       1024
  remote-ip        192.168.0.11
  remote-port      1025
  session 1
   local-session-id       10
   remote-session-id      20
   l2tp-specific-sublayer default
   vlan 4
   !
  !
  session 2
   local-session-id       30
   remote-session-id      40
   l2tp-specific-sublayer default
  !
 !
!
```

Falls keine Tunnel konfiguriert wurden, fügen Sie je nach Bedarf Tunnel hinzu. Weitere Informationen finden Sie unter Abschnitt 11.4.3.3, „Hinzufügen eines statischen L2TPv3-Tunnels“.

Abschnitt 11.4.3.3

Hinzufügen eines statischen L2TPv3-Tunnels

Um einen statischen L2TPv3-Tunnel hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.

   HINWEIS
   Der Tunnelname muss aus einem bis drei numerischen und/oder alphanumerischen Kleinbuchstaben bestehen.

2. Fügen Sie den Tunnel hinzu, indem Sie Folgendes eingeben:

   ```
   tunnel l2tpv3 static tunnel name
   ```

   Erläuterung: *name* ist die Bezeichnung des Tunnels.

3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
aktiviert	**Zusammenfassung:** { true, false } **Standard:** false Aktiviert den Static L2TPv3 Tunnel.
tunnel-id	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl Lokale Tunnel-ID Dieser Parameter ist obligatorisch.
remote-tunnel-id	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl Die dezentrale Tunnel-ID

Parameter	Beschreibung
	Dieser Parameter ist obligatorisch.
transport-encap	**Zusammenfassung:** Eine Zeichenkette Die Transport-Einkapselung (UDP oder IP). Dieser Parameter ist obligatorisch.
local-ip	**Zusammenfassung:** Eine Zeichenkette Die Schnittstelle, an der der Tunnel erstellt wird. Dieser Parameter ist obligatorisch.
local-port	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl Lokaler Transportport für L2TPv3-Dienst Dieser Parameter ist obligatorisch.
remote-ip	**Zusammenfassung:** Eine Zeichenkette mit 6 bis 40 Zeichen IP-Adresse des entfernten Tunnelendes Dieser Parameter ist obligatorisch.
remote-port	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl Transportport des entfernten Tunnelendes Dieser Parameter ist obligatorisch.
status	**Zusammenfassung:** Eine Zeichenkette Aktueller Status des Tunnels Dieser Parameter ist obligatorisch.

4. Fügen Sie eine oder mehrere Sitzungen zur Tunnelkonfiguration hinzu. Weitere Informationen finden Sie unter Abschnitt 11.4.5.2, „Hinzufügen einer Sitzung“.
5. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.4.3.4
Einen statischen L2TPv3-Tunnel löschen

Um einen statischen L2TPv3-Tunnel zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den Tunnel durch Eingabe von:

```
no tunnel l2tpv3 static tunnel name
```

Erläuterung: *`name`* ist die Bezeichnung des Tunnels.

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.4.4
Dynamische L2TPv3-Tunnel verwalten

Für den Datenverkehr mit dem Point-to-Point-(PPP)-Protokoll oder wenn das Peer-Gerät keine statischen L2TPv3-Tunnel unterstützt, können Sie wie bei L2TPv2 dynamische L2TPv3-Tunnel konfigurieren. Dynamische

L2TPv3-Tunnel können automatisch Verbindungen verhandeln und Verbindungen nach einem Netzwerkausfall wiederherstellen.

INHALT

- Abschnitt 11.4.4.1, „Dynamische L2TPv3-Tunnel aktivieren und konfigurieren“
- Abschnitt 11.4.4.2, „Eine Liste der dynamischen L2TPv3-Tunnel anzeigen“
- Abschnitt 11.4.4.3, „Hinzufügen eines dynamischen L2TPv3-Tunnels“
- Abschnitt 11.4.4.4, „Einen dynamischen L2TPv3-Tunnel löschen“

Abschnitt 11.4.4.1

Dynamische L2TPv3-Tunnel aktivieren und konfigurieren

Um dynamische L2TPv3-Tunnel zu aktivieren und zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Aktivieren Sie dynamische L2TPv3-Tunnel, indem Sie Folgendes eingeben:

```
tunnel l2tpv3 dynamic enabled
```

3. Konfigurieren Sie je nach Bedarf die folgenden Parameter:

Parameter	Beschreibung
mode { mode }	**Zusammenfassung:** { lac, lns } **Standard:** lns Die Betriebsart l2tp **HINWEIS** *System "lac" lässt das Aktivieren von /tunnel/l2tp/ nicht zu*
log-level { log-level }	**Zusammenfassung:** { none, error, warning, notice, info, all } **Standard:** none Maß der Logging-Nachricht
log-message { log-message }	**Zusammenfassung:** { none, protocol, fsm, api, transport, data, ppp, avp, func, system, all } **Standard:** none Kategorie der Logging-Nachricht **HINWEIS** *Zum Aktivieren der Logging-Nachricht muss das log-level "none" sein.*

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.4.4.2

Eine Liste der dynamischen L2TPv3-Tunnel anzeigen

Um eine Liste der dynamischen L2TPv3-Tunnel anzusehen, geben Sie Folgendes ein:

```
show running-config tunnel l2tpv3 dynamic tunnel
```

Falls Tunnel konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config tunnel l2tpv3 dynamic tunnel
tunnel
 l2tpv3 dynamic tunnel 1
  hostname       ruggedcom
  authentication none
  digest         md5
  interop        0
 !
!
```

Falls keine Tunnel konfiguriert wurden, fügen Sie je nach Bedarf Tunnel hinzu. Weitere Informationen finden Sie unter Abschnitt 11.4.4.3, „Hinzufügen eines dynamischen L2TPv3-Tunnels“.

Abschnitt 11.4.4.3

Hinzufügen eines dynamischen L2TPv3-Tunnels

Um einen dynamischen L2TPv3-Tunnel hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.

   HINWEIS
   Der Tunnelname muss aus einem bis drei numerischen und/oder alphanumerischen Kleinbuchstaben bestehen.

2. Fügen Sie den Tunnel hinzu, indem Sie Folgendes eingeben:

   ```
   tunnel l2tpv3 dynamic tunnel name
   ```

   Erläuterung: *name* ist die Bezeichnung des Tunnels.

3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

   HINWEIS
   Die transparente Kapselung ist nur dann konfigurierbar, wenn der dynamische L2TPv3-Tunnel sich im `lac` *Modus befindet.*

Parameter	Beschreibung
enabled	**Zusammenfassung:** { true, false } **Standard:** true Aktiviert/deaktiviert den Tunnel
remote-ip { remote-ip }	**Zusammenfassung:** Eine Zeichenkette mit 7 bis 15 Zeichen oder eine Zeichenkette mit 6 bis 40 Zeichen IP-Adresse des entfernten Tunnelendpunktes
hostname { hostname }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 63 Zeichen In AVP verwendeter Hostname Dieser Parameter ist obligatorisch.
local-ip { local-ip }	**Zusammenfassung:** Eine Zeichenkette mit 7 bis 15 Zeichen oder eine Zeichenkette mit 6 bis 40 Zeichen IP-Adresse der lokalen Schnittstelle, die als IP-Quelladresse des ausgehenden Verkehrs über Tunnel verwendet wird.

Parameter	Beschreibung
transport-encap { transport-encap }	**Zusammenfassung:** { udp, ip } **Standard:** udp Das Transportprotokoll (UDP oder IP) zum Einkapseln der Tunnel-Nachrichten
authentication { authentication }	**Zusammenfassung:** { none, challenge } **Standard:** none Die Authentifizierung des Tunnels **HINWEIS** *Tunnel-Authentifizierung erfordert Tunnel-Geheimnisse*
secret { secret }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 63 Zeichen Das Passwort der Tunnel-Verhandlung
digest { digest }	**Zusammenfassung:** { md5, sha1 } **Standard:** md5 AVP-Verschlüsselung von Message Digest
interop { interop }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 0 und 65535 **Standard:** 0 Eine Bitmaske von Flags festlegen, um nicht-standardisiertes Verhalten für die Interoperabilität mit einer anderen L2TPv3-Implementierung zu steuern.
persist-pend-timeout { persist-pend-timeout }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 10 und 6000 **Standard:** 60 Die Zeit (in Sekunden), die ein bestehender Tunnel im RETRY-Zustand wartet, bevor er sich erneut aufzubauen versucht.
hello { hello }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 5 und 1000 **Standard:** 60 Timeout für periodische L2TP-"Hello"-Nachrichten (in Sekunden)
hidden	**Zusammenfassung:** { true, false } **Standard:** false Aktiviert/Deaktiviert verborgenes AVP **HINWEIS** *Verborgenes AVP erfordert Tunnel-Authentifizierung und -Geheimnis*
receive-windows { receive-windows }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 5 und 512 **Standard:** 10 Empfangsfenstergröße
established-timeout { established-timeout }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 30 und 1000 **Standard:** 120 Die Zeit (in Sekunden), die ein Tunnel wartet, bis der Peer den Nachrichtenaustausch zum Tunnel-Aufbau beendet hat.
log	**Zusammenfassung:** { true, false } **Standard:** false Aktiviert/Deaktiviert die Protokollierung der Tunnel-Steuernachrichten **HINWEIS** *Zum Aktivieren von Tunnel-Steuernachrichten dürfen sowohl "log-level" als "log-message" nicht "none" sein.*

4. Fügen Sie eine oder mehrere Sitzungen zur Tunnelkonfiguration hinzu. Weitere Informationen finden Sie unter Abschnitt 11.4.5.2, „Hinzufügen einer Sitzung“.
5. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.4.4.4
Einen dynamischen L2TPv3-Tunnel löschen

Um einen dynamischen L2TPv3-Tunnel zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den Tunnel durch Eingabe von:

   ```
   no tunnel l2tpv3 dynamic tunnel name
   ```

   Erläuterung: *name* ist die Bezeichnung des Tunnels.
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.4.5
Sitzungen für L2TPv3-Tunnel verwalten

Dieser Abschnitt beschreibt, wie Sie Sitzungen für L2TPv3-Tunnel erstellen und verwalten können. Ein L2TPv3 kann bis zu 128 aktive Sitzungen unterstützen.

INHALT

- Abschnitt 11.4.5.1, „Eine Liste der Sitzungen anzeigen“
- Abschnitt 11.4.5.2, „Hinzufügen einer Sitzung“
- Abschnitt 11.4.5.3, „Eine Sitzung löschen“

Abschnitt 11.4.5.1
Eine Liste der Sitzungen anzeigen

Um eine Liste der Sitzungen, die für einen L2TPv3-Tunnel definiert sind, anzuzeigen, geben Sie Folgendes ein:

```
show running-config tunnel l2tpv3 [ static | dynamic ] tunnel tunnel-name session
```

Erläuterung: *tunnel-name* ist die Bezeichnung des Tunnels.

Falls Sitzungen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config tunnel l2tpv3 static tunnel 1 session
tunnel
 l2tpv3 static tunnel 1
  session 1
   local-session-id       10
   remote-session-id      20
   l2tp-specific-sublayer default
   vlan 4
   !
```

```
  !
  session 2
   local-session-id       30
   remote-session-id      40
   l2tp-specific-sublayer default
  !
 !
!
```

Falls keine Sitzungen konfiguriert wurden, fügen Sie je nach Bedarf Sitzungen hinzu. Weitere Informationen finden Sie unter Abschnitt 11.4.5.2, „Hinzufügen einer Sitzung“.

Abschnitt 11.4.5.2
Hinzufügen einer Sitzung

Um einem statischen oder dynamischen L2TPv3-Tunnel eine Sitzung hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie die Sitzung hinzu, indem Sie Folgendes eingeben:

   ```
   tunnel l2tpv3 [ static | dynamic ] tunnel tunnel-name session tunnel-session
   ```

   Erläuterung:

   - *`tunnel-name`* ist die Bezeichnung des Tunnels
   - *`tunnel-session`* ist die Bezeichnung der Tunnel-Sitzung
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

   HINWEIS
   Der `Log` Parameter gilt nur für Sitzungen des dynamischen L2TPv3-Tunnels.

Parameter	Beschreibung
enabled	**Zusammenfassung:** { true, false } **Standard:** true Aktiviert/deaktiviert die Sitzung
remote-end-id { remote-end-id }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 1 und 65535 ID des entfernten Endpunktes zur Identifizierung der Sitzung mit dem entfernten System Dieser Parameter ist obligatorisch.
l2tp-specific-sublayer { l2tp-specific-sublayer }	**Zusammenfassung:** { default, none } **Standard:** default L2TP-spezifischer Sublayer-Verarbeitungstyp
mtu { mtu }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 68 und 9216 **Standard:** 1460 MTU der Netzwerkschnittstelle
log	**Zusammenfassung:** { true, false } **Standard:** false Aktiviert/Deaktiviert die Protokollierung der Sitzungs-Steuernachrichten **HINWEIS** *Zum Aktivieren von Sitzungs-Steuernachrichten dürfen sowohl "log-level" als "log-message" nicht "none" sein*

WICHTIG!
Die Konfiguration des lokalen Cookies muss mit der Konfiguration des dezentralen Cookies auf dem Gerät am anderen Ende des L2TPv3-Tunnels übereinstimmen.

4. Geben Sie **`local-cookie`** ein und konfigurieren Sie anschließend je nach Bedarf die folgenden Parameter:

Parameter	Beschreibung
size { size }	**Zusammenfassung:** { 4, 8 } Cookie-Größe in Byte.
low-value { low-value }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Unterer Cookie-Wert. Dieser Wert muss mit dem "low-value" des anderen entfernten Cookie des Endpunkts übereinstimmen
high-value { high-value }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Oberer Cookie-Wert, wenn Cookie-Größe 8 ist. Dieser Wert muss mit dem "high-value" des anderen entfernten Cookie des Endpunkts übereinstimmen

WICHTIG!
Die Konfiguration des dezentralen Cookies muss mit der Konfiguration des lokalen Cookies auf dem Gerät am anderen Ende des L2TPv3-Tunnels übereinstimmen.

5. Geben Sie **`remote-cookie`** ein und konfigurieren Sie anschließend je nach Bedarf die folgenden Parameter:

Parameter	Beschreibung
size { size }	**Zusammenfassung:** { 4, 8 } Cookie-Größe in Byte
low-value { low-value }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Unterer Cookie-Wert. Dieser Wert muss mit dem "low-value" des anderen lokalen Cookie des Endpunkts übereinstimmen
high-value { high-value }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Oberer Cookie-Wert, wenn Cookie-Größe 8 ist. Dieser Wert muss mit dem "high-value" des anderen lokalen Cookie des Endpunkts übereinstimmen

6. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.4.5.3
Eine Sitzung löschen

Um eine Sitzung für einen statischen oder dynamischen L2TPv3-Tunnel zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den Tunnel, indem Sie Folgendes eingeben:

```
no tunnel l2tpv3 [ static | dynamic ] tunnel tunnel-name session tunnel-session
```

Erläuterung:

- *`tunnel-name`* ist die Bezeichnung des Tunnels
- *`tunnel-session`* ist die Bezeichnung der Tunnel-Sitzung

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.4.6
VLANs für L2TPv3-Tunnel verwalten

Dieser Abschnitt beschreibt, wie Sie VLANs für L2TPv3-Tunnelsitzungen verwalten können. Jede Sitzung unterstützt bis zu 128 VLAN-Mitglieder.

INHALT

- Abschnitt 11.4.6.1, „Eine Liste der VLANs anzeigen“
- Abschnitt 11.4.6.2, „Ein VLAN hinzufügen“
- Abschnitt 11.4.6.3, „Ein VLAN löschen“

Abschnitt 11.4.6.1
Eine Liste der VLANs anzeigen

Um eine Liste der VLANs, die für eine statische oder dynamische L2TPv3-Tunnel-Sitzung konfiguriert sind, anzuzeigen, geben Sie Folgendes ein:

```
show running-config tunnel l2tpv3 [ static | dynamic ] tunnel tunnel-name session tunnel-session vlan
```

Erläuterung:

- *`tunnel-name`* ist die Bezeichnung des Tunnels
- *`tunnel-session`* ist die Bezeichnung der Tunnel-Sitzung

Eine Tabelle oder Liste ähnlich dem folgenden Beispiel wird angezeigt:

```
ruggedcom# show running-config tunnel l2tpv3 static tunnel 1 session vlan
tunnel
 l2tpv3 static tunnel 1
  session 1
   vlan 4
   !
  !
 !
!
```

Falls keine VLANs konfiguriert wurden, fügen Sie je nach Bedarf VLANs hinzu. Weitere Informationen finden Sie unter Abschnitt 11.4.6.2, „Ein VLAN hinzufügen“.

Abschnitt 11.4.6.2
Ein VLAN hinzufügen

Um zu einer statischen oder dynamischen L2TPv3-Tunnel-Sitzung ein VLAN hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie die Sitzung hinzu, indem Sie Folgendes eingeben:

```
tunnel l2tpv3 [ static | dynamic ] tunnel tunnel-name session tunnel-session vlan vid
```

Erläuterung:

- *tunnel-name* ist die Bezeichnung des Tunnels.
- *tunnel-session* ist die Bezeichnung der Tunnel-Sitzung.
- *vid* ist die VLAN-ID für die routingfähige logische Schnittstelle. Der Wert muss zwischen 1 und 4094 liegen.

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.4.6.3
Ein VLAN löschen

Um ein VLAN für eine statische oder dynamische L2TPv3-Tunnel-Sitzung zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den Tunnel, indem Sie Folgendes eingeben:

```
no tunnel l2tpv3 [ static | dynamic ] tunnel tunnel-name session tunnel-session vlan vid
```

Erläuterung:

- *tunnel-name* ist die Bezeichnung des Tunnels
- *tunnel-session* ist die Bezeichnung der Tunnel-Sitzung
- *vid* ist die VLAN-ID für die routingfähige logische Schnittstelle

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.5
Verwalten von GOOSE-Tunneln

Mit der GOOSE-Tunnel-Funktion können GOOSE-Frames über ein Wide Area Network (WAN) überbrückt werden.

GOOSE-Tunnel bieten die folgenden Funktionen:

- Der GOOSE-Verkehr wird via UDP/IP über das WAN überbrückt.
- Eine GOOSE-Verkehrsquelle kann meshartig auf mehrere dezentrale Router-Ethernet-Schnittstellen abgebildet werden.
- Zur Verringerung des Bandbreitenverbrauchs können GOOSE-Daemons sich an jedem *Ende* und in der Mitte eines Sternnetzwerks befinden. Der zentrale Daemon akzeptiert GOOSE-Pakete und verteilt diese weiter.
- Statistiken informieren über die Verfügbarkeit von dezentralen GOOSE-Daemons, Paket-Zählwerten und die Round Trip Time (RTT) für jeden dezentralen Daemon.
- Bei Verwendung des Virtual Router Redundancy-Protokolls (VRRP) wird der GOOSE-Transport durch Senden redundanter GOOSE-Pakete von jedem VRRP-Gateway verbessert.
- Sie können die GOOSE-Weiterleitung durch Konfigurieren eines generischen Layer-2-Tunnels aktivieren. Im konfigurierten Zustand hören die Geräte nach GOOSE-Paketen an einem VLAN und leiten diese an ein anderes VLAN weiter.

Das GOOSE-Protokoll wird vom Layer-2-Tunnel-Daemon unterstützt. Der Daemon hört auf konfigurierte Ethernet-Schnittstellen und auf das Netzwerk selbst (d.h. nach Tunnelverbindungen von anderen Daemoninstanzen) an einem konfigurierten UDP-Port.

Die Media Access Control (MAC)-Zieladresse der vom Ethernet empfangenen Frames wird geprüft, um zu bestimmen, welcher Gruppe sie angehören. Die Frames werden anschließend in Netzwerk-Headern gekapselt und als GOOSE-Pakete an das Netzwerk weitergeleitet (mit intakter MAC-Quell- und Zieladresse).

Laut Empfehlungen von IEC 61850 sollte die MAC-Zieladresse im Bereich zwischen 01:0c:cd:01:00:00 und 01:0c:cd:01:01:ff liegen.

Aus dem Netzwerk empfangene GOOSE-Pakete werden von ihren Netzwerk-Headern getrennt und an die Ethernet-Ports weitergeleitet, die für dieselbe Multicast-Adresse konfiguriert sind. Die weitergeleiteten Frames enthalten die MAC-Quelladresse des ursprünglichen Geräts, jedoch nicht die der übertragenden Schnittstelle. Bei dem verwendeten VLAN handelt es sich um das VLAN, das lokal für die Schnittstelle programmiert ist und von dem ursprünglichen VLAN abweichen kann. Der Frame wird mit der höchsten 802.1p-Prioritätsstufe (p4) übertragen.

Aus dem Netzwerk empfangene Pakete werden ebenfalls an alle anderen dezentralen Daemons in der Gruppe weitergeleitet.

Zum Aktivieren der Weiterleitung von GOOSE-Paketen konfigurieren Sie einen generischen Layer-2-Tunnel, der nach GOOSE-Paketen an einem VLAN hört und diese an ein zweites VLAN weiterleitet. Um den generischen Layer-2-Tunnel für diesen Betrieb zu konfigurieren, nehmen Sie folgende Einstellungen für den Tunnel vor:

- Ethernet-Schnittstelle: wählen Sie das VLAN, von dem die GOOSE-Pakete stammen
- Ethernet-Typ: stellen Sie "0x88b8" ein
- Dezentraler Daemon: wählen Sie das VLAN, an das die GOOSE-Pakete weitergeleitet werden sollen

INHALT

- Abschnitt 11.5.1, „Statistik der GOOSE-Tunnel anzeigen“
- Abschnitt 11.5.2, „Eine Liste der GOOSE-Tunnel anzeigen“
- Abschnitt 11.5.3, „Einen GOOSE-Tunnel hinzufügen“
- Abschnitt 11.5.4, „Einen GOOSE-Tunnel löschen“
- Abschnitt 11.5.5, „Entfernte Daemons für GOOSE-Tunnel verwalten“

Abschnitt 11.5.1

Statistik der GOOSE-Tunnel anzeigen

Um die Statistik der GOOSE-Tunnel anzusehen, geben Sie Folgendes ein:

```
show tunnel l2tunneld status goose
```

Eine Tabelle oder Liste ähnlich dem folgenden Beispiel wird angezeigt:

```
ruggedcom# show tunnel l2tunneld status goose
l2tunneld status goose test
 ifname    switch.0100
 mac       01:0c:cd:01:00:33
 rx frames 2
 tx frames 0
 rx chars  114
 tx chars  0
 errors    0
 connections
```

```
             RX       TX       RX     TX
REMOTE IP    PACKETS  PACKETS  BYTES  BYTES  ERRORS
-------------------------------------------------
192.168.2.2  2        0        122    0      0
```

Diese Tabelle oder Liste liefert die folgenden Informationen:

Parameter	Beschreibung
tunnel-name	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 32 Zeichen Der Name des GOOSE-Tunnels Dieser Parameter ist obligatorisch.
ifname	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 15 Zeichen Der Name der VLAN-Schnittstelle. Dieser Parameter ist obligatorisch.
mac	**Zusammenfassung:** Eine Zeichenkette mit 17 Zeichen Die Multicast-MAC-Zieladresse der GOOSE-Nachricht. Dieser Parameter ist obligatorisch.
rx-frames	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl der durch den Tunnel empfangenen Frames. Dieser Parameter ist obligatorisch.
tx-frames	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl der durch den Tunnel übertragenen Frames. Dieser Parameter ist obligatorisch.
rx-chars	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl durch den Tunnel empfangener Bytes. Dieser Parameter ist obligatorisch.
tx-chars	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl der durch den Tunnel übertragenen Bytes. Dieser Parameter ist obligatorisch.
errors	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl der Fehler durch den Tunnel. Dieser Parameter ist obligatorisch.

Abschnitt 11.5.2
Eine Liste der GOOSE-Tunnel anzeigen

Um eine Liste der GOOSE-Tunnel anzusehen, geben Sie Folgendes ein:

```
show running-config tunnel l2tunneld goose
```

Falls Tunnel konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config tunnel l2tunneld goose tunnel | tab
                                      IP
NAME  INTERFACE    MULTICAST MAC      ADDRESS
-----------------------------------------------
1     switch.0001  01:0c:cd:01:01:01

!
```

Falls keine GOOSE-Tunnel konfiguriert wurden, fügen Sie je nach Bedarf Tunnel hinzu. Weitere Informationen finden Sie unter Abschnitt 11.5.3, „Einen GOOSE-Tunnel hinzufügen“.

Abschnitt 11.5.3
Einen GOOSE-Tunnel hinzufügen

Um einen GOOSE-Tunnel zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den Tunnel hinzu, indem Sie Folgendes eingeben:

   ```
   tunnel l2tunneld goose tunnel name
   ```

   Erläuterung:

   - *name* ist die Bezeichnung des GOOSE-Tunnels
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
interface { interface }	**Zusammenfassung:** Eine Zeichenkette Die Schnittstelle zum Empfang für GOOSE-Frames.
multicast-mac { multicast-mac }	**Zusammenfassung:** Eine Zeichenkette mit 17 Zeichen Die Multicast-MAC-Adresse zum Empfangen. Dieser Parameter ist obligatorisch.

4. Falls erforderlich konfigurieren Sie einen oder mehrere entfernte Daemon für den Tunnel. Weitere Informationen finden Sie unter Abschnitt 11.5.5.2, „Einen entfernten Daemon hinzufügen“.
5. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.5.4
Einen GOOSE-Tunnel löschen

Um einen GOOSE-Tunnel zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den GOOSE-Tunnel durch Eingabe von:

   ```
   no tunnel l2tunneld goose tunnel name
   ```

   Erläuterung:

   - *name* ist die Bezeichnung des GOOSE-Tunnels
3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.5.5

Entfernte Daemons für GOOSE-Tunnel verwalten

An Stelle einer lokalen Ethernet-Schnittstelle für den Tunnel-Ausgang können IP-Adressen für einen entfernten Daemon konfiguriert werden. Es können mehrere Endpunkte mit diesen Feldern hinzugefügt werden, indem die Tunnelkonfiguration mehrfach bearbeitet wird.

INHALT

- Abschnitt 11.5.5.1, „Eine Liste der entfernten Daemons anzeigen“
- Abschnitt 11.5.5.2, „Einen entfernten Daemon hinzufügen“
- Abschnitt 11.5.5.3, „Einen entfernten Daemon löschen“

Abschnitt 11.5.5.1

Eine Liste der entfernten Daemons anzeigen

Um eine Liste der entfernten Daemons, die für einen GOOSE-Tunnel konfiguriert sind, anzuzeigen, geben Sie Folgendes ein:

```
show running-config tunnel l2tunneld goose tunnel name remote-daemon
```

Erläuterung:

- *name* ist die Bezeichnung des GOOSE-Tunnels

Falls Tunnel konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config tunnel l2tunneld goose tunnel 1 remote-daemon
tunnel
 l2tunneld goose tunnel 1
  remote-daemon 192.168.10.2
  !
 !
!
```

Falls keine entfernten Daemons konfiguriert wurden, fügen Sie je nach Bedarf Daemons hinzu. Weitere Informationen finden Sie unter Abschnitt 11.5.5.2, „Einen entfernten Daemon hinzufügen“.

Abschnitt 11.5.5.2

Einen entfernten Daemon hinzufügen

Um einen entfernten Daemon für einen GOOSE-Tunnel zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den entfernten Daemon hinzu, indem Sie Folgendes eingeben:

   ```
   tunnel l2tunneld goose tunnel remote-daemon address
   ```

   Erläuterung:

   - *address* ist die IP-Adresse des entfernten Daemon
3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.5.5.3
Einen entfernten Daemon löschen

Um einen entfernten Daemon zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den entfernten Daemon, indem Sie Folgendes eingeben:

   ```
   no tunnel l2tunneld goose tunnel name remote-daemon address
   ```

   Erläuterung:

   - *name* ist die Bezeichnung des GOOSE-Tunnels
   - *address* ist die IP-Adresse des entfernten Daemon
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.6
Generische Tunnel verwalten

Der Layer-2-Tunnel-Daemon unterstützt eine generische Betriebsart, die auf dem Ethernet-Typ des Layer-2-Datenverkehrs beruht, die der Router erkennt. Es können mehrere Tunnel konfiguriert werden, jeder mit:

- einem Ethernet-Typ
- einem Tunnel-Ingress (Ethernet-Schnittstelle)
- einem Tunnel-Egress (entweder eine andere lokal angebundene Ethernet-Schnittstelle oder die entfernte IP-Adresse einer anderen Instanz des Layer-2-Tunnel-Daemons, die auf einem anderen Router läuft)

INHALT

- Abschnitt 11.6.1, „Statistik generischer Tunnel anzeigen“
- Abschnitt 11.6.2, „Eine Liste generischer Tunnel anzeigen“
- Abschnitt 11.6.3, „Hinzufügen eines generischen Tunnels“
- Abschnitt 11.6.4, „Einen generischen Tunnel löschen“
- Abschnitt 11.6.5, „IP-Adressen entfernter Daemons für generische Tunnel verwalten“
- Abschnitt 11.6.6, „Ausgehende (egress) Schnittstellen entfernter Daemons für generische Tunnel verwalten“
- Abschnitt 11.6.7, „Ethernet-Typen für generische Tunnel verwalten“

Abschnitt 11.6.1
Statistik generischer Tunnel anzeigen

Um die Statistik der generischen Tunnel anzusehen, geben Sie Folgendes ein:

```
show tunnel l2tunneld status generic
```

Eine Tabelle oder Liste ähnlich dem folgenden Beispiel wird angezeigt:

```
ruggedcom# show tunnel l2tunneld status generic
```

```
TUNNEL               RX      TX      RX     TX                          RX       TX       RX     TX
NAME    IFNAME       FRAMES  FRAMES  CHARS  CHARS  ERRORS  REMOTE IP    PACKETS  PACKETS  BYTES  BYTES
 ERRORS
-------------------------------------------------------------------------------------------------
iso     switch.0002  5       6       300    360    0
                                                   192.168.5.1  11       0        704    0
 0
```

Diese Tabelle oder Liste liefert die folgenden Informationen:

Parameter	Beschreibung
tunnel-name	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 32 Zeichen Der Name des generischen Tunnels. Dieser Parameter ist obligatorisch.
ifname	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 15 Zeichen Der Name der eingehenden Schnittstelle. Dieser Parameter ist obligatorisch.
rx-frames	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl der durch den Tunnel empfangenen Frames. Dieser Parameter ist obligatorisch.
tx-frames	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl der durch den Tunnel übertragenen Frames. Dieser Parameter ist obligatorisch.
rx-chars	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl durch den Tunnel empfangener Bytes. Dieser Parameter ist obligatorisch.
tx-chars	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl der durch den Tunnel übertragenen Bytes. Dieser Parameter ist obligatorisch.
errors	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl der durch den Tunnel empfangenen Fehler. Dieser Parameter ist obligatorisch.

Abschnitt 11.6.2

Eine Liste generischer Tunnel anzeigen

Um eine Liste der generischen Tunnel anzusehen, geben Sie Folgendes ein:

```
show running-config tunnel l2tunneld generic tunnel
```

Falls Tunnel konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config tunnel l2tunneld generic tunnel | tab
                  REPLACE        EGRESS  IP
NAME  INGRESS IF  MAC      TYPE  IF      ADDRESS
-------------------------------------------------
1     switch.0001 -
                         iso

!
```

Falls keine Tunnel konfiguriert wurden, fügen Sie je nach Bedarf Tunnel hinzu. Weitere Informationen finden Sie unter Abschnitt 11.6.3, „Hinzufügen eines generischen Tunnels“.

Abschnitt 11.6.3
Hinzufügen eines generischen Tunnels

Um einen generischen Tunnel zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den Tunnel hinzu, indem Sie Folgendes eingeben:

   ```
   tunnel l2tunneld generic tunnel name
   ```

   Erläuterung:

   - *name* ist die Bezeichnung des generischen Tunnels
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
ingress-if { ingress-if }	**Zusammenfassung:** Eine Zeichenkette Die Schnittstelle zum Empfang für Ethernet-Typ-Frames.
replace-mac	Ersetzt die MAC des Senders durch die MAC der Out-Schnittstelle.

4. Bei Bedarf konfigurieren Sie die IP-Adressen eines oder mehrerer entfernter Daemons für den Tunnel. Weitere Informationen finden Sie unter Abschnitt 11.6.5.2, „Eine IP-Adresse hinzufügen“.
5. Bei Bedarf definieren Sie einen oder mehrere weiterzuleitende Ethernet-Typen. Weitere Informationen finden Sie unter Abschnitt 11.6.7.2, „Einen Ethernet-Typ hinzufügen“.
6. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.6.4
Einen generischen Tunnel löschen

Um einen generischen Tunnel zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den generischen Tunnel durch Eingabe von:

   ```
   no tunnel l2tunneld generic tunnel name
   ```

   Erläuterung:

   - *name* ist die Bezeichnung des generischen Tunnels
3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.6.5

IP-Adressen entfernter Daemons für generische Tunnel verwalten

An Stelle einer lokalen Ethernet-Schnittstelle für den Tunnel-Ausgang können IP-Adressen für einen entfernten Daemon konfiguriert werden. Es können mehrere Endpunkte mit diesen Feldern hinzugefügt werden, indem die Tunnelkonfiguration mehrfach bearbeitet wird.

HINWEIS
Wenn eine IP-Adresse eines entfernten Daemons konfiguriert wird, sollte die Schnittstelle auf der Empfängerseite, von der der Verkehr abgeht, an der Eingangsschnittstelle (statt der Ausgangsschnittstelle) konfiguriert werden.

INHALT

- Abschnitt 11.6.5.1, „Eine Liste der IP-Adressen anzeigen“
- Abschnitt 11.6.5.2, „Eine IP-Adresse hinzufügen“
- Abschnitt 11.6.5.3, „Eine IP-Adresse löschen“

Abschnitt 11.6.5.1

Eine Liste der IP-Adressen anzeigen

Um eine Liste der IP-Adressen des entfernten Layer-2-Protokollservers für eine generische Tunnelkonfiguration anzuzeigen, geben Sie Folgendes ein:

```
show running-config tunnel l2tunneld generic tunnel remote-daemon
```

Falls Tunnel konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config tunnel l2tunneld generic tunnel remote-daemon ip-address | tab
NAME  IP ADDRESS
--------------------
1
      172.112.10.1

!
```

Falls keine Tunnel konfiguriert wurden, fügen Sie je nach Bedarf Tunnel hinzu. Weitere Informationen finden Sie unter Abschnitt 11.6.3, „Hinzufügen eines generischen Tunnels“.

Abschnitt 11.6.5.2

Eine IP-Adresse hinzufügen

Um die IP-Adresse eines dezentralen Layer-2-Protokollservers zu einer generischen Tunnelkonfiguration hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie die IP-Adresse hinzu, indem Sie Folgendes eingeben:

   ```
   tunnel l2tunneld generic tunnel name remote-daemon ip-address address
   ```

   Erläuterung:

- *name* ist die Bezeichnung des generischen Tunnels
- *address* ist die IP-Adresse des dezentralen Layer 2-Protokollservers

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.6.5.3
Eine IP-Adresse löschen

Um die IP-Adresse eines dezentralen Layer-2-Protokollservers aus einer generischen Tunnelkonfiguration zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die IP-Adresse, indem Sie Folgendes eingeben:

```
no tunnel l2tunneld generic tunnel name remote-daemon ip-address address
```

Erläuterung:

- *name* ist die Bezeichnung des generischen Tunnels
- *address* ist die IP-Adresse des dezentralen Layer 2-Protokollservers

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.6.6
Ausgehende (egress) Schnittstellen entfernter Daemons für generische Tunnel verwalten

Dieser Abschnitt beschreibt, wie Sie an entfernten Daemons für generische Tunnel ausgehende (egress) Schnittstellen erstellen und verwalten können

INHALT

- Abschnitt 11.6.6.1, „Eine Liste der ausgehenden (egress) Schnittstellen anzeigen“
- Abschnitt 11.6.6.2, „Eine ausgehende (egress) Schnittstelle hinzufügen“
- Abschnitt 11.6.6.3, „Eine ausgehende (egress) Schnittstelle löschen“

Abschnitt 11.6.6.1
Eine Liste der ausgehenden (egress) Schnittstellen anzeigen

Um eine Liste aller für einen generischen Tunnel konfigurierten ausgehenden Schnittstellen anzusehen, geben Sie Folgendes ein:

```
show running-config tunnel l2tunneld generic tunnel remote-daemon egress-if
```

Falls Schnittstellen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config tunnel l2tunneld generic tunnel remote-daemon egress-if | tab
NAME  EGRESS IF
```

```
-------------------
1
      switch.0001

!
```

Falls keine Schnittstellen konfiguriert wurden, fügen Sie je nach Bedarf Schnittstellen hinzu. Weitere Informationen finden Sie unter Abschnitt 11.6.6.2, „Eine ausgehende (egress) Schnittstelle hinzufügen“.

Abschnitt 11.6.6.2

Eine ausgehende (egress) Schnittstelle hinzufügen

Um eine ausgehende (egress) Schnittstelle für einen generischen Tunnel hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie die ausgehende (egress) Schnittstelle hinzu, indem Sie Folgendes eingeben:

   ```
   tunnel l2tunneld generic tunnel name remote-daemon egress-if interface
   ```

   Erläuterung:

   - *name* ist die Bezeichnung des generischen Tunnels
   - *interface* ist die ausgehende (egress) Schnittstelle für Ethernet-Frames
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.6.6.3

Eine ausgehende (egress) Schnittstelle löschen

Um eine ausgehende (egress) Schnittstelle für einen generischen Tunnel zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die ausgehende (egress) Schnittstelle, indem Sie Folgendes eingeben:

   ```
   no tunnel l2tunneld generic tunnel name remote-daemon egress-if interface
   ```

   Erläuterung:

   - *name* ist die Bezeichnung des generischen Tunnels
   - *interface* ist die ausgehende (egress) Schnittstelle für Ethernet-Frames
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.6.7

Ethernet-Typen für generische Tunnel verwalten

Dieser Abschnitt beschreibt, wie Sie die Ethernet Protokolltypen festlegen, die durch generische Tunnel weitergeleitet werden.

INHALT

- Abschnitt 11.6.7.1, „Eine Liste der Ethernet-Typen anzeigen“
- Abschnitt 11.6.7.2, „Einen Ethernet-Typ hinzufügen“
- Abschnitt 11.6.7.3, „Einen Ethernet-Typ löschen“

Abschnitt 11.6.7.1

Eine Liste der Ethernet-Typen anzeigen

Um eine Liste der für einen generischen Tunnel konfigurierten Ethernet-Typen anzusehen, geben Sie Folgendes ein:

```
show running-config tunnel l2tunneld generic tunnel ethernet-type
```

Falls Ethernet-Typen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config tunnel l2tunneld generic tunnel ethernet-type | tab
NAME  TYPE
------------
1
      iso

!
```

Falls keine Ethernet-Typen konfiguriert wurden, fügen Sie je nach Bedarf Typen hinzu. Weitere Informationen finden Sie unter Abschnitt 11.6.7.2, „Einen Ethernet-Typ hinzufügen“.

Abschnitt 11.6.7.2

Einen Ethernet-Typ hinzufügen

Um einen Ethernet-Typ für einen generischen Tunnel hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Um den Ethernet-Typ hinzuzufügen, geben Sie Folgendes ein:

   ```
   tunnel l2tunneld generic tunnel name ethernet-type type
   ```

   Erläuterung:

   - *name* ist die Bezeichnung des generischen Tunnels
   - *type* ist der weiterzuleitende Ethernet-Typ (d. h. 0xFEFE)
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.6.7.3

Einen Ethernet-Typ löschen

Um einen Ethernet-Typ für einen generischen Tunnel zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Um den Ethernet-Typ zu löschen, geben Sie Folgendes ein:

   ```
   no tunnel l2tunneld generic tunnel name ethernet-type type
   ```

   Erläuterung:

   - *name* ist die Bezeichnung des generischen Tunnels
   - *type* ist der Ethernet-Typ (d. h. 0xFEFE)
3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.7

GRE (Generic Routing Encapsulation)-Tunnel verwalten

RUGGEDCOM ROX II kann mithilfe des GRE (Generic Routing Encapsulation)-Protokolls Multicast-Verkehrs- und IPv6-Pakete zusammenkapseln und über einen IPv4-Netzwerktunnel transportieren. GRE-Tunnel können somit den Verkehr durch beliebig viele Zwischennetze transportieren.

Die wichtigsten Parameter für GRE-Tunnel sind der Tunnelname, die Adresse des lokalen und des entfernten Routers sowie das entfernte Subnetz.

Im Folgenden ist eine typische GRE-Tunnelkonfiguration dargestellt:



Abbildung 22: Beispiel – GRE-Tunnelkonfiguration

In diesem Beispiel erstellt Router 1 einen GRE-Tunnel zu Router 2 mit einer Adresse des lokalen Routers von 172.16.17.18, einer Adresse des entfernten Routers von 172.19.20.21 und einem entfernten Subnetz von 192.168.2.0/24.

HINWEIS
*Beim Anschließen eines Cisco-Routers (anstelle von Router 1 im vorherigen Beispiel) entspricht die Adresse des lokalen Routers der Cisco IOS **Quell**adresse und die Adresse des entfernten Routers der **Ziel**adresse.*

Die Kalkulation des GRE-Tunnels kann auch dann festgelegt werden, wenn eine andere Routing-Methode zwischen Router 1 und Router 2 zur Verfügung steht. Die Pakete werden automatisch durch die Route mit den geringsten Kosten geleitet.

Pakete können auch durch die Angabe eines lokalen ausgehenden Geräts, wie z. B. w1pp bei Router 1 im vorherigen Beispiel, eingeschränkt werden.

INHALT

- Abschnitt 11.7.1, „Statistiken für GRE-Tunnel anzeigen“
- Abschnitt 11.7.2, „Eine Liste der GRE-Tunnel anzeigen“
- Abschnitt 11.7.3, „Hinzufügen eines GRE-Tunnels“
- Abschnitt 11.7.4, „Konfigurieren einer DSCP-Kennzeichnung für den GRE-Tunnelverkehr“
- Abschnitt 11.7.5, „Einen GRE-Tunnel löschen“

Abschnitt 11.7.1

Statistiken für GRE-Tunnel anzeigen

Um die Statistiken für GRE-Tunnel anzusehen, geben Sie Folgendes ein:

```
show interfaces gre
```

Eine Tabelle oder Liste ähnlich dem folgenden Beispiel wird angezeigt:

```
ruggedcom# show interfaces gre
        TUNNEL  RX       RX      RX     TX       TX      TX
IFNAME  STATUS  PACKETS  ERRORS  DROPS  PACKETS  ERRORS  DROPS
-----------------------------------------------------------------
g1      Active  52       0       0      855      51      0
g2      Active  0        0       0      0        791     0
```

Diese Tabelle oder Liste liefert die folgenden Informationen:

Parameter	Beschreibung
ifname	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 10 Zeichen Der Schnittstellen-Name des GRE-Tunnels.
tunnel-status	**Zusammenfassung:** Eine Zeichenkette Der Status des Tunnels. Dieser Parameter ist obligatorisch.
rx-packets	**Zusammenfassung:** Eine vorzeichenlose 64-Bit-Ganzzahl Die Anzahl der durch den Tunnel empfangenen Pakete. Dieser Parameter ist obligatorisch.
rx-errors	**Zusammenfassung:** Eine vorzeichenlose 64-Bit-Ganzzahl Die durch den Tunnel empfangenen Fehler-Pakete. Dieser Parameter ist obligatorisch.
rx-drops	**Zusammenfassung:** Eine vorzeichenlose 64-Bit-Ganzzahl Die Anzahl der Pakete, die vom Tunnel verworfen wurden. Dieser Parameter ist obligatorisch.
tx-packets	**Zusammenfassung:** Eine vorzeichenlose 64-Bit-Ganzzahl

Parameter	Beschreibung
	Die Anzahl der durch den Tunnel übertragenen Pakete. Dieser Parameter ist obligatorisch.
tx-errors	**Zusammenfassung:** Eine vorzeichenlose 64-Bit-Ganzzahl Die Anzahl der durch den Tunnel übertragenen Fehler-Pakete. Dieser Parameter ist obligatorisch.
tx-drops	**Zusammenfassung:** Eine vorzeichenlose 64-Bit-Ganzzahl Die Anzahl der Pakete, die vom Tunnel verworfen wurden. Dieser Parameter ist obligatorisch.

Abschnitt 11.7.2
Eine Liste der GRE-Tunnel anzeigen

Um eine Liste der GRE-Tunnel anzusehen, geben Sie Folgendes ein:

```
show running-config tunnel gre
```

Falls GRE-Tunnel konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config tunnel gre | tab
IF
NAME  LOCAL IP      REMOTE IP     REMOTE NET      MTU   MULTICAST  COST
-------------------------------------------------------------------------
gre   172.16.17.18  172.19.20.21  192.168.2.0/24  1476  -          0
```

Falls keine GRE-Tunnel konfiguriert wurden, fügen Sie je nach Bedarf Tunnel hinzu. Weitere Informationen finden Sie unter Abschnitt 11.7.3, „Hinzufügen eines GRE-Tunnels“.

Abschnitt 11.7.3
Hinzufügen eines GRE-Tunnels

Um einen GRE-Tunnel hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den GRE-Tunnel hinzu, indem Sie Folgendes eingeben:

   ```
   tunnel gre name
   ```

   Erläuterung:

   - *name* ist die Bezeichnung der Schnittstelle des GRE-Tunnelnetzwerks. Die Bezeichnung der Schnittstelle muss mit einem Kleinbuchstaben beginnen und kann eine beliebige Kombination aus Kleinbuchstaben, Ziffern und Gedankenstrichen bis maximal zehn Zeichen enthalten. Das Präfix *gre-* wird zur Bezeichnung dieser Schnittstelle hinzugefügt.
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
local-ip { local-ip }	**Zusammenfassung:** Eine Zeichenkette mit 7 bis 15 Zeichen oder eine Zeichenkette mit 6 bis 40 Zeichen Die IP-Adresse des lokalen Tunnelendes.

Parameter	Beschreibung
	Dieser Parameter ist obligatorisch.
remote-ip { remote-ip }	**Zusammenfassung:** Eine Zeichenkette mit 7 bis 15 Zeichen oder eine Zeichenkette mit 6 bis 40 Zeichen Die IP-Adresse des entfernten Tunnelendes. Dieser Parameter ist obligatorisch.
remote-net { remote-net }	**Zusammenfassung:** Eine Zeichenkette mit 9 bis 18 Zeichen oder eine Zeichenkette mit 4 bis 43 Zeichen Das Zielnetzwerk des entfernten Tunnelendes.
mtu { mtu }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl **Standard:** 1476 Die MTU der GRE-Schnittstelle
multicast	Aktiviert Multicast-Verkehr an der Tunnel-Schnittstelle.
cost { cost }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 1 und 255 **Standard:** 1 Die Routing-Kosten für das Netzrouting, das Verkehr durch den Tunnel leitet.
key { key }	**Zusammenfassung:** { none, input, output, both } **Standard:** none Der Schlüssel für getunnelte Pakete
key-id { key-id }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 0 und 4294967295 **Standard:** 0 Die Schlüssel-ID für getunnelte Pakete
checksum { checksum }	**Zusammenfassung:** { none, input, output, both } **Standard:** none Die Prüfsumme für getunnelte Pakete
sequence { sequence }	**Zusammenfassung:** { none, input, output, both } **Standard:** none Die Sequenznummer für getunnelte Pakete

4. [Optional] Konfigurieren Sie das Verfahren zum Zuweisen von Differentiated Services Code Point (DSCP)-Kennzeichnungen zu Paketen, die durch den GRE-Tunnel geleitet werden. Weitere Informationen finden Sie unter Abschnitt 11.7.4, „Konfigurieren einer DSCP-Kennzeichnung für den GRE-Tunnelverkehr“.

   HINWEIS
   *Eine Schnittstelle in der Form **gre-{tunnel}** (z. B. gre-t1) wird automatisch zum **ip** Menü hinzugefügt.*

5. Weisen Sie dem Tunnel eine IP-Adresse zu. Für weitere Informationen siehe Abschnitt 7.1.3.2, „Eine IPv4-Adresse hinzufügen“ oder Abschnitt 7.1.4.2, „Eine IPv6-Adresse hinzufügen“.
6. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.7.4

Konfigurieren einer DSCP-Kennzeichnung für den GRE-Tunnelverkehr

Jedem Paket, das durch einen GRE-Tunnel geleitet wird, kann eine Differentiated Services Code Point (DSCP)-Kennzeichnung zugewiesen werden, die entweder vom Gerät definiert wird oder die der ursprüngliche IP-Header besitzt.

Um zu konfigurieren, wie DSCP-Kennzeichnungen für einen bestimmten GRE-Tunnel zugewiesen werden, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***tunnel » gre » {tunnel} » mark-choice***, wobei *{tunnel}*die Bezeichnung des GRE-Tunnels ist.
3. Konfigurieren Sie die DSCP-Kennzeichnung, indem Sie Folgendes eingeben:

   ```
   tunnel gre name mark-choice dscpmarking dscp-type [ mark | forward ]
   ```

   Erläuterung: *name* ist die Bezeichnung des GRE-Tunnels.

   Optionen sind u.a.:

   - `mark` – Weist die durch **DSCP Mark** gesetzte DSCP-Kennzeichnung Paketen zu, die durch den Tunnel geleitet werden
   - `forward` – Weist die DSCP-Kennzeichnung zu, die im ursprünglichen IP-Header aller durch den Tunnel geleiteten Pakete definiert sind
4. Wenn `mark` gewählt wird, wählen Sie eine zuzuweisende DSCP-Kennzeichnung, indem Sie Folgendes eingeben:

   ```
   dscp-mark [ AF11 | AF12 | AF13 | AF21 | AF22 | AF23 | AF31 | AF32 | AF33 | AF41 | AF42 | AF43 | BE
   | CS1 | CS2 | CS3 | CS4 | CS5 | CS6 | CS7 | EF ]
   ```
5. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.7.5

Einen GRE-Tunnel löschen

Um einen GRE-Tunnel zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den GRE-Tunnel durch Eingabe von:

   ```
   no tunnel gre name
   ```

   Erläuterung:

   - *name* ist die Bezeichnung des GRE-Tunnels
3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.8

IPsec-Tunnel verwalten

IPsec (Internet Protocol SECurity) nutzt starke Kryptografietechniken, um Authentifizierungs- und Verschlüsselungsdienste bereitzustellen. Die Authentifizierung stellt sicher, dass die Pakete vom richtigen Absender stammen und während des Transports nicht verändert wurden. Die Verschlüsselung verhindert das unbefugte Lesen von Paketinhalten.

Diese Dienste ermöglichen, dass in nicht vertrauenswürdigen Netzen sichere Tunnel erstellt werden. Alles, was durch das nicht vertrauenswürdiges Netzwerk geleitet wird, wird vom IPsec-Gateway verschlüsselt und am anderen Ende vom Gateway entschlüsselt. Das Ergebnis ist ein Virtual Private Network (VPN), ein praktisch privates Netzwerk, obwohl es mehrere Rechner an mehreren verschiedenen Orten umfasst, die über das unsichere Internet verbunden sind.

Weitere Informationen über IPsec-Tunnel finden Sie unter Abschnitt 11.8.1, „IPsec-Tunneling-Konzepte“.

WICHTIG!
IPsec ist zeitkritisch. Um sicherzustellen, dass die Zeit zwischen den Netzwerk-Peers korrekt eingegeben wird, muss die Zeit auf beiden Peers synchronisiert werden. Es wird dringend empfohlen, auf beiden IPsec-Peers NTP (Network Time Protocol) zu verwenden, um ihre Uhren zu synchronisieren. Für weitere Informationen über das Konfigurieren des NTP siehe Abschnitt 16.8, „NTP-Server verwalten“.

INHALT

- Abschnitt 11.8.1, „IPsec-Tunneling-Konzepte“
- Abschnitt 11.8.2, „Konfigurieren von IPsec-Tunneln“
- Abschnitt 11.8.3, „Konfigurieren von Zertifikaten und Schlüsseln“
- Abschnitt 11.8.4, „Anzeigen des Status des IPSec-Tunnels“
- Abschnitt 11.8.5, „Vorher vereinbarte (pre-shared) Schlüssel verwalten“
- Abschnitt 11.8.6, „Verbindungen verwalten“
- Abschnitt 11.8.7, „Das IKE-(Internet Key Exchange)-Protokoll verwalten“
- Abschnitt 11.8.8, „Ein ESP-Protokoll (Encapsulated Security Payload) verwalten“
- Abschnitt 11.8.9, „Konfigurieren der Verbindungsenden“
- Abschnitt 11.8.10, „Private Subnetze verwalten“

Abschnitt 11.8.1

IPsec-Tunneling-Konzepte

Die IPsec-Protokolle wurden von der Internet Engineering Task Force (IETF) entwickelt und sind als Teil der IP Version 6 erforderlich. Libreswan ist die Open-Source-Implementierung von IPsec, die von RUGGEDCOM ROX II verwendet wird.

IPsec verwendet die Protokolle ESP (Encapsulating Security Payload) und IKE (Internet Key Exchange). ESP bietet Verschlüsselung und Authentifizierung (als Sicherheit, dass eine Meldung vom erwarteten Absender stammt und während der Übertragung nicht verändert wurde). IKE verhandelt Verbindungsparameter, einschließlich

Schlüssel, für ESP. IKE basiert auf dem Diffie-Hellman-Protokoll für Schlüsselaustausch, mit dem zwei Partner einen gemeinsamen geheimen Schlüssel vereinbaren können, den ein potenzieller Lauscher nicht berechnen kann.

INHALT

- Abschnitt 11.8.1.1, „IPsec-Betriebsarten“
- Abschnitt 11.8.1.2, „Unterstützte Verschlüsselungsprotokolle“
- Abschnitt 11.8.1.3, „Kryptografie von öffentlichen und geheimen Schlüsseln“
- Abschnitt 11.8.1.4, „X.509-Zertifikate“
- Abschnitt 11.8.1.5, „NAT Traversal“
- Abschnitt 11.8.1.6, „Unterstützung eines entfernten IPsec-Clients“
- Abschnitt 11.8.1.7, „IPsec- und Router-Schnittstellen“

Abschnitt 11.8.1.1

IPsec-Betriebsarten

IPsec hat zwei grundsätzliche Betriebsarten. In der Betriebsart *transport* werden beim Erstellen des ursprünglichen IP-Datagramm IPsec-Header eingefügt. Das resultierende Paket besteht aus einem IP-Header, IPsec-Headern und der IP-Payload (einschließlich eines Transport-Headers). Diese Betriebsart wird meistens zwischen IPsec-Endstationen oder zwischen einer Endstation und einem Gateway verwendet.

In der Betriebsart *tunnel* wird das ursprüngliche IP-Datagramm normal erstellt und dann in ein neues IP-Datagramm gekapselt. Das resultierende Paket besteht aus einem neuen IP-Header, IPsec-Headern, dem alten IP-Header und der IP-Payload. Diese Betriebsart wird meist zwischen Gateways verwendet, wobei das Gateway als Proxy für die Hosts hinter ihm fungiert.

Abschnitt 11.8.1.2

Unterstützte Verschlüsselungsprotokolle

Libreswan unterstützt die folgenden Standard-Verschlüsselungsprotokolle:

- **3DES (Triple DES)**

  Wendet drei DES-(Data Encryption Standard)-Verschlüsselungen in einem einzelnen Datenblock mit mindestens zwei verschiedenen Schlüsseln an, um eine höhere Sicherheit als mit einem einzelnen DES-Durchgang zu erzielen. 3DES ist die CPU-intensivste Verschlüsselung.

- **AES**

  Das AES-(Advanced Encryption Standard)-Protokoll verwendet einen 128-Bit-Block und 128-, 192- oder 256-Bit-Schlüssel. Dies ist heute das sicherste Protokoll und wird auf Grund seiner Effizienz gegenüber 3DES bevorzugt.

Abschnitt 11.8.1.3

Kryptografie von öffentlichen und geheimen Schlüsseln

In der Kryptografie mit *öffentlichem Schlüssel* werden Schlüssel paarweise (bestehend aus öffentlichem und privatem Schlüssel) erstellt. Der öffentliche Schlüssel wird öffentlich zugänglich gemacht, während der private Schlüssel geheim gehalten wird. Nachrichten können dann von jedem versendet werden, der den öffentlichen

Schlüssel des Besitzers des privaten Schlüssels kennt. Nur der Besitzer des privaten Schlüssels kann die Nachricht entschlüsseln.

Wenn diese Verschlüsselungsart verwendet wird, konfiguriert jeder Router seine VPN-Verbindung so, dass er den RSA-Algorithmus anwendet und die öffentliche Signatur seines Peers einbindet.

In der Kryptografie mit *geheimem Schlüssel* wird ein einziger Schlüssel, der beiden Parteien bekannt ist, sowohl für die Verschlüsselung als auch für die Entschlüsselung verwendet.

Bei dieser Verschlüsselungsart konfiguriert jeder Router seine VPN-Verbindung so, dass er einen geheimen, vorher vereinbarten Schlüssel verwendet. Informationen zum Konfigurieren von vorher vereinbarten Schlüsseln finden Sie unter Abschnitt 11.8.5, „Vorher vereinbarte (pre-shared) Schlüssel verwalten".

Abschnitt 11.8.1.4
X.509-Zertifikate

Neben vorher vereinbarten Schlüsseln verwendet IPSec auch Zertifikate, um die Verbindungen mit Hosts und Routern zu authentifizieren. Bei den Zertifikaten handelt es sich um digitale Signaturen, die von einer vertrauenswürdigen Quelle, d. h. einer Zertifizierungsstelle (Certificate Authority, CA) ausgestellt werden, Die CA erstellt für jeden Host ein Zertifikat, das Angaben zu CA und Host enthält. Das Zertifikat wird "signiert", indem ein Digest aller Felder im Zertifikat erstellt und anschließend der Hash-Wert mit dessen privaten Schlüssel verschlüsselt wird. Das Zertifikat des Hosts und der öffentliche Schlüssel der CA werden auf allen Gateways installiert, mit denen der Host verbunden ist.

Wenn das Gateway einen Verbindungsaufforderung empfängt, entschlüsselt es mithilfe des öffentlichen Schlüssels der CA die Signatur zurück in das Digest. Daraufhin berechnet es das eigene Digest aus dem Klartext im Zertifikat neu und vergleicht die zwei. Wenn beide Digests übereinstimmen, ist die Integrität des Zertifikats bestätigt (es wurde nicht manipuliert), und der öffentliche Schlüssel im Zertifikat wird als gültiger öffentlicher Schlüssel des verbindenden Hosts angenommen.

Abschnitt 11.8.1.5
NAT Traversal

IPsec hatte früher Probleme, wenn Verbindungen eine Firewall mit Network Address Translation (NAT) passieren mussten. Der in IPsec verwendete Internet Key Exchange (IKE) ist nicht NAT-fähig. Wenn IPsec-Verbindungen eine Firewall passieren müssen, müssen IKE-Meldungen und IPsec-geschützte Pakete als UDP-(User Datagram Protocol)-Meldungen gekapselt werden. Durch die Kapselung kann das unübersetzte Originalpaket von IPsec untersucht werden.

Die Kapselung wird während der Konfiguration von IPsec aktiviert. Weitere Informationen finden Sie unter Abschnitt 11.8.2, „Konfigurieren von IPsec-Tunneln".

Abschnitt 11.8.1.6
Unterstützung eines entfernten IPsec-Clients

Soll der Router einen entfernten IPsec-Client unterstützen und dem Client wird eine Adresse in einem Subnetz einer lokalen Schnittstelle zugewiesen, muss ein Proxy-ARP für diese Schnittstelle aktiviert werden. Der Router kann dann im Namen des Client auf ARP-Anforderungen antworten und dem Client den Verkehr über seine Verbindung leiten.

IPsec verwendet die folgenden Protokolle und Ports:

- protocol 51, IPSEC-AH Authentication Header (RFC2402)

- protocol 50, IPSEC-ESP Encapsulating Security Payload (RFC2046)
- UDP port 500

Die Firewall muss so konfiguriert werden, dass sie Verbindungen für diese Ports und Protokolle akzeptiert. Weitere Informationen finden Sie unter Abschnitt 6.7.6, „Konfigurieren der Firewall für ein VPN“.

Abschnitt 11.8.1.7
IPsec- und Router-Schnittstellen

Wenn IPsec an einer Schnittstelle betrieben wird, die verschwinden kann, zum Beispiel einer PPP-Verbindung, oder wenn sich die IP-Adresse ändern kann, muss Option **Monitor Interface** für die IPsec-Verbindung gesetzt werden. Wenn diese Option gesetzt ist, startet IPsec neu, wenn die Schnittstelle verschwindet und wieder zurückkehrt, oder wenn die IP-Adresse sich ändert.

Option **Monitor Interface** wird im Formular **Connection** gesetzt, das für jede Verbindung vorhanden ist. Weitere Informationen über Verbindungen finden Sie unter Abschnitt 11.8.6, „Verbindungen verwalten“.

Abschnitt 11.8.2
Konfigurieren von IPsec-Tunneln

Um IPSec-Tunnel zu konfigurieren, gehen Sie wie folgt vor:

HINWEIS
Der RUGGEDCOM ROX II unterstützt die Erstellung von auf Grundregeln basierenden VPNs, die wie folgt charakterisiert werden:

- *Es wurden keine IPsec-Netzwerkschnittstellen erstellt.*
- *Die Routing-Tabelle ist nicht an der Umleitung von Paketen an IPSec beteiligt.*
- *Es wird nur der Datenverkehr an den Tunnel weitergeleitet, der mit den lokalen und dezentralen Subnetzen des Tunnels übereinstimmt. Normaler Verkehr wird von einem Satz Firewall-Regeln und VPN-Verkehr wird basierend auf separaten Regeln geleitet.*
- *Die Firewall wird mit einer VPN-Zone vom Typ **ipsec** konfiguriert.*
- *Bei Empfang von IPSec-Paketen werden diese dekodiert, als IPSec-codiert markiert und so präsentiert, als wären sie direkt von derselben Netzwerkschnittstelle gekommen, an der sie ursprünglich empfangen wurden.*
- *Firewall-Regeln werden geschrieben, um den Datenverkehr zu und von VPN-Tunneln zuzulassen. Diese basieren auf der normalen Form der IP-Quell-/Zieladressen und IP-Protokoll- und Portnummern. Diese Regeln verwenden, kraft der Zonen, mit denen sie übereinstimmen, vom Netkey stammende Grundregelmerker, um übereinstimmenden Datenverkehr an die korrekte Schnittstelle zu leiten.*

Weitere Informationen über das Konfigurieren eines auf Grundregeln basierenden VPN finden Sie in Abschnitt 6.7, „Verwalten von Firewalls“.

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***tunnel » ipsec*** und konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
enabled	Aktiviert IPsec.

Parameter	Beschreibung
nat-traversal	Dieser Parameter wird nicht unterstützt und sämtliche Werte werden vom System ignoriert. "nat-traversal" ist im IPsec-VPN-System immer aktiviert.
keep-alive { keep-alive }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 1 und 86400 **Standard:** 20 Die Verzögerung (in Sekunden) für das Senden von Keepalive-Paketen, um zu verhindern, dass ein NAT-Router seinen Port schließt, wenn nicht genügend Datenverkehr auf der IPsec-Verbindung vorhanden ist.

3. Konfigurieren Sie einen oder mehrere vorher vereinbarte Schlüssel. Weitere Informationen finden Sie unter Abschnitt 11.8.5.2, „Einen vorher vereinbarten Schlüssel hinzufügen“.
4. Konfigurieren Sie eine oder mehrere verschlüsselte Verbindungen. Weitere Informationen finden Sie unter Abschnitt 11.8.6.2, „Hinzufügen einer Verbindung“.
5. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.8.3

Konfigurieren von Zertifikaten und Schlüsseln

Um Zertifikate und Schlüssel für IPSec-Tunnel zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie ein CA-Zertifikat und die Zertifikatsperrliste (CRL) hinzu. Weitere Informationen finden Sie unter Abschnitt 6.6.4.3, „Hinzufügen eines CA-Zertifikats und der CRL“.
3. Fügen Sie einen privaten Schlüssel hinzu. Weitere Informationen finden Sie unter Abschnitt 6.6.5.2, „Einen privaten Schlüssel hinzufügen“.
4. Fügen Sie ein Zertifikat hinzu. Weitere Informationen finden Sie unter Abschnitt 6.6.7.3, „Hinzufügen eines Zertifikats“.
5. Fügen Sie einen öffentlichen Schlüssel hinzu. Weitere Informationen finden Sie unter Abschnitt 6.6.6.2, „Hinzufügen eines öffentlichen Schlüssels“.
6. Navigieren Sie zu ***tunnel » ipsec » connection » {connection} » {end}***, wobei *{connection}* die Bezeichnung der Verbindung und *{end}* entweder das linke (lokaler Router) oder rechte (dezentraler Router) Verbindungsende ist.
7. Konfigurieren Sie den öffentlichen Schlüssel des Systems, indem Sie Folgendes eingeben:

   ```
   tunnel ipsec connection connection [ left | right ] key type certificate
   ```

   Erläuterung:

   - *`connection`* ist die Bezeichnung der Verbindung
8. Konfigurieren Sie die Kennung des Systems, indem Sie Folgendes eingeben:

   ```
   tunnel ipsec connection connection [ left | right ] identifier type from-certificate
   ```

   Erläuterung:

   - *`connection`* ist die Bezeichnung der Verbindung
9. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.8.4

Anzeigen des Status des IPSec-Tunnels

Um den Status des IPSec-Tunnels anzuzeigen, geben Sie Folgendes ein:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Zeigen Sie den Status an, indem Sie Folgendes eingeben:

```
tunnel ipsec status
```

Eine Tabelle oder Liste ähnlich dem folgenden Beispiel wird angezeigt:

```
status
============================================================
000 using kernel interface: netkey
000 interface lo/lo :1
000 interface lo/lo 127.0.0.1
000 interface vrf_gw0/vrf_gw0 169.254.0.1
000 interface switch.0001/switch.0001 192.168.0.2
000 interface switch.1000/switch.1000 172.30.151.38
000 %myid = (none)
000 debug none
000
000 virtual_private (%priv):
000 - allowed 0 subnets:
000 - disallowed 0 subnets:
000 WARNING: Either virtual_private= is not specified, or there is a syntax
000          error in that line. 'left/rightsubnet=vhost:%priv' will not work!
000 WARNING: Disallowed subnets in virtual_private= is empty. If you have
000          private address space in internal use, it should be excluded!
000
000 algorithm ESP encrypt: id=2, name=ESP_DES, ivlen=8, keysizemin=64, keysizemax=64
000 algorithm ESP encrypt: id=3, name=ESP_3DES, ivlen=8, keysizemin=192, keysizemax=192
000 algorithm ESP encrypt: id=11, name=ESP_NULL, ivlen=0, keysizemin=0, keysizemax=0
000 algorithm ESP encrypt: id=12, name=ESP_AES, ivlen=8, keysizemin=128, keysizemax=256
000 algorithm ESP encrypt: id=14, name=ESP_AES_CCM_A, ivlen=8, keysizemin=128, keysizemax=256
000 algorithm ESP encrypt: id=15, name=ESP_AES_CCM_B, ivlen=8, keysizemin=128, keysizemax=256
000 algorithm ESP encrypt: id=252, name=ESP_SERPENT, ivlen=8, keysizemin=128, keysizemax=256
000 algorithm ESP encrypt: id=253, name=ESP_TWOFISH, ivlen=8, keysizemin=128, keysizemax=256
000 algorithm ESP auth attr: id=1, name=AUTH_ALGORITHM_HMAC_MD5, keysizemin=128, keysizemax=128
000 algorithm ESP auth attr: id=2, name=AUTH_ALGORITHM_HMAC_SHA1, keysizemin=160, keysizemax=160
000 algorithm ESP auth attr: id=251, name=(null), keysizemin=0, keysizemax=0
000
000 algorithm IKE encrypt: id=0, name=(null), blocksize=16, keydeflen=131
000 algorithm IKE encrypt: id=3, name=OAKLEY_BLOWFISH_CBC, blocksize=8, keydeflen=128
000 algorithm IKE encrypt: id=65289, name=OAKLEY_TWOFISH_CBC_SSH, blocksize=16, keydeflen=128
000 algorithm IKE hash: id=1, name=OAKLEY_MD5, hashsize=16
000 algorithm IKE hash: id=2, name=OAKLEY_SHA1, hashsize=20
000 algorithm IKE hash: id=4, name=OAKLEY_SHA2_256, hashsize=32
000 algorithm IKE hash: id=6, name=OAKLEY_SHA2_512, hashsize=64
000 algorithm IKE dh group: id=2, name=OAKLEY_GROUP_MODP1024, bits=1024
000 algorithm IKE dh group: id=5, name=OAKLEY_GROUP_MODP1536, bits=1536
000 algorithm IKE dh group: id=18, name=OAKLEY_GROUP_MODP8192, bits=8192
000
000 stats db_ops: {curr_cnt, total_cnt, maxsz} :context={0,0,0} trans={0,0,0} attrs={0,0,0}
000
000 "ipsec-12": 192.168.22.0/24===192.168.12.2<192.168.12.2>[C=CA, ST=Ontario, O=RuggedCom,
 CN=router2, E=router2@example.com,+S=C]...192.168.12.1<192.168.12.1>[C=CA, ST=Ontari o,
 O=RuggedCom, CN=router1, E=router1@example.com,+S=C]===192.168.11.0/24; erouted; eroute owner: #2
000 "ipsec-12":     myip=unset; hisip=unset; myup=ipsec _updown --route yes; hisup=ipsec _updown --
route yes; mycert=router2;
000 "ipsec-12":   CAs: 'C=CA, ST=Ontario, O=RuggedCom, CN=CA, E=ca@example.com'...'%any'
000 "ipsec-12":   ike_life: 3600s; ipsec_life: 28800s; rekey_margin: 540s; rekey_fuzz: 100%;
 keyingtries: 0
```

```
000 "ipsec-12":   policy: RSASIG+ENCRYPT+TUNNEL+PFS+UP+IKEv2ALLOW+lKOD+rKOD; prio: 24,24;
 interface: switch.0012;
000 "ipsec-12":   newest ISAKMP SA: #4; newest IPsec SA: #2;
000 "ipsec-12":   IKE algorithm newest: AES_CBC_128-SHA1-MODP2048
000
000 #4: "ipsec-12":500 STATE_MAIN_I4 (ISAKMP SA established); EVENT_SA_REPLACE in 106s; newest
 ISAKMP; lastdpd=-1s(seq in:0 out:0); idle; import:admin initiate
000 #2: "ipsec-12":500 STATE_QUICK_I2 (sent QI2, IPsec SA established); EVENT_SA_REPLACE in 19349s;
 newest IPSEC; eroute owner; isakmp#1; idle; import:admin initiate
000 #2: "ipsec-12" esp.edfbc8f8@192.168.12.1 esp.53ffca14@192.168.12.2 tun.0@192.168.12.1
 tun.0@192.168.12.2 ref=0 refhim=4294901761
000
```

Abschnitt 11.8.5

Vorher vereinbarte (pre-shared) Schlüssel verwalten

Vorher vereinbarte Schlüssel werden in der Verschlüsselung von *geheimen Schlüsseln* verwendet. Weitere Informationen über die Verschlüsselung *geheimer Schlüssel* und vorher vereinbarte Schlüssel finden Sie unter Abschnitt 11.8.1.3, „Kryptografie von öffentlichen und geheimen Schlüsseln“.

INHALT

- Abschnitt 11.8.5.1, „Eine Liste der vorher vereinbarten Schlüssel anzeigen“
- Abschnitt 11.8.5.2, „Einen vorher vereinbarten Schlüssel hinzufügen“
- Abschnitt 11.8.5.3, „Einen vorher vereinbarten Schlüssel löschen“

Abschnitt 11.8.5.1

Eine Liste der vorher vereinbarten Schlüssel anzeigen

Um eine Liste der vorher vereinbarten (pre-shared) Schlüssel anzusehen, geben Sie Folgendes ein:

```
show running-config tunnel ipsec preshared-key
```

Falls solche Schlüssel konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config tunnel ipsec preshared-key
tunnel
 ipsec
  preshared-key 192.168.12.1 192.168.12.2
   key $4$9YslfOBfkyYV8c1tqN4IDw==
  !
 !
!
```

Falls keine vorher vereinbarten Schlüssel konfiguriert wurden, fügen Sie je nach Bedarf Schlüssel hinzu. Weitere Informationen finden Sie unter Abschnitt 11.8.5.2, „Einen vorher vereinbarten Schlüssel hinzufügen“.

Abschnitt 11.8.5.2

Einen vorher vereinbarten Schlüssel hinzufügen

Um einen vorher vereinbarten Schlüssel hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.

2. Fügen Sie den vorher vereinbarten Schlüssel hinzu, indem Sie Folgendes eingeben:

```
tunnel ipsec preshared-key [ remote-address | local-address ] key key
```

Erläuterung:

- *remote-address* ist die dezentrale IP-Adresse
- *local-address* ist die lokale IP-Adresse
- *key* ist der Inhalt des vorher vereinbarten Schlüssels

3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
key { key }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 8192 Zeichen Der vorher vereinbarte Schlüssel. Dieser Parameter ist obligatorisch.

4. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.8.5.3

Einen vorher vereinbarten Schlüssel löschen

Um einen vorher vereinbarten Schlüssel zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den vorher vereinbarten Schlüssel, indem Sie Folgendes eingeben:

```
no tunnel ipsec preshared-key [ remote-address | local-address ] key key
```

Erläuterung:

- *remote-address* ist die dezentrale IP-Adresse
- *local-address* ist die lokale IP-Adresse
- *key* ist der Inhalt des vorher vereinbarten Schlüssels

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.8.6

Verbindungen verwalten

Eine IPsec-Verbindung ist eine verschlüsselte Verbindung zwischen zwei Geräten mit dem gleichen zuvor autorisierten Authentifizierungsschlüssel.

INHALT

- Abschnitt 11.8.6.1, „Eine Liste der Verbindungen anzeigen“
- Abschnitt 11.8.6.2, „Hinzufügen einer Verbindung“
- Abschnitt 11.8.6.3, „Konfigurieren der Dead Peer Detection“
- Abschnitt 11.8.6.4, „Eine Verbindung löschen“

Abschnitt 11.8.6.1

Eine Liste der Verbindungen anzeigen

Um eine Liste der für ein VPN konfigurierten Verbindungen anzusehen, geben Sie Folgendes ein:

```
show tunnel ipsec connection
```

Falls Verbindungen konfiguriert wurden, wird eine Tabelle ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config tunnel ipsec connection
tunnel
 ipsec
  connection ipsec-12
   no l2tp
   ike algorithm 3des md5 modp8192
   !
   esp algorithm aes256 sha1
   !
   left
    public-ip type default-route
    subnet 192.168.11.0/24
    !
   !
   right
    public-ip type any
   !
  !
 !
!
```

Falls keine Verbindungen konfiguriert wurden, fügen Sie je nach Bedarf Verbindungen hinzu. Weitere Informationen finden Sie unter Abschnitt 11.8.6.2, „Hinzufügen einer Verbindung“.

Abschnitt 11.8.6.2

Hinzufügen einer Verbindung

Um zu einem VPN eine neue Verbindung hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie die Verbindung hinzu, indem Sie Folgendes eingeben:

   ```
   tunnel ipsec connection name
   ```

   Erläuterung:

   - *name* ist der Verbindungsname. Wenn der Name *default* ist, ist dies die Standardeinstellung für alle Verbindungen.
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
startup { startup }	**Zusammenfassung:** { ignore, add, start, route, default } **Standard:** default Zu treffende Maßnahme, wenn IPsec initialisiert ist. Der Standardwert ist 'ignore', sofern er nicht von der Standard-Verbindungseinstellung überschrieben ist.
authenticate { authenticate }	**Zusammenfassung:** { default, rsasig, secret } **Standard:** default Die Authentifizierungsmethode. Der Standardwert ist 'default', sofern er nicht von der Standard-Verbindungseinstellung überschrieben ist.

Parameter	Beschreibung
connection-type { connection-type }	**Zusammenfassung:** { tunnel, transport, passthrough, default } **Standard:** default Der Typ/Modus der Verbindung. Mögliche Optionen sind: • tunnel: Verschlüsselt den Verkehr in Host-zu-Host-, Host-zu-Subnetz- oder Subnetz-zu-Subnetz-Tunneln. Dieser Typ/Modus ist voreingestellt, sofern er nicht von der Standard-Verbindungseinstellung überschrieben ist. • transport: Verschlüsselt den Verkehr in einem Host-zu-Host-Tunnel. • passthrough: Der Verkehr ist nicht verschlüsselt.
address-family { address-family }	**Zusammenfassung:** { ipv4, ipv6 } **Standard:** ipv4 Die für die Verbindung auszuführende "adress-family". Zulässige Werte sind 'ipv4' (Default-Wert) und 'ipv6'. Die Familie aller in der Verbindung verwendeten Adressen muss übereinstimmen.
pfs { pfs }	**Zusammenfassung:** { default, yes, no } **Standard:** default Aktiviert/deaktiviert Perfect Forwarding Secrecy (PFS). Wenn aktiviert, verhandelt IPsec neue Schlüssel für jede Sitzung. Wenn ein Angreifer einen Schlüssel gefährdet, wird nur die Sitzung erkannt, die durch den Schlüssel geschützt ist. Nicht alle Clients unterstützen PFS. Der Standardwert ist 'yes', sofern er nicht von der Standard-Verbindungseinstellung überschrieben ist.
keylife { keylife }	**Zusammenfassung:** { default } oder eine vorzeichenlose 32-Bit-Ganzzahl zwischen 1081 und 28800 **Standard:** default Die Lebensdauer in Sekunden für den Security Association (SA)-Schlüssel. Sie bestimmt, wie lange eine bestimmte Instanz einer Verbindung von erfolgreicher Verhandlung zum Ablaufen dauern soll. Normalerweise wird die Verbindung vor dem Ablaufen erneut verhandelt. Der Standardwert ist 28800, sofern er nicht von der Standard-Verbindungseinstellung überschrieben ist. Peers können unterschiedliche Lebensdauerintervalle festlegen. Wenn sich Peers jedoch nicht einigen, kommt es zu einem Überschuss an abgelaufenen Verbindungen an dem Peer, der glaubt, dass die SA-Lebensdauer länger ist.
ike-lifetime { ike-lifetime }	**Zusammenfassung:** { default } oder eine vorzeichenlose 32-Bit-Ganzzahl zwischen 60 und 86400 **Standard:** default Die Lebensdauer in Sekunden für das IKE-Protokoll. Sie bestimmt, wie lange der IKE-Schlüsselfindungs-Kanal einer Verbindung dauern soll, bis er erneut verhandelt wird. Der Standardwert ist 3600, sofern er nicht von der Standard-Verbindungseinstellung überschrieben ist. Peers können unterschiedliche Lebensdauerintervalle festlegen. Wenn sich Peers jedoch nicht einigen, kommt es zu einem Überschuss an abgelaufenen Verbindungen an dem Peer, der glaubt, dass die IKE-Lebensdauer länger ist.
l2tp	Aktiviert/deaktiviert L2TP für diese Verbindung.
monitor-interface { monitor-interface }	**Zusammenfassung:** Eine Zeichenkette Die zu überwachende Schnittstelle. Wenn die gewählte Schnittstelle nicht verfügbar ("down") und dann wieder verfügbar ("up") ist, wird diese Verbindung neugestartet.

4. Bei Bedarf aktivieren und konfigurieren Sie Dead Peer Detection. Weitere Informationen finden Sie unter Abschnitt 11.8.6.3, „Konfigurieren der Dead Peer Detection“.
5. Bei Bedarf konfigurieren Sie das Internet Key Exchange (IKE)-Protokoll, indem Sie einen oder mehrere Algorithmen hinzufügen. Weitere Informationen finden Sie unter Abschnitt 11.8.7.2, „Hinzufügen eines IKE-Algorithmus“.
6. Bei Bedarf konfigurieren Sie die Encapsulated Security Payload-(ESP)-Verschlüsselung für die Verbindung. Weitere Informationen finden Sie unter Abschnitt 11.8.8, „Ein ESP-Protokoll (Encapsulated Security Payload) verwalten“.

7. Bei Bedarf konfigurieren Sie das linke (lokaler Router) oder rechte (dezentraler Router) Verbindungsende. Weitere Informationen finden Sie unter Abschnitt 11.8.9, „Konfigurieren der Verbindungsenden“.
8. Bei Bedarf konfigurieren Sie L2TP-Tunnel. Weitere Informationen finden Sie unter Abschnitt 11.3.1, „Konfigurieren von L2TP-Tunneln“.
9. Falls Zertifikate und Schlüssel erforderlich sind, stellen Sie sicher, dass diese auf dem Gerät konfiguriert sind. Weitere Informationen finden Sie unter Abschnitt 11.8.3, „Konfigurieren von Zertifikaten und Schlüsseln“.
10. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.8.6.3

Konfigurieren der Dead Peer Detection

Die Dead Peer Detection (DPD) wird gemäß RFC 3706 [http://tools.ietf.org/html/rfc3706] zum Erkennen von Dead Internet Key Exchange (IKE)-Peers verwendet. Bei diesem Verfahren tauschen Peers DPD-Anfragenachrichten (ISAKMP R-U-THERE) und DPD-Antwortnachrichten (ISAKMP R-U-THERE-ACK) aus. Wenn eine DPD-Antwort nach einer festgelegten Zeit bzw. nach einer festgelegten Anzahl an Versuchen nicht von einem Peer empfangen wurde, wird der andere Peer als *Dead* betrachtet. Der verbleibende Peer kann die Verbindung entweder halten, bis der andere Peer antwortet, oder die Verbindung löschen, neu starten und die Security Association (SA) neu verhandeln oder alle SAs zum Dead Peer neu starten.

Der RUGGEDCOM ROX II sendet DPD-Anfragen, wenn vom Peer kein Verkehr erkannt wird. Die Zeit, die bis zum Senden einer DPD-Anfrage bzw. die für das Warten auf eine DPD-Antwort gewartet werden soll, ist vom Benutzer konfigurierbar.

Im Allgemeinen wird empfohlen, DPD so zu konfigurieren, dass Verbindungen mit Dead Peers gelöscht werden.

Um eine Dead Peer Detection für eine IPSec-Verbindung zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Aktivieren Sie Dead Peer Detection, indem Sie Folgendes eingeben:

```
tunnel ipsec connection name dead-peer-detect enabled [ true | false ]
```

   Erläuterung:

   - *`name`* ist der Verbindungsname.

3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:



HINWEIS
Der Timeout-Zeitraum muss zwei Minuten länger andauern als der Intervall-Zeitraum.

Parameter	Beschreibung
interval { interval }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 1 und 3600 **Standard:** 30 Das Intervall (in Sekunden) zwischen Dead Peer Detection-Keepalive-Meldungen, die für diese Verbindung gesendet werden, wenn kein Verkehr (Bereitschaft) von einem DPD-fähigen Peer gesendet zu werden scheint.
timeout { timeout }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 1 und 28800 **Standard:** 120 Die Wartezeit (in Sekunden), bevor der Peer für tot erklärt wird.

Parameter	Beschreibung
	HINWEIS *Der Timeout-Zeitraum muss mehr als das Doppelte des Intervalls sein.*
action { action }	**Zusammenfassung:** { hold, clear, restart, restart-all-sa } **Standard:** restart Die zu ergreifende Maßnahme, wenn ein DPD-fähiger Peer für tot erklärt ist. Mögliche Optionen sind: • hold: Die Route wird in einen Halten-Status versetzt • clear: Sowohl Route als auch Security Association (SA) werden beide gelöscht. • restart: Die SA wird unmittelbar neu verhandelt • restart-all-sa: Alle SA zum toten Peer werden neu verhandelt

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.8.6.4
Eine Verbindung löschen

Um eine Verbindung für ein VPN zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die Verbindung durch Eingabe von:

```
no tunnel ipsec connection name
```

Erläuterung:

- *`name`* ist die Bezeichnung der Verbindung

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.8.7
Das IKE-(Internet Key Exchange)-Protokoll verwalten

Das IKE-(Internet Key Exchange)-Protokoll verhandelt Verbindungsparameter einschließlich Schlüssel für das von IPsec benutzte ESP-(Encapsulated Security Payload)-Protokoll. IKE basiert auf dem Diffie-Hellman-Protokoll für Schlüsselaustausch, mit dem zwei Partner einen gemeinsamen geheimen Schlüssel vereinbaren können, den ein potenzieller Lauscher nicht berechnen kann.

INHALT

• Abschnitt 11.8.7.1, „Eine Liste der IKE-Algorithmen anzeigen“
• Abschnitt 11.8.7.2, „Hinzufügen eines IKE-Algorithmus“
• Abschnitt 11.8.7.3, „Löschen eines IKE-Algorithmus“

Abschnitt 11.8.7.1
Eine Liste der IKE-Algorithmen anzeigen

Um eine Liste der Algorithmen für das IKE-(Internet Key Exchange)-Protokoll anzusehen, geben Sie Folgendes ein:

```
show running-config tunnel ipsec connection connection ike algorithm
```

Erläuterung:

- *connection* ist die Bezeichnung der Verbindung

Falls Algorithmen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
tunnel
 ipsec
  connection ipsec-12
   ike algorithm 3des md5 modp8192
   !
  !
 !
!
```

Falls keine Algorithmen konfiguriert wurden, fügen Sie je nach Bedarf Algorithmen hinzu. Weitere Informationen finden Sie unter Abschnitt 11.8.7.2, „Hinzufügen eines IKE-Algorithmus“.

Abschnitt 11.8.7.2
Hinzufügen eines IKE-Algorithmus

Um einen neuen Algorithmus zum Internet Key Exchange (IKE)-Protokoll hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den Algorithmus hinzu, indem Sie Folgendes eingeben:

   ```
   tunnel ipsec connection connection ike algorithm cipher method modpgroup
   ```

   Erläuterung:

   - *connection* ist die Bezeichnung der Verbindung.
   - *cipher* ist der Verschlüsselungsalgorithmus. Optionen sind u.a. `3des`, `aes`, `aes128`, `aes192`, `aes256` und `any`. Die Voreinstellung ist `aes`. Die Option `any` wählt die Voreinstellung.
   - *method* ist das Hash-Verfahren. Optionen sind u.a. `any`, `md5`, `sha1` und `sha2`. Die Voreinstellung ist `sha1`. Die Option `any` wählt die Voreinstellung.
   - *modpgroup* ist der Wert der Modular Exponential (MODP)-Gruppe. Optionen sind u.a. `any`, `modp1024`, `modp1536`, `modp2048`, `modp3072`, `modp4096`, `modp6144` und `modp8192`. Die Voreinstellung ist `modp2048`. Die Option `any` wählt die Voreinstellung.
3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.8.7.3
Löschen eines IKE-Algorithmus

Um einen Algorithmus zum Internet Key Exchange (IKE)-Protokoll zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.

2. Löschen Sie den Algorithmus, indem Sie Folgendes eingeben:

```
no tunnel ipsec connection connection ike algorithm cipher method modpgroup
```

Erläuterung:

- *connection* ist die Bezeichnung der Verbindung.
- *cipher* ist der Verschlüsselungsalgorithmus. Optionen sind u.a. 3des, aes, aes128, aes192, aes256 und any. Die Voreinstellung ist aes. Die Option any wählt die Voreinstellung.
- *method* ist das Hash-Verfahren. Optionen sind u.a. any, md5, sha1 und sha2. Die Voreinstellung ist sha1. Die Option any wählt die Voreinstellung.
- *modpgroup* ist der Wert der Modular Exponential (MODP)-Gruppe. Optionen sind u.a. any, modp1024, modp1536, modp2048, modp3072, modp4096, modp6144 und modp8192. Die Voreinstellung ist modp2048. Die Option any wählt die Voreinstellung.

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.8.8

Ein ESP-Protokoll (Encapsulated Security Payload) verwalten

Das von IPsec benutzte ESP (Encapsulated Security Payload) stellt Verschlüsselungs- und Authentifizierungsfunktionen bereit, mit denen sichergestellt werden kann, dass während der Übertragung Meldungen von einem erwarteten Absender nicht verändert wurden.

INHALT

- Abschnitt 11.8.8.1, „Konfigurieren der ESP-Verschlüsselung“
- Abschnitt 11.8.8.2, „Eine Liste der ESP-Algorithmen anzeigen“
- Abschnitt 11.8.8.3, „Einen ESP-Algorithmus hinzufügen“
- Abschnitt 11.8.8.4, „Einen ESP-Algorithmus löschen“

Abschnitt 11.8.8.1

Konfigurieren der ESP-Verschlüsselung

Um den Verschlüsselungsalgorithmus für das Encapsulated Security Payload (ESP)-Protokoll zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***tunnel » ipsec » connection » {connection} » esp***, wobei *{connection}* die Bezeichnung der Verbindung ist.
3. Konfigurieren Sie den Verschlüsselungsalgorithmus, indem Sie Folgendes eingeben:

```
tunnel ipsec connection connection esp modpgroup modpgroup
```

Erläuterung:

- *connection* ist die Bezeichnung der Verbindung.

- *modpgroup* ist die Modular Exponential (MODP)-Gruppe. Optionen sind u.a. `any`, `modp1024`, `modp1536`, `modp2048`, `modp3072`, `modp4096`, `modp6144` und `modp8192`. Die Voreinstellung ist `modp2048` je nach Standard-Verbindungseinstellung. Die Option `any` wählt die Voreinstellung.

4. Fügen Sie bei Bedarf zusätzliche Verschlüsselungsalgorithmen hinzu. Weitere Informationen über das Hinzufügen von Algorithmen finden Sie unter Abschnitt 11.8.8.3, „Einen ESP-Algorithmus hinzufügen“.
5. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.8.8.2
Eine Liste der ESP-Algorithmen anzeigen

Um eine Liste der Algorithmen für das ESP-(Encapsulate Security Payload)-Protokoll anzusehen, geben Sie Folgendes ein:

```
show running-config tunnel ipsec connection connection esp algorithm
```

Erläuterung:

- *connection* ist die Bezeichnung der Verbindung

Falls Algorithmen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
tunnel
 ipsec
  connection ipsec-12
   esp algorithm aes256 sha1
   !
  !
 !
!
```

Falls keine Algorithmen konfiguriert wurden, fügen Sie je nach Bedarf Algorithmen hinzu. Weitere Informationen finden Sie unter Abschnitt 11.8.8.3, „Einen ESP-Algorithmus hinzufügen“.

Abschnitt 11.8.8.3
Einen ESP-Algorithmus hinzufügen

Um einen neuen Algorithmus für das Encapsulated Security Payload (ESP)-Protokoll hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den Algorithmus hinzu, indem Sie Folgendes eingeben:

   ```
   tunnel ipsec connection connection esp algorithm cipher method
   ```

   Erläuterung:

   - *connection* ist die Bezeichnung der Verbindung.
   - *cipher* ist der Verschlüsselungsalgorithmus. Optionen sind u.a. `3des`, `aes`, `aes128`, `aes192`, `aes256` und `any`. Die Voreinstellung ist `aes`. Die Option `any` wählt die Voreinstellung.
   - *method* ist das Hash-Verfahren. Optionen sind u.a. `any`, `md5`, `sha1` und `sha2`. Die Voreinstellung ist `sha1`. Die Option `any` wählt die Voreinstellung.

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.8.8.4
Einen ESP-Algorithmus löschen

Um einen Algorithmus für das Encapsulated Security Payload (ESP)-Protokoll zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den Algorithmus, indem Sie Folgendes eingeben:

   ```
   no tunnel ipsec connection connection esp algorithm cipher method
   ```

   Erläuterung:

   - *`connection`* ist die Bezeichnung der Verbindung
   - *`cipher`* ist der Verschlüsselungsalgorithmus. Optionen sind u.a. `3des`, `aes`, `aes128`, `aes192`, `aes256` und `any`. Die Voreinstellung ist `aes`. Die Option `any` wählt die Voreinstellung.
   - *`method`* ist das Hash-Verfahren. Optionen sind u.a. `any`, `md5`, `sha1` und `sha2`. Die Voreinstellung ist `sha1`. Die Option `any` wählt die Voreinstellung.
3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.8.9
Konfigurieren der Verbindungsenden

Jeder IPSec-Tunnel besitzt zwei Enden: den lokalen Router und den dezentralen Router. Diese werden auch als die linke bzw. rechte Verbindung bezeichnet. Beide Enden können dieselbe Konfiguration oder eine einmalige Konfiguration haben.

Um ein Verbindungsende für einen IPSec-Tunnel zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***tunnel » ipsec » connection » {name} » {end}***, wobei *{name}* die Bezeichnung der Verbindung und *{end}* entweder das linke (lokaler Router) oder rechte (dezentraler Router) Verbindungsende ist.
3. Konfigurieren Sie die öffentliche IP-Adresse mithilfe der folgenden Parameter:

Parameter	Beschreibung
type { type }	**Zusammenfassung:** { none, default-route, any, address, hostname } **Standard:** none Der Typ der öffentlichen IP-Adresse.
value { value }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 4095 Zeichen Der öffentliche Hostname oder die öffentliche IP-Adresse.

4. Konfigurieren Sie den öffentlichen Schlüssel des Systems mithilfe der folgenden Parameter:

Parameter	Beschreibung
type { type }	**Zusammenfassung:** { none, rsasig, certificate-any, certificate } **Standard:** none

Parameter	Beschreibung
	Schlüsseltyp.
rsa-sig { rsa-sig }	**Zusammenfassung:** Eine Zeichenkette Der Schlüsselname der RSA-Signatur. **HINWEIS** *Schlüssel "ipsec rsa-sig" muss RSA-Algorithmus verwenden*
rsa-sig-ipsec	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 8192 Zeichen Die RSA-Signatur im IPsec-Format.
certificate { certificate }	**Zusammenfassung:** Eine Zeichenkette Das ausgewählte Zertifikat.

5. Konfigurieren Sie die Kennung des Systems mithilfe der folgenden Parameter:

Parameter	Beschreibung
type { type }	**Zusammenfassung:** { default, none, from-certificate, address, hostname, der-asn1-dn, user-fqdn } **Standard:** default Der Typ der Systemkennung. Der Standardwert ist 'left side public-ip', sofern er nicht von der Standard-Verbindungseinstellung überschrieben ist.
value { value }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 1024 Zeichen Der Hostname, die IP-Adresse oder der im Zertifikat gekennzeichnete Name.

6. Konfigurieren Sie den nächsten Hop zum anderen System mithilfe der folgenden Parameter:

Parameter	Beschreibung
type { type }	**Zusammenfassung:** { default, default-route, address } **Standard:** default Der Typ des nächsten Hops. Der Standardwert ist 'right side public-ip', sofern er nicht von der Standard-Verbindungseinstellung überschrieben ist.
value { value }	**Zusammenfassung:** Eine Zeichenkette mit 7 bis 15 Zeichen Die IP-Adresse des nächsten Hops, die zum Erreichen des Zielnetzwerks verwendet werden kann.

7. Konfigurieren Sie die Traversal-Negotiationsmethode der Netzadressenübersetzung (NAT), indem Sie die folgenden Parameter konfigurieren:

HINWEIS
Die Verwendung der RFC 3947-Negotiationsmethode anstelle von draft-ietf-ipsec-nat-t-ike-02 führt möglicherweise zu Problemen beim Herstellen der Verbindung zum IPSec-Server, da RFC 3947 andere Kennungen verwendet, wenn NAT involviert ist. Wenn sich beispielsweise ein Windows XP/2003-Client verbindet, dann meldet Libreswan die Main-Mode-Peer-ID ***ID_FQDN: '@example.com'****. Wenn sich jedoch ein Vista-, Windows 7- oder anderer RFC 3947-konformer Client verbindet, dann meldet Libreswan die Main-Mode-Peer-ID* ***ID_IPV4_ADDR: '192.168.1.1'****. Sofern möglich, verwenden Sie die Methode "draft-ietf-ipsec-nat-t-ike-02", um dieses Problem zu vermeiden.*

Parameter	Beschreibung
nat-traversal-negotiation { nat-traversal-negotiation }	**Zusammenfassung:** { default, draft-ietf-ipsec-nat-t-ike-02, rfc-3947 } **Standard:** default Die NAT Traversal-Negotiationsmethode. Einige IPsec-Endpunkte bevorzugen bei der Verbindung mit Libreswan RFC 3947 gegenüber "draft-ietf-ipsec-nat-t-ike-02", da diese Implementierungen unterschiedliche Kennungen verwenden, wenn NAT verwendet wird. Wenn beispielsweise ein Windows XP/2003-Client eine Verbindung herstellt, meldet Libreswan, dass die Main-Mode-Peer-ID D_FQDN: '@example.com' lautet. Wenn sich jedoch ein Vista-, Windows 7- oder anderer RFC 3947-konformer Client verbindet, dann meldet Libreswan die Main-Mode-Peer-ID ID_IPV4_ADDR: '192.168.1.1'. Dies führt zu Problemen beim Verbinden mit dem IPsec-Server. In solchen Fällen ist das Problem gelöst, wenn die Option auf "draft-ietf-ietf-ipsec-nat-t-ike-02" eingestellt wird. Der Standardwert ist 'rfc-3947', sofern er nicht von der Standard-Verbindungseinstellung überschrieben ist. **HINWEIS** *"left/nat-traversal-negotiation" und "right/nat-traversal-negotiation" können beide auf "draft-ietf-ipsec-nat-t-ike-02" eingestellt werden.*

8. Bei Bedarf konfigurieren Sie ein Subnetz für das Verbindungsende. Weitere Informationen finden Sie unter Abschnitt 11.8.10.3, „Eine Adresse für ein privates Subnetz hinzufügen“.
9. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.8.10

Private Subnetze verwalten

Ist das Gerät mit einem internen privaten Subnetz verbunden, so kann für das Gerät der Zugang zum Subnetz am anderen Ende des IPsec-Tunnels freigegeben werden. Nur die IP-Adresse und die Maske des privaten Subnetzes sind erforderlich.

INHALT

- Abschnitt 11.8.10.1, „Private Subnetze für Verbindungsenden konfigurieren“
- Abschnitt 11.8.10.2, „Eine Adressliste für private Subnetze anzeigen“
- Abschnitt 11.8.10.3, „Eine Adresse für ein privates Subnetz hinzufügen“
- Abschnitt 11.8.10.4, „Löschen einer Adresse für ein privates Subnetz“

Abschnitt 11.8.10.1

Private Subnetze für Verbindungsenden konfigurieren

Um ein privates Subnetz für entweder die linken (lokaler Router) oder die rechten (dezentraler Router) Verbindungsenden zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***tunnel » ipsec » connection/{end} » subnet***, wobei *{end}* entweder das linke (lokaler Router) oder rechte (dezentraler Router) Verbindungsende ist.
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
{ network }	**Zusammenfassung:** Eine Zeichenkette mit 9 bis 18 Zeichen Die IP-Adresse /Präfix.

4. Fügen Sie ein oder mehrere Subnetze hinzu. Für weitere Informationen siehe Abschnitt 11.8.10.3, „Eine Adresse für ein privates Subnetz hinzufügen“.
5. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.8.10.2
Eine Adressliste für private Subnetze anzeigen

Um eine Liste von IP-Adressen für private Subnetze anzuzeigen, geben Sie Folgendes ein:

```
show running-config tunnel ipsec connection name [ right | left ] subnet
```

Erläuterung:

- *`name`* ist die Bezeichnung der Verbindung

Falls IP-Adressen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich der Folgenden angezeigt:

```
ruggedcom# show running-config tunnel ipsec connection ipsec-12 left subnet
tunnel
 ipsec
  connection ipsec-12
   left
    subnet 192.168.11.0/24
    !
   !
  !
 !
!
```

Falls keine IP-Adressen konfiguriert wurden, fügen Sie je nach Bedarf Adressen hinzu. Für weitere Informationen siehe Abschnitt 11.8.10.3, „Eine Adresse für ein privates Subnetz hinzufügen“.

Abschnitt 11.8.10.3
Eine Adresse für ein privates Subnetz hinzufügen

Um eine IP-Adresse für ein privates Subnetz hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie die IP-Adresse und das Präfix hinzu, indem Sie Folgendes eingeben:

   ```
   tunnel ipsec connection name [ right | left ] subnet address
   ```

   Erläuterung:

   - *`name`* ist die Bezeichnung der Verbindung
   - *`address`* ist die IP-Adresse und das Präfix des privaten Subnetzes
3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.8.10.4

Löschen einer Adresse für ein privates Subnetz

Um eine IP-Adresse für ein privates Subnetz zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die IP-Adresse, indem Sie Folgendes eingeben:

   ```
   no tunnel ipsec connection name [ right | left ] subnet address
   ```

   Erläuterung:

   - *name* ist die Bezeichnung der Verbindung
   - *address* ist die IP-Adresse und das Präfix des privaten Subnetzes
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.9

6in4- und 4in6-Tunnel verwalten

In Netzwerken, in denen IPv4 und IPv6 gleichzeitig vorhanden sind, können 6in4- und 4in6-Tunnel verwendet werden, um es IPv6/IPv4-Hosts zu ermöglichen, Dienste mit dem jeweils anderen Protokoll zu erreichen. Voneinander getrennte IPv6/IPv4-Hosts und -Netzwerke können diese Tunnel auch für den gegenseitigen Zugriff verwenden.

In einem 6in4-Tunnel wird der IPv6-Verkehr über konfigurierte IPv4-Links gekapselt; dies gilt umgekehrt für 4in6-Tunnel.

HINWEIS
Informationen zur Überwachung des Verkehrs über den Tunnel finden Sie in Abschnitt 7.1.2, „Statistiken für routingfähige Schnittstellen anzeigen“.

INHALT

- Abschnitt 11.9.1, „6in4- oder 4in6-Tunnel aktivieren/deaktivieren“
- Abschnitt 11.9.2, „Eine Liste der 6in4- oder 4in6-Tunnel anzeigen“
- Abschnitt 11.9.3, „Den Status von 6in4/4in6-Tunneln anzeigen“
- Abschnitt 11.9.4, „Einen 6in4- oder 4in6-Tunnel hinzufügen“
- Abschnitt 11.9.5, „Einen 6in4- oder 4in6-Tunnel löschen“

Abschnitt 11.9.1

6in4- oder 4in6-Tunnel aktivieren/deaktivieren

Um 6in4- oder 4in6-Tunnel zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Aktivieren oder deaktivieren Sie 6in4-/4in6-Tunnel, indem Sie Folgendes eingeben:

Zum Aktivieren

```
tunnel [ ip6in4 | ip4in6 ] enabled
```

Zum Deaktivieren

```
no tunnel [ ip6in4 | ip4in6 ] enabled
```

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.9.2
Eine Liste der 6in4- oder 4in6-Tunnel anzeigen

Um eine Liste der im Gerät konfigurierten 6in4- oder 4in6-Tunnel anzusehen, geben Sie Folgendes ein:

```
show running-config tunnel [ ip6in4 | ip4in6 ] tunnel
```

Eine Tabelle oder Liste ähnlich dem folgenden Beispiel wird angezeigt:

```
ruggedcom# show running-config tunnel ip6in4 tunnel | tab
NAME       ENABLED  LOCAL IP       REMOTE IP     MTU
-----------------------------------------------------
ruggedcom  true     192.168.30.14  172.23.30.14  1480

!
```

Abschnitt 11.9.3
Den Status von 6in4/4in6-Tunneln anzeigen

Um den Status eines 6in4- oder 4in6-Tunnels anzusehen, geben Sie Folgendes ein:

```
show interfaces [ ip6in4 | ip4in6 ] tunnel name
```

Erläuterung:

- *name* ist die Bezeichnung des Tunnels

Eine Tabelle oder Liste ähnlich dem folgenden Beispiel wird angezeigt:

```
ruggedcom# show interfaces ip6in4 tunnel
TUNNEL
NAME    LOCAL IP       REMOTE IP      STATUS
-----------------------------------------------
tu      192.168.20.10  192.168.20.20  Active
```

Abschnitt 11.9.4
Einen 6in4- oder 4in6-Tunnel hinzufügen

Um einen 6in4- oder 4in6-Tunnel hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den Tunnel hinzu, indem Sie Folgendes eingeben:

```
tunnel [ ip6in4 | ip4in6 ] tunnel name
```

Erläuterung:

- *name* ist die Bezeichnung des Tunnels

3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
local-ip	**Zusammenfassung:** Eine Zeichenkette mit 7 bis 15 Zeichen Die Schnittstelle, an der der Tunnel erstellt wird. Dieser Parameter ist obligatorisch.
remote-ip	**Zusammenfassung:** Eine Zeichenkette mit 7 bis 15 Zeichen IP-Adresse des entfernten Tunnelendes Dieser Parameter ist obligatorisch.
status	**Zusammenfassung:** Eine Zeichenkette Aktueller Status des Tunnels Dieser Parameter ist obligatorisch.

4. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.9.5
Einen 6in4- oder 4in6-Tunnel löschen

Um einen 6in4- oder 4in6-Tunnel zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den Tunnel durch Eingabe von:

```
no tunnel [ ip6in4 | ip4in6 ] tunnel name
```

Erläuterung:

- *name* ist die Bezeichnung des Tunnels

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.10
DMVPN verwalten

Dieser Abschnitt beschreibt, wie Sie das Gerät in einem DMVPN-Hub-and-Spoke-Netzwerk als Spoke konfigurieren können.

INHALT

- Abschnitt 11.10.1, „Beschreibung des DMVPN“
- Abschnitt 11.10.2, „Konfigurieren von DMVPN“
- Abschnitt 11.10.3, „DMVPN-Schnittstellen verwalten“

- Abschnitt 11.10.4, „Anzeigen des Status von DMVPN“

Abschnitt 11.10.1

Beschreibung des DMVPN

Das Dynamic Multipoint Virtual Private Network (DMVPN) ist eine Routing-Lösung zum Aufbau skalierbarer und sicherer VPN-Netzwerke. Damit ist es möglich, Router für mittlere bis große Unternehmen schnell bereitzustellen, ohne statische Verbindungen zwischen allen Geräten konfigurieren zu müssen.

DMPVN kann auf zwei Arten eingesetzt werden.

- Hub-and-Spoke
- Spoke-to-Spoke

RUGGEDCOM ROX II unterstützt Hub-and-Spoke-Anwendungen, bei denen ein zentraler Router (der Hub) Multipoint Generic Routing Encapsulation (mGRE) verwendet, um GRE-Tunnel mit einem oder mehreren Routern (den Spokes) aufzubauen. Wenn die Spokes einander Datenverkehr zusenden müssen, schicken sie ihn zuerst an den Hub und der Hub leitet die Datenpakete an das entsprechende Ziel weiter. Mit dieser Methode kann die komplexe Aufgabe vermieden werden, für jede mögliche Verbindung statische GRE-Tunnel zu definieren.

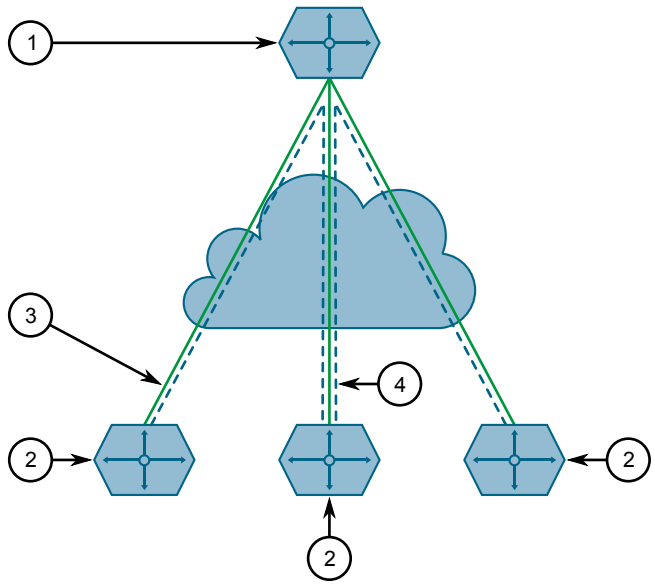


Abbildung 23: Topologie des Hub-and-Spoke – Einzelner Hub

1. Hub (statische IP-Adresse) **2.** Spoke (statische IP-Adresse) **3.** Hub-to-Spoke GRE/IPsec-Tunnel

Wenn Redundanz notwendig ist, können die Spokes auch an einen zweiten Hub angeschlossen werden.

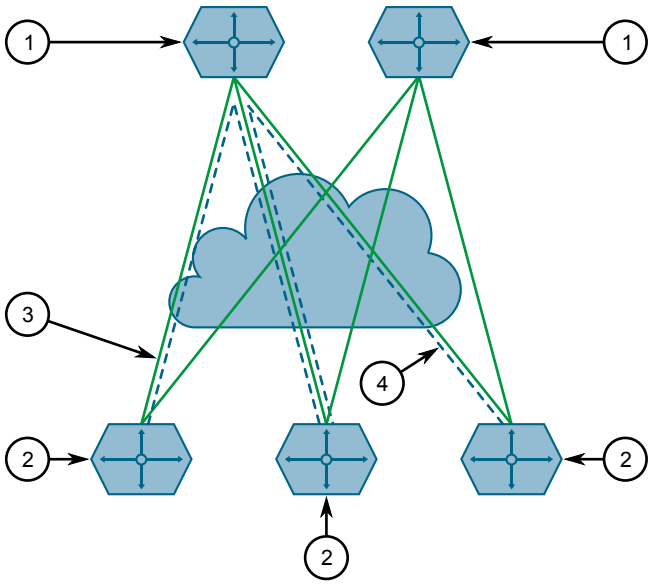


Abbildung 24: Topologie des Hub-and-Spoke – Dualer Hub

1. Hub (statische IP-Adresse) **2.** Spoke (statische IP-Adresse) **3.** Hub-to-Spoke GRE/IPsec-Tunnel

Abschnitt 11.10.2

Konfigurieren von DMVPN

Um das Gerät so zu konfigurieren, dass es in einem Hub-und-Spoke-Netzwerk als Spoke agiert, gehen Sie wie folgt vor:

HINWEIS
Der RUGGEDCOM ROX II unterstützt Verbindungen mit bis zu zwei Hubs.

1. Ermitteln Sie die statische IP-Adresse des Hub-Routers.
2. Konfigurieren Sie einen GRE-Tunnel zum Hub. Weitere Informationen finden Sie unter Abschnitt 11.7.3, „Hinzufügen eines GRE-Tunnels“.
3. Konfigurieren Sie IPSec für den GRE-Tunnel und stellen Sie sicher, dass der Verbindungsname mit dem Namen der GRE-Schnittstelle (z. B. gre-t1) übereinstimmt. Weitere Informationen finden Sie unter Abschnitt 11.8.2, „Konfigurieren von IPsec-Tunneln“.
4. Konfigurieren Sie eine BGP-Route für den GRE-Tunnel. Weitere Informationen finden Sie unter Abschnitt 12.8.1, „Konfigurieren von BGP“.
5. Aktivieren Sie den DMVPN-Dienst, indem Sie Folgendes eingeben:

```
services nhrp enabled
```

HINWEIS
Der RUGGEDCOM ROX II unterstützt bis zu zwei DMVPN-Schnittstellen, wobei jede einem anderen GRE-Tunnel zugewiesen werden kann.

6. Konfigurieren Sie für jeden GRE-Tunnel eine DMVPN-Schnittstelle. Weitere Informationen finden Sie unter Abschnitt 11.10.3.2, „Eine DMVPN-Schnittstelle hinzufügen“.
7. Konfigurieren Sie einen IPsec/GRE-Tunnel vom Hub zum Gerät und verwenden Sie dafür die IP-Adresse, die für die DMVPN-Schnittstelle des Geräts festgelegt wurde.
8. Verifizieren Sie den Status der DMVPN-Verbindung. Weitere Informationen finden Sie unter Abschnitt 11.10.4, „Anzeigen des Status von DMVPN“.

Abschnitt 11.10.3

DMVPN-Schnittstellen verwalten

Sie können eine DMVPN-Schnittstelle für die Verbindung mit einem Host konfigurieren. Bis zu zwei Schnittstellen können konfiguriert werden, durch die das Gerät eine Verbindung mit zwei Hubs herstellen kann.

INHALT

- Abschnitt 11.10.3.1, „Eine Liste der DMVPN-Schnittstellen anzeigen“
- Abschnitt 11.10.3.2, „Eine DMVPN-Schnittstelle hinzufügen“
- Abschnitt 11.10.3.3, „Eine DMVPN-Schnittstelle löschen“

Abschnitt 11.10.3.1

Eine Liste der DMVPN-Schnittstellen anzeigen

Um eine Liste der DMVPN-Schnittstellen anzusehen, geben Sie Folgendes ein:

```
show running-config services nrhp interface-nhrp
```

Falls Schnittstellen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config services nrhp interface-nhrp | tab
IFNAME   ENABLED  ADDRESS           HOLDTIME  AUTHENTICATION  KEY
-------------------------------------------------------------------------------------
gre-t1   true     192.168.0.100/24  10        cisco           $4$wocla9w68FRwhYYI0d4IDw==

 !
!
```

Falls keine Schnittstellen konfiguriert wurden, fügen Sie je nach Bedarf Schnittstellen hinzu. Weitere Informationen finden Sie unter Abschnitt 11.10.3.2, „Eine DMVPN-Schnittstelle hinzufügen“.

Abschnitt 11.10.3.2

Eine DMVPN-Schnittstelle hinzufügen

Um eine DMVPN-Schnittstelle hinzuzufügen, gehen Sie wie folgt vor:

1. Fügen Sie die Schnittstelle für den gewünschten GRE-Tunnel hinzu, indem Sie Folgendes eingeben:

   ```
   services nhrp interface-nhrp gre-tunnel
   ```

   Erläuterung: *gre-tunnel* ist die Bezeichnung des gewünschten GRE-Tunnels.
2. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

ACHTUNG!
Sicherheitsgefahr – Risiko eines unberechtigten Zugriffs und/oder einer unberechtigten Nutzung Für eine erhöhte Sicherheit empfiehlt Siemens, einen Code zu konfigurieren, um die NHRP-Schnittstelle zu authentifizieren.

Parameter	Beschreibung
enabled	Eine Boolesche Flag, die anzeigt, dass an dieser Schnittstelle das Next Hop Resolution Protocol (NHRP) aktiviert ist.
address { address }	**Zusammenfassung:** Eine Zeichenkette mit 9 bis 18 Zeichen IPv4-Adresse der entfernten GRE-Schnittstelle, die für diese NHRP-Sitzung zu verwenden ist.
holdtime { holdtime }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl **Standard:** 7200 Die Zeit (in Sekunden), in der Non-Broadcast Multi-Access (NBMA)-Adressen in autoritativen NHRP-Antworten als gültig angekündigt werden. Der Standardwert ist 7200 Sekunden.
authentication { authentication }	**Zusammenfassung:** { none, cisco } Die Authentifizierungszeichenkette, die eine Interkommunikation zwischen NHRP-Quell- und -Zielknoten zulässt. Maximale Länge beträgt 8 Zeichen. Derzeit wird nur CISCO-Authentifizierung unterstützt.
key { key }	**Zusammenfassung:** Eine Zeichenkette Der Authentifizierungsschlüssel, der eine Interkommunikation zwischen NHRP-Quell- und -Zielknoten zulässt. Maximale Länge beträgt 8 Zeichen.

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.10.3.3
Eine DMVPN-Schnittstelle löschen

Um eine DMVPN-Schnittstelle zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den Adressen-Pool durch Eingabe von:

```
no services nhrp interface-nhrp gre-tunnel
```

   Erläuterung *`gre-tunnel`* ist der Name des gewünschten GRE-Tunnels.

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 11.10.4
Anzeigen des Status von DMVPN

Um den Status eines DMVPN-Diensts anzuzeigen, geben Sie Folgendes ein:

```
show services nhrp status
```

Falls DMVPN-Schnittstellen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show services nhrp status
ROW  RAW FROM OPENNHRPCTL
-----------------------------------------
0
1    Status: ok
2
3    Interface: gre-t1
4    Type: local
5    Protocol-Address: 172.30.168.2/32
6    Flags: up
7
8    Status: ok
9
10   Interface: gre-t1
11   Type: static
12   Protocol-Address: 192.168.0.100/24
13   NBMA-Address: 172.19.20.21
14
```

Die bereitgestellten Informationen werden direkt vom NHRP bezogen. Im Folgenden sehen Sie einige der Felder, die angezeigt werden können:

HINWEIS
Bestimmte Felder werden nur angezeigt, sofern zutreffend.

Feld	Beispiel	Beschreibung
Status	Status: ok	Der Status der Schnittstelle.
Interface	Interface: gre-t1	Die Bezeichnung der Schnittstelle.
Type	Type: local	Der NHRP-Peer-Typ. Mögliche Werte: • `shortcut-route` – Empfangene oder weitergegebene Auflösung für die Route • `incomplete` – Auflösungsanfrage gesendet, jedoch noch keine Antwort empfangen • `negative` – Negativ im Cache gepuffert • `cached` – Empfangene oder weitergegebene Auflösung • `dynamic` – NHC-Registrierung • `dynamic-nhs` – Dynamic NHS von der DNS-Abbildung • `static` – Statische Abbildung von der Konfigurationsdatei • `static-dns` – Statische DNS-Abbildung von der Konfigurationsdatei • `local-route` – Nicht-lokales Ziel, mit lokaler Route • `local` – Lokales Ziel, IP oder Off-NBMA-Subnetz
Protocol-Address	Protocol-Address: 172.30.168.2/32	Die IP-Adresse der Schnittstelle.
Flags	Flags: up	Der bzw. die Merker, der bzw. die dem Paket der letzten NHRP-Registrierungsanfrage zugeordnet wurden. Mögliche Werte: • `unique` – Der NHRP-Peer ist eindeutig. Sein NRHP-Abbildungseintrag kann durch einen Abbildungseintrag mit derselben IP-Adresse auch dann nicht überschrieben werden, wenn der zugeordnete Peer eine verschiedene NBMA-Adresse besitzt.

Feld	Beispiel	Beschreibung
		• `used` – Der NHRP-Peer befindet sich in der ARP-Tabelle des Kernels. • `up` – Eine Verbindung zum NHRP-Peer wurde hergestellt und die Verbindung ist aktiv. • `lower-up` – Eine Verbindung zum NHRP-Peer wurde hergestellt.
NBMA-Address	NBMA-Address: 172.19.20.21	Die NBMA-Adresse der Schnittstelle.
NBMA-NAT_OA-Address	NBMA-NAT_OA-Address: 172.16.0.0/12	Die externe IP-Adresse und Maske der Schnittstelle. Wird nur angezeigt, wenn sich der Hub hinter einem NAT-fähigen Router befindet.
Expires-in	Expires-in: 120	Die Zeit in Sekunden, bevor die NBMA-Informationen des Responders als ungültig betrachtet und verworfen werden. Wird nur angezeigt, wenn die *`holdtime`* konfiguriert ist.
Hostname	Hostname: ruggedcom	Der Hostname des NBMA-Responders, sofern verfügbar.

12 Unicast- und Multicast-Routing

Dieses Kapitel beschreibt, wie Sie Unicast- und Multicast-Verkehr über statische und dynamische Routen konfigurieren, überwachen und verwalten können.

INHALT

- Abschnitt 12.1, „Den Status der IPv4-Routen anzeigen“
- Abschnitt 12.2, „Den Status von IPv6-Routen anzeigen“
- Abschnitt 12.3, „Speicherstatistik anzeigen“
- Abschnitt 12.4, „Konfigurieren von ICMP“
- Abschnitt 12.5, „Event-Tracker verwalten“
- Abschnitt 12.6, „IS-IS verwalten“
- Abschnitt 12.7, „Verwalten des RIP“
- Abschnitt 12.8, „BGP verwalten“
- Abschnitt 12.9, „Verwalten von OSPF“
- Abschnitt 12.10, „MPLS verwalten“
- Abschnitt 12.11, „Verwalten von VRF (Virtual Routing and Forwarding)“
- Abschnitt 12.12, „Statische Routen verwalten“
- Abschnitt 12.13, „Statisches Multicast-Routing verwalten“
- Abschnitt 12.14, „Verwalten des dynamischen Multicast-Routing“

Abschnitt 12.1

Den Status der IPv4-Routen anzeigen

Um den Status der auf dem Gerät konfigurierten IPv4-Routen anzuzeigen, geben Sie Folgendes ein:

HINWEIS
Es ist möglich, eine Route auf einem lokal angebundenen Broadcast-Netzwerk (d. h. ohne Gateway) zu erstellen, ohne dass dabei eine zugehörige IP-Adresse an dieser Schnittstelle vorhanden ist. Beispielsweise wäre es möglich, 192.168.1.0/24 zu switch.0001 hinzuzufügen, der eine IP-Adresse von 10.0.1.1, aber keine zugehörige Alias-Adresse auf dem Subnetz 192.168.1.0/24 hat.

```
show routing status ipv4routes
```

Sofern IPv4-Routen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich der Folgenden angezeigt:

```
ruggedcom# show routing status ipv4routes
DESTINATION     GATEWAY  INTERFACE    TYPE    WEIGHT  METRIC
-----------------------------------------------------------------
```

```
192.168.0.0/24           switch.0001  kernel
```

Diese Tabelle/Liste liefert die folgenden Informationen:

Parameter	Beschreibung
destination	**Zusammenfassung:** Eine Zeichenkette Das Netzwerk/Präfix.
gateway	**Zusammenfassung:** Eine Zeichenkette Die Gateway-Adresse.
interface	**Zusammenfassung:** Eine Zeichenkette Der Schnittstellenname.
type	**Zusammenfassung:** Eine Zeichenkette Der Routentyp.
weight	**Zusammenfassung:** Eine Zeichenkette Das Routengewicht.
metric	**Zusammenfassung:** Eine Zeichenkette Der metrische Wert der Route.

Falls keine IPv4-Routen konfiguriert wurden, fügen Sie nach Bedarf Routen hinzu. Für weitere Informationen siehe Abschnitt 7.1.3.2, „Eine IPv4-Adresse hinzufügen“.

Abschnitt 12.2

Den Status von IPv6-Routen anzeigen

Um den Status der auf dem Gerät konfigurierten IPv6-Routen anzuzeigen, geben Sie Folgendes ein:

```
show routing status ipv6routes
```

Sofern IPv6-Routen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich der Folgenden angezeigt:

```
ruggedcom# show routing status ipv6routes
DESTINATION  GATEWAY  INTERFACE    TYPE    WEIGHT  METRIC
-------------------------------------------------------------
fe80:/64             switch       kernel          256
fe80:/64             dp1          kernel          256
fe80:/64             vrf_lo       kernel          256
fe80:/64             switch.0001  kernel          256
fe80:/64             fe-cm-1      kernel          256
fe80:/64             switch.4094  kernel          256
ff00:/8              switch                       256
ff00:/8              dp1                          256
ff00:/8              vrf_lo                       256
ff00:/8              switch.0001                  256
ff00:/8              fe-cm-1                      256
ff00:/8              switch.4094                  256
```

Diese Tabelle/Liste liefert die folgenden Informationen:

Parameter	Beschreibung
destination	**Zusammenfassung:** Eine Zeichenkette Das Netzwerk/Präfix.
gateway	**Zusammenfassung:** Eine Zeichenkette

Parameter	Beschreibung
	Die Gateway-Adresse.
interface	**Zusammenfassung:** Eine Zeichenkette Der Schnittstellenname.
type	**Zusammenfassung:** Eine Zeichenkette Der Routentyp.
weight	**Zusammenfassung:** Eine Zeichenkette Das Routengewicht.
metric	**Zusammenfassung:** Eine Zeichenkette Der metrische Wert.

Falls keine IPv6-Routen konfiguriert wurden, fügen Sie nach Bedarf Routen hinzu. Weitere Informationen finden Sie unter Abschnitt 12.12.3, „Eine statische IPv6-Route hinzufügen“.

Abschnitt 12.3

Speicherstatistik anzeigen

Um Statistiken zu den Core-, RIP-, OSPF- und BGP-Daemons aufzurufen, geben Sie Folgendes ein:

```
show routing status memory
```

Eine Liste ähnlich dem folgenden Beispiel wird angezeigt:

```
ruggedcom# show routing status memory
routing status memory
 zebra
  total 405504
  used  359424
  free  46080
 rip
  total 0
  used  0
  free  0
 ospf
  total 0
  used  0
  free  0
 bgp
  total 0
  used  0
  free  0
```

Diese Liste liefert die folgenden Informationen:

Parameter	Beschreibung
total	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Der gesamte zugewiesene Heap (in Bytes). Dieser Parameter ist obligatorisch.
used	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl der verwendeten gewöhnlichen Blöcke (in Bytes). Dieser Parameter ist obligatorisch.
free	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl

Parameter	Beschreibung
	Die Anzahl der freien gewöhnlichen Blöcke (in Bytes). Dieser Parameter ist obligatorisch.

Abschnitt 12.4

Konfigurieren von ICMP

Um zu konfigurieren wie der RUGGEDCOM ROX IIICMP-Redirect-Nachrichten handhabt, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***admin*** und konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

HINWEIS
ICMP-Redirect-Nachrichten werden von Routern an Hosts gesendet, um diese darüber zu informieren, wann eine bessere Route für ein bestimmtes Ziel verfügbar ist. Beachten Sie, bevor Sie das Senden von ICMP-Nachrichten im RUGGEDCOM ROX II aktivieren, dass ICMP-Umleitungen einfach zu manipulieren sind, sodass Angreifer die Kontrolle über den Pfad, über den die Pakete weitergeleitet werden, übernehmen können, und diese daher unter Umständen als Sicherheitsrisiko betrachtet werden. Senden Sie ICMP-Redirect-Nachrichten nur, wenn dies angemessen ist.

Parameter	Beschreibung
ignore-icmp-all	**Zusammenfassung:** { true, false } **Standard:** false Ignoriert alle an ihn gesendeten ICMP-Echo-Anfragen.
ignore-icmp-broadcast	**Zusammenfassung:** { true, false } **Standard:** true Ignoriert alle per Broadcast/Multicast an ihn gesendeten ICMP-Echo- und Zeitstempel-Anfragen.
tcp-syn-cookies	**Zusammenfassung:** { true, false } **Standard:** false Sendet Syncookies, wenn die „syn backlog"-Warteschlange eines Sockels überläuft. Dies schützt vor den üblichen "SYN Flood-Angriffen".
send-icmp-redirect	**Zusammenfassung:** { true, false } **Standard:** true Sendet die ICMP-Weiterleitung.
tcp-est-conn-track-timeout { tcp-est-conn-track-timeout }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 300 und 432000 **Standard:** 432000 Legt das Timeout für die von TCP aufgebaute Verbindungsspur in Sekunden fest. Niedrigere Timeout-Werte verhindern, dass tote TCP-Verbindungen fortbestehen. Eine TCP-Verbindung gilt dann als tot, wenn ein Peer unerwartet getrennt wird.

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.5

Event-Tracker verwalten

Tracker überwachen die Verfügbarkeit von Hosts oder Geräten durch regelmäßige Übertragung von ICMP-Meldungen (oder Pings). Je nach ICMP-Ergebnis aktualisiert der Tracker die Betriebsdaten mit dem Status des Hosts oder des Geräts, wenn dieser sich verändert (d. h. von "up" zu "down" und umgekehrt). Andere Teile des Systems können sich dann anmelden, um bei Veränderungen der Betriebsdaten benachrichtigt zu werden.

Ein Tracker kann einem Benutzer mehr Flexibilität beim Konfigurieren eines Merkmals ermöglichen. So können beispielsweise angekündigte oder empfangene Routen je nach Status des Trackers gefiltert oder vollständig blockiert werden.

HINWEIS
Tracker nutzen nur ICMP-Meldungen zum Pingen eines IP-Zielgeräts. Sie können daher nur die Verfügbarkeit für IP-Geräte und diese nur bis zur IP-Schicht sicherstellen.

INHALT

- Abschnitt 12.5.1, „Eine Liste der Event-Tracker anzeigen“
- Abschnitt 12.5.2, „Statistiken für Event-Tracker anzeigen“
- Abschnitt 12.5.3, „Einen Event Tracker hinzufügen“
- Abschnitt 12.5.4, „Einen Event-Tracker löschen“

Abschnitt 12.5.1

Eine Liste der Event-Tracker anzeigen

Um eine Liste der Event-Tracker anzusehen, geben Sie Folgendes ein:

```
show running-config global tracking
```

Falls Event-Tracker konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config global tracking
global
 tracking
  event host-in-lan-11
   target   192.168.11.100
   timeout  500
   interval 500
   fall     3
   rise     3
  !
 !
!
```

Falls keine Event-Tracker konfiguriert wurden, fügen Sie je nach Bedarf Tracker hinzu. Weitere Informationen finden Sie unter Abschnitt 12.5.3, „Einen Event Tracker hinzufügen“.

Abschnitt 12.5.2
Statistiken für Event-Tracker anzeigen

RUGGEDCOM ROX II erfasst Statistiken für jeden Event-Tracker.

Um die Statistiken für einen Event-Tracker anzusehen, geben Sie Folgendes ein:

```
show global tracking event statistics
```

Eine Liste ähnlich dem folgenden Beispiel wird angezeigt:

```
ruggedcom# show global tracking event statistics
                                                          STANDARD
                 ECHO      ECHO     MIN  AVERAGE  MAX   DEVIATION
NAME             ATTEMPTS  REPLIES  RTT  RTT      RTT   RTT
-------------------------------------------------------------------
host-in-lan-11   0         0        0.0  0.0      0.0   0.0
```

Die Liste liefert die folgenden Informationen:

Parameter	Beschreibung
echo-attempts	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl der Echoversuche.
echo-replies	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl der Echo-Erwiderungen.
min-rtt	**Zusammenfassung:** Eine Zeichenkette Das Minimum der Hin- und Rücklaufzeit (in Millisekunden)
average-rtt	**Zusammenfassung:** Eine Zeichenkette Der Durchschnitt der Hin- und Rücklaufzeit (in Millisekunden)
max-rtt	**Zusammenfassung:** Eine Zeichenkette Das Maximum der Hin- und Rücklaufzeit (in Millisekunden)
standard-deviation-rtt	**Zusammenfassung:** Eine Zeichenkette Die Standardabweichung der Hin- und Rücklaufzeit (in Millisekunden)

Abschnitt 12.5.3
Einen Event Tracker hinzufügen

Um einen Event Tracker hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den Event Tracker hinzu, indem Sie Folgendes eingeben:

   ```
   global tracking event name
   ```

   - *name* ist die Bezeichnung des verfolgten Ereignisses
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
target { target }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 253 Zeichen Konfiguriert das Ping-Ziel als IPv4-Adresse oder „hostname.domain".

Parameter	Beschreibung
	Dieser Parameter ist obligatorisch.
source-ip { source-ip }	**Zusammenfassung:** Eine Zeichenkette mit 7 bis 15 Zeichen oder eine Zeichenkette mit 6 bis 40 Zeichen Legt die Quelladresse auf eine bestimmte IPv4-Adresse fest.
source-interface { source-interface }	**Zusammenfassung:** Eine Zeichenkette Erzwingt einen Ping an einer ausgewählten Schnittstelle.
timeout { timeout }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Bestimmt, wie viele Millisekunden auf die ICMP-Reaktion zu warten ist. Dieser Parameter ist obligatorisch.
interval { interval }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl von 100 oder höher Bestimmt, wie viele Millisekunden vor dem Senden einer weiteren ICMP-Anforderung zu warten ist. Dieser Parameter ist obligatorisch.
fall { fall }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl von 1 oder höher Die Häufigkeit, in der ein Ausfall auftritt, bevor der Tracking-Zustand von verfügbar ("up") zu nicht verfügbar ("down") wechselt. Dieser Parameter ist obligatorisch.
rise { rise }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl von 1 oder höher Die Häufigkeit, in der ein Erfolg auftritt, bevor der Tracking-Zustand von nicht verfügbar ("down") zu verfügbar ("up") wechselt.
state	**Zusammenfassung:** { up, down } **Standard:** up Der Zustand des Ereignisses.

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.5.4
Einen Event-Tracker löschen

Um einen Event-Tracker zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den Event-Tracker durch Eingabe von:

```
no global tracking event name
```

   - *`name`* ist die Bezeichnung des verfolgten Ereignisses
3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.6

IS-IS verwalten

Intermediate System - Intermediate System (IS-IS) ist eine Suite von Routing-Protokollen, die Routing-Informationen zwischen Routern teilen. Aufgabe des Routers ist es, die effiziente Datenbewegung in manchmal komplexen Netzwerken zu ermöglichen. Routing-Protokolle sollen Routing-Informationen in diesen Netzwerken verteilen und mit Hilfe fortschrittlicher Algorithmen den kürzesten Weg der Information von Punkt A zu Punkt B ermitteln. Eines der ersten Link-State-Routing-Protokolle war das 1986 entwickelte IS-IS, das 1987 von ISO als ISO/IEC 10589 veröffentlicht wurde. Später wurde es erneut als IETF-Standard (RFC 1142 [http://tools.ietf.org/html/rfc1142]) veröffentlicht.

INHALT

- Abschnitt 12.6.1, „IS-IS-Konzepte“
- Abschnitt 12.6.2, „Konfigurieren von IS-IS“
- Abschnitt 12.6.3, „Anzeigen des Status von Nachbarn“
- Abschnitt 12.6.4, „Anzeigen des Status einer Link-State-Datenbank“
- Abschnitt 12.6.5, „Bereichsvariablen verwalten“
- Abschnitt 12.6.6, „Schnittstellen verwalten“
- Abschnitt 12.6.7, „LSP-Generierung verwalten“
- Abschnitt 12.6.8, „SPF-Berechnungen verwalten“
- Abschnitt 12.6.9, „Die Lebensdauer von LSPs verwalten“
- Abschnitt 12.6.10, „LSP-Auffrischungsintervalle verwalten“
- Abschnitt 12.6.11, „Verwalten von Network Entity Titles (NETs)“
- Abschnitt 12.6.12, „Umverteilungsmetriken verwalten“

Abschnitt 12.6.1

IS-IS-Konzepte

IS-IS ist ein Interior Gateway Protocol (IGP), das zum Austausch von Informationen innerhalb von autonomen Systemen (AS) vorgesehen ist. Es wurde entwickelt, um innerhalb einer administrativen Domain oder eines Netzwerks anhand von Link-State-Informationen das optimale Datenpaket-Routing zu bestimmen, ähnlich wie bei OSPF. IS-IS füllt das Netzwerk mit Link-State-Informationen und erstellt eine Datenbank der Netzwerktopologie. Das Protokoll berechnet den besten Pfad durch das Netzwerk (mit dem Dijkstra-Algorithmus) und leitet die Pakete dann an ihr Ziel weiter.

Obwohl es ursprünglich als ISO Connectionless-mode Network Protocol (CLNP) konzipiert war, wurde es später in RFC 1195 [http://tools.ietf.org/html/rfc1195] für den Einsatz in IP-Netzwerken (Dual IS-IS) adaptiert. IS-IS wird vor allem in ISP-Umgebungen eingesetzt und eignet sich im Gegensatz zu zentralen Kernnetzen besser für *fadenförmige* Netzwerke.

HINWEIS
In komplexen vorhandenen Netzwerken können RIP, OSPF, BGP und IS-IS gleichzeitig auf demselben Router aktiv sein. In der Regel wird jedoch nur ein dynamisches Routingprotokoll zur Zeit verwendet.

INHALT

- Abschnitt 12.6.1.1, „IS-IS-Router“
- Abschnitt 12.6.1.2, „NET-(Network Entity Title)-Adressen“
- Abschnitt 12.6.1.3, „Vor- und Nachteile der Verwendung von IS-IS“

Abschnitt 12.6.1.1

IS-IS-Router

IS-IS-Router können als Level-1, Level-2 oder beides definiert werden. Level-1-Router bilden den Bereich, während Level-2-Router das Backbone des Netzwerks bilden. Standardmäßig konfiguriert RUGGEDCOM ROX II Bereiche derart, dass sie beides sind (oder Level-1-2). Dadurch kann das Gerät zwischen verschiedenen Bereichen mit minimaler Konfiguration interagieren.

- **Level-1**-Router sind Intra-Area-Router. Sie unterhalten eine einzige Link-State-Datenbank (LSD), die nur Informationen über die Level-1- und Level-2 Nachbarn in ihrem Bereich enthält. Um mit Routern in einem anderen Bereich zu kommunizieren, leiten Level-1-Router den Verkehr über ihren nächstgelegenen Level-2-Router weiter.
- **Level-2**-Router sind Inter-Area-Router, d. h. sie können mit Routern in anderen Bereichen kommunizieren. Sie unterhalten auch eine einzige LSD, aber diese enthält nur Informationen über andere Level-2-Router aus dem Bereich des Routers oder aus anderen Bereichen. Der Router hat keine Kenntnisse über die Level-1-Router in seinem Bereich.
- **Level-1-2**-Router sind sowohl Inter- als auch Intra-Area-Router, d. h. sie können mit Level-1- und Level-2-Routern in jedem Bereich kommunizieren. Sie unterhalten separate LSD für Level-1- und Level-2-Router innerhalb und außerhalb des Bereichs des Routers.

Abschnitt 12.6.1.2

NET-(Network Entity Title)-Adressen

IS-IS-Router werden mit ihrer NET-(Network Entity Title)-Adresse identifiziert, die das NSAP-(Network Service Access Point)-Format hat (RFC 1237 [http://tools.ietf.org/html/rfc1237]). NSAP-Adressen haben 8 bis 20 Oktette und bestehen aus dem Authority and Format Identifier (1 Byte), der Area ID (0 bis 12 Byte), der System ID (6 Byte) und dem Selector (1 Byte).

Nachstehend ein Beispiel für eine NSAP-Adresse:

```
NSAP address: 49.0001.1921.6800.1001.00

AFI: 49 (typical for IS-IS NET addresses)
Area ID: 0001 (typically 4 bytes)
System ID: 1921.6800.1001 (equates to the IP address 192.168.1.1)
Selector: 00 (NET addresses always have a selector of 00)
```

Abschnitt 12.6.1.3

Vor- und Nachteile der Verwendung von IS-IS

Die Verwendung von IS-IS hat die folgenden Vor- und Nachteile:

Vorteile

- läuft nativ in der OSI-Netzwerkschicht
- kann dank Unabhängigkeit von der IP-Adressierung sowohl IPv4- als auch IPv6-Netzwerke unterstützen
- das IS-IS-Bereichskonzept ist einfacher zu verstehen und umzusetzen
- IS-IS-Updates werden gesammelt als ein LSP gesendet, anstelle mehrerer kleiner LSAs wie bei OSPF
- bessere Skalierbarkeit als OSPF durch einen schlankeren Daemon mit geringerer Auslastung
- wird bei Dienstanbietern immer beliebter
- kann in MPLS integriert werden
- schützt dank der Nutzung der Sicherungsschicht vor *Spoofing*- und Denial- of-Service-(DoS)-Angriffen

Nachteile

- wird vorwiegend von Dienstanbietern genutzt
- begrenzter Support von Netzwerk-Stack-Anbietern und Geräteherstellern
- CLNP-Adressierung kann für viele Benutzer neu und verwirrend sein

Abschnitt 12.6.2

Konfigurieren von IS-IS

Um das dynamische Routing mit IS-IS zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Aktivieren Sie IS-IS, indem Sie Folgendes eingeben:

   ```
   routing isis enabled
   ```

3. Weisen Sie das Gerät einem oder mehreren Bereichen im IS-IS-Netzwerk zu, indem Sie Bereichsvariablen definieren. Weitere Informationen finden Sie unter Abschnitt 12.6.5, „Bereichsvariablen verwalten“.
4. Konfigurieren Sie eine oder mehrere Schnittstellen, an denen das IS-IS-Routing ausgeführt werden soll. Weitere Informationen finden Sie unter Abschnitt 12.6.6, „Schnittstellen verwalten“.
5. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

» Beispiel

Im Folgenden wird dargestellt, wie ein IS-IS-Netzwerk mit allen Schaltkreisarten zu konfigurieren ist. In diesem Beispiel ist R1 ein Level-1-Router, der den Verkehr an Level-2-Router weiterleiten muss. R2 und R3 werden als Level-1-2-Router konfiguriert, um die Verbindung zu den Routern R4 und R5 zu vereinfachen, die reine Level-2-Router sind. Jeder Router ist so konfiguriert, dass er eine nicht-passive Schnittstelle besitzt, die Punkt-zu-Punkt-Netzwerkkommunikation nutzt und sich im selben Bereich befindet.

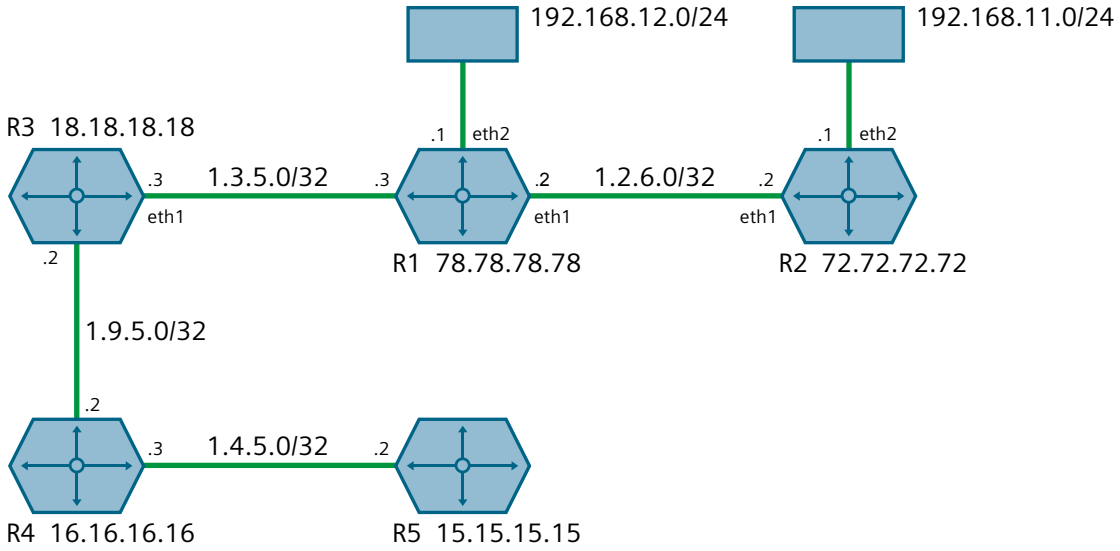


Abbildung 25: Multilevel-IS-IS-Konfiguration

Abschnitt 12.6.3

Anzeigen des Status von Nachbarn

Um den Status von benachbarten Geräten in einem IS-IS-Netzwerk anzuzeigen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass das IS-IS-Netzwerk konfiguriert ist. Weitere Informationen finden Sie unter Abschnitt 12.6.2, „Konfigurieren von IS-IS“.
2. Zeigen Sie den Status an, indem Sie Folgendes eingeben:

```
routing status isis isis-neighbors-status
```

Sofern IS-IS-Routen konfiguriert wurden, wird eine Tabelle ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# routing status isis isis-neighbors-status
isis-neighbors-status
Area area1:

  System Id           Interface   L  State        Holdtime SNPA

  Spirent-            switch.0012 3  Up           24       2020.2020.2020
```

Diese Tabelle zeigt die folgenden Informationen:

Parameter	Beschreibung
System ID	Die System-ID.
Interface	Die Bezeichnung der Schnittstelle.
L	Die Ebene. Folgende Ebenen sind möglich: `1`, `2` und `3`wobei `3` für Ebene 1 und 2 steht.
State	Adjazenzstatus.
Holdtime	Die verbleibende Haltezeit in Sekunden.

Parameter	Beschreibung
SNPA	Die MAC-Adresse des Anschlusspunkts des Subnetzwerks (SNPA).

Abschnitt 12.6.4

Anzeigen des Status einer Link-State-Datenbank

Um den Basic-Status der Link-State-Datenbank in einem IS-IS-Netzwerk anzuzeigen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass das IS-IS-Netzwerk konfiguriert ist. Weitere Informationen finden Sie unter Abschnitt 12.6.2, „Konfigurieren von IS-IS“.
2. Zeigen Sie den Basic-Status an, indem Sie Folgendes eingeben:

```
routing status isis isis-database-status
```

Oder zeigen Sie einen detaillierteren Status an, indem Sie Folgendes eingeben:

```
routing status isis isis-database-detail-status
```

Sofern IS-IS-Routen konfiguriert wurden, wird eine Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# routing status isis isis-database-status
isis-database-status
Area area1:

IS-IS Level-1 link-state database:

LSP ID                  PduLen  SeqNumber   Chksum  Holdtime  ATT/P/OL

R1.00-00             *     75   0x00000015  0xe43a    1129    0/0/0

    1 LSPs


IS-IS Level-2 link-state database:

LSP ID                  PduLen  SeqNumber   Chksum  Holdtime  ATT/P/OL

Spirent-.00-00            121   0x0000000f  0xd5e6     871    0/0/0

R1.00-00             *     75   0x00000015  0xe636    1031    0/0/0

Spirent-right.00-00      1465   0x0000000f  0x3d65     871    0/0/0

Spirent-right.00-01       295   0x0000000f  0x6a0d     872    0/0/0

Spirent-right.00-00      1465   0x0000000f  0x4638     872    0/0/0

Spirent-right.00-01       287   0x0000000f  0x54d0     872    0/0/0

Spirent-right.00-00      1462   0x0000000f  0x6528     872    0/0/0

Spirent-right.00-01       269   0x0000000f  0x7e8a     872    0/0/0

Spirent-right.00-00      1463   0x0000000f  0x99a0     872    0/0/0

Spirent-right.00-01       261   0x0000000f  0xb0d2     872    0/0/0

Spirent-right.00-00      1460   0x0000000f  0x80c6     872    0/0/0
```

```
Spirent-right.00-01       253   0x0000000f  0x97fb     872    0/0/0

Spirent-right.00-00      1460   0x0000000f  0x1137     872    0/0/0

Spirent-right.00-01       237   0x0000000f  0x0db7     872    0/0/0

    14 LSPs
```

Diese Liste zeigt die folgenden Informationen:

Parameter	Beschreibung
LSP-ID	Kennung der Link-State-PDU.
Pdulength	Größe des PDU-Pakets.
SeqNumber	Sequenznummer der Link-State-PDU.
ChkSum	Prüfsummenwert der Link-State-PDU.
Holdtime	Alter der Link-State-PDU in Sekunden.
ATT	"Attach"-Bit, gibt an, ob der Router einem anderen Bereich zugeordnet ist.
P	"Partition"-Bit ist nur gesetzt, wenn LSP die Partitionsreparatur unterstützt.
OL	"Overload" ist nur gesetzt, wenn die LSP-Datenbank des Erstellers überlastet ist.

Abschnitt 12.6.5

Bereichsvariablen verwalten

Ein IS-IS-Bereich ist eine Gruppierung miteinander verschalteter (oder benachbarter) konfigurierter IS-IS-Router. Im Gegensatz zu OSPF, wo ein Area Border Router (ABR) in zwei Bereichen gleichzeitig vorhanden sein kann, sind IS-IS-Router nur einem Bereich zugeordnet. Die Verbindung zwischen Routern in zwei verschiedenen Bereichen bildet die Grenze. Der Grund dafür ist, dass ein IS-IS-Router nur eine NSAP-(Network Service Access Point)-Adresse besitzt.

Ein Router kann als Level-1-, Level-2- oder Level-1-2-Router in einem oder mehreren Bereichen konfiguriert werden.

Router sind Bereichen durch Bereichsvariablen zugeordnet, die den Routing-Typ, die Routing-Metrik und die Authentifizierungs-/Autorisierungsregeln festlegen.

INHALT

- Abschnitt 12.6.5.1, „Eine Liste der Bereichsvariablen anzeigen“
- Abschnitt 12.6.5.2, „Hinzufügen einer Bereichsvariablen“
- Abschnitt 12.6.5.3, „Eine Bereichsvariable löschen“

Abschnitt 12.6.5.1

Eine Liste der Bereichsvariablen anzeigen

Um eine Liste der für dynamische IS-IS-Routen konfigurierten Bereichsvariablen anzuzeigen, geben Sie Folgendes ein:

```
show running-config routing isis area
```

Falls Bereichsvariablen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich der Folgenden angezeigt:

```
ruggedcom# show running-config routing isis area
routing isis
 area Area_1
  is-type               level-1-2
  metric-style          narrow
  area-authorization    md5
  area-password         admin
  area-authentication   validate
  domain-authorization  md5
  domain-password       admin
  domain-authentication validate
  net 49.0001.1921.6800.1001.00
  !
  redistribute bgp
   is-type     level-1-2
   metric-type internal
   metric      10
  !
  lsp-gen-interval is-type level-1-only
   interval 60
  !
  lsp-refresh-interval is-type level-1-2
   interval 20
  !
  max-lsp-lifetime is-type level-2-only
   interval 10
  !
  spf-interval is-type level-1-2
   interval 5
  !
 !
!
```

Falls keine Bereichsvariablen konfiguriert wurden, fügen Sie Bereichsvariablen je nach Bedarf hinzu. Weitere Informationen finden Sie unter Abschnitt 12.6.5.2, „Hinzufügen einer Bereichsvariablen“.

Abschnitt 12.6.5.2

Hinzufügen einer Bereichsvariablen

Um eine Bereichsvariable für dynamische IS-IS-Routen hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den Bereich hinzu, indem Sie Folgendes eingeben:

   ```
   routing isis area name
   ```

   Erläuterung:

   - *name* ist die eindeutige Bezeichnung für einen Routingprozess, der zu einem bestimmten Router gehört.
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
is-type { is-type }	**Zusammenfassung:** { level-1-only, level-2-only, level-1-2 } Der IS-Typ für diesen Bereich: level-1-only, level-2-only oder level-1-2. Level-1-Router haben Nachbarn nur im selben Bereich. Level-2-only (Backbone) können Nachbarn in verschiedenen Bereichen haben. Level-1-2 können Nachbarn in allen Bereichen haben. Voreinstellung ist "level-1-2".
metric-style { metric-style }	**Zusammenfassung:** { narrow, transition, wide }

Parameter	Beschreibung
	Standard: wide Der metrische Stil Type Length Value (TLV) für diesen Bereich: narrow, transition oder wide. Voreinstellung ist "wide".
area-authorization { area-authorization }	**Zusammenfassung:** { clear, md5 } **Standard:** clear Die Autorisierungsart für das Bereichspasswort. Voreinstellung ist "clear".
area-password { area-password }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 254 Zeichen Das zur Übertragung von Level-1-LSPs zu verwendende Bereichspasswort.
area-authentication { area-authentication }	**Zusammenfassung:** { send-only, validate } **Standard:** send-only Die mit dem Bereichspasswort an SNP PDUs zu verwendende Authentifizierungsoption. Voreinstellung ist "send-only".
domain-authorization { domain-authorization }	**Zusammenfassung:** { clear, md5 } **Standard:** clear Die Autorisierungsart für das Domänenpasswort. Voreinstellung ist "clear".
domain-password { domain-password }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 254 Zeichen Das zur Übertragung von Level-2-LSPs zu verwendende Domänenpasswort.
domain-authentication { domain-authentication }	**Zusammenfassung:** { send-only, validate } **Standard:** send-only Die mit dem Domänenpasswort an SNP PDUs zu verwendende Authentifizierungsoption. Voreinstellung ist "send-only".

4. Fügen Sie einen oder mehrere Network Entity Titles (NETs) hinzu. Weitere Informationen finden Sie unter Abschnitt 12.6.11, „Verwalten von Network Entity Titles (NETs)“.
5. Konfigurieren Sie bei Bedarf Intervalle für die Erzeugung von Link-State-Paketen (LSPs). Der Standardwert ist 30 Sekunden. Weitere Informationen finden Sie unter Abschnitt 12.6.7, „LSP-Generierung verwalten“.
6. Konfigurieren Sie bei Bedarf Aktualisierungsintervalle für Link-State-Pakete (LSPs). Der Standardwert ist 900 Sekunden. Weitere Informationen finden Sie unter Abschnitt 12.6.10, „LSP-Auffrischungsintervalle verwalten“.
7. Konfigurieren Sie bei Bedarf das Mindestintervall zwischen aufeinanderfolgenden SPF-Berechnungen. Der Standardwert ist 1 Sekunde. Weitere Informationen finden Sie unter Abschnitt 12.6.8, „SPF-Berechnungen verwalten“.
8. Konfigurieren Sie bei Bedarf, wie lange LSPs in der Link-State-Datenbank (LSDB) verweilen, bevor sie aktualisiert werden. Der Standardwert ist 1200 Sekunden. Weitere Informationen finden Sie unter Abschnitt 12.6.9, „Die Lebensdauer von LSPs verwalten“.
9. Definieren Sie bei Bedarf Regeln für umverteilte statische, RIP-, BGP- oder OSPF-Routen. Weitere Informationen finden Sie unter Abschnitt 12.6.12, „Umverteilungsmetriken verwalten“.
10. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.6.5.3

Eine Bereichsvariable löschen

Um eine Bereichsvariable für dynamische IS-IS-Routen zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.

2. Löschen Sie die Bereichsvariable, indem Sie Folgendes eingeben:

```
no routing isis area name
```

   Erläuterung:

   - *name* ist die eindeutige Bezeichnung für einen Routingprozess, der zu einem bestimmten Router gehört.

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.6.6

Schnittstellen verwalten

IS-IS sendet Hello-Pakete und Link-State-Pakete (LSP) über Schnittstellen, für die IS-IS-aktiviert ist.

HINWEIS
IS-IS wird nur an Ethernet-Schnittstellen unterstützt.

INHALT

- Abschnitt 12.6.6.1, „Eine Liste der Schnittstellen anzeigen“
- Abschnitt 12.6.6.2, „Konfigurieren einer Schnittstelle“

Abschnitt 12.6.6.1

Eine Liste der Schnittstellen anzeigen

Um eine Liste der Schnittstellen für dynamische IS-IS-Routen anzuzeigen, geben Sie Folgendes ein:

```
show running-config routing isis interface
```

Falls Schnittstellen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config routing isis interface | tab
             IPV4                  POINT
             AREA                  TO              CIRCUIT   CIRCUIT                CSNP      HELLO
 HELLO       PSNP
IFNAME       TAG     CIRCUIT TYPE  POINT  PASSIVE  PASSWORD  AUTHORIZATION  METRIC  INTERVAL  INTERVAL
 MULTIPLIER  INTERVAL
-------------------------------------------------------------------------------------------------
fe-cm-1      Area_1  level-1-2     true   true     admin     md5            10      10        3
 10          2
switch.0001  Area_2  level-1-only  false  true     admin     clear          10      10        3
 10          2

!
```

Schnittstellen werden automatisch hinzugefügt, wenn ein VLAN erstellt wird. Weitere Informationen über das Erstellen eines VLAN finden Sie unter Abschnitt 8.5, „VLANs verwalten“.

Abschnitt 12.6.6.2

Konfigurieren einer Schnittstelle

Bei aktivierter IS-IS ist die Schnittstelle *switch.0001* bereits konfiguriert.

Um optionale Parameter für diese und andere zu IS-IS hinzugefügte Schnittstellen zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zur Schnittstelle, indem Sie Folgendes eingeben:

```
routing isis interface name
```

Erläuterung:

- *name* ist die Bezeichnung der Schnittstelle. Wenn die gewünschte Schnittstelle nicht verfügbar ist, muss diese als VLAN erstellt werden. Weitere Informationen über das Erstellen eines VLANs finden Sie in Abschnitt 8.5, „VLANs verwalten“.

3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
ipv4-area-tag { ipv4-area-tag }	**Zusammenfassung:** Eine Zeichenkette Die Bezeichnung der Bereichsvariablen, die für IS-IS über IPv4 zu verwenden ist.
circuit-type { circuit-type }	**Zusammenfassung:** { level-1-only, level-2-only, level-1-2 } Die IS-IS-Schaltkreisart. Level-1-Router haben Nachbarn nur im selben Bereich. Level-2 (Backbone) können Nachbarn in verschiedenen Bereichen haben. Level-1-2 können Nachbarn in allen Bereichen haben. Voreinstellung ist "level-1-2".
point-to-point	**Zusammenfassung:** { true, false } **Standard:** false Punkt-zu-Punkt-Netzwerkkommunikation aktivieren oder deaktivieren
passive	**Zusammenfassung:** { true, false } **Standard:** true Gibt an, ob eine Schnittstelle aktiv oder passiv ist. Passive Schnittstellen senden keine Pakete an andere Router und gehören nicht zu einem IS-IS-Bereich.
circuit-password { circuit-password }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 254 Zeichen Der bei IIHPDUs, die von diesem Transitsystem (IS, en: Intermediate System) übertragen werden, als ein Übertragungspasswort zu verwendende Wert.
circuit-authorization { circuit-authorization }	**Zusammenfassung:** { clear, md5 } **Standard:** clear Die bei IIHPDUs, die von diesem Transitsystem (IS, en: Intermediate System) übertragen werden, nicht mit dem Übertragungspasswort verbundene Autorisierungsart.
metric { metric }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 1 und 16777214 **Standard:** 10 Der Verbindung zugewiesene Metrik, die zur Berechnung der Kosten der Route verwendet wird. Wert liegt im Bereich von 1 bis 16777214. Voreinstellung ist 10.
csnp-interval { csnp-interval }	**Zusammenfassung:** Eine vorzeichenlose 16-Bit-Ganzzahl zwischen 1 und 600 **Standard:** 10 CSNP-Intervall in Sekunden, im Bereich von 1 bis 600. Voreinstellung ist 10.
hello-interval { hello-interval }	**Zusammenfassung:** Eine vorzeichenlose 16-Bit-Ganzzahl zwischen 1 und 600 **Standard:** 3 Hello-Intervall in Sekunden, im Bereich von 1 bis 600. Voreinstellung ist 3.

Parameter	Beschreibung
hello-multiplier { hello-multiplier }	**Zusammenfassung:** Eine vorzeichenlose 16-Bit-Ganzzahl zwischen 2 und 100 **Standard:** 10 Multiplikator für Hello-Haltezeit. Wert liegt im Bereich von 2 bis 100. Voreinstellung ist 10.
psnp-interval { psnp-interval }	**Zusammenfassung:** Eine vorzeichenlose 8-Bit-Ganzzahl zwischen 1 und 120 **Standard:** 2 PSNP-Intervall in Sekunden, im Bereich von 1 bis 120. Voreinstellung ist 2.

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.6.7
LSP-Generierung verwalten

IS-IS generiert standardmäßig alle 30 Sekunden neue Link-State-Packets (LSP). Dieses Intervall kann jedoch beliebig zwischen 1 und 120 Sekunden eingestellt werden.

Da die Festlegung eines neuen LSP bewirkt, dass andere Router im Bereich Routen neu berechnen, sollte das Intervall erhöht werden, um in Zeiten mit Netzwerkinstabilität eine Überflutung einzudämmen und damit die Auslastung anderer Router im Bereich zu verringern.

INHALT

- Abschnitt 12.6.7.1, „Eine Liste der Intervalle zur LSP-Generierung anzeigen“
- Abschnitt 12.6.7.2, „Hinzufügen eines LSP-Generierungsintervalls“
- Abschnitt 12.6.7.3, „Ein Intervall zur LSP-Generierung löschen“

Abschnitt 12.6.7.1
Eine Liste der Intervalle zur LSP-Generierung anzeigen

Um eine Liste der Intervalle zur LSP-Generierung, die für einen IS-IS-Bereich konfiguriert sind, anzuzeigen, geben Sie Folgendes ein:

```
show running-config routing isis area name lsp-gen-interval
```

Erläuterung:

- *`name`* ist die eindeutige Bezeichnung für einen Routingprozess, der zu einem bestimmten Router gehört.

Falls Intervalle konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config routing isis area Area_1 lsp-gen-interval | tab
ISTYPE        INTERVAL
------------------------
level-1-only  60

 !
!
```

Falls keine Intervalle konfiguriert wurden, fügen Sie je nach Bedarf Intervalle hinzu. Weitere Informationen finden Sie unter Abschnitt 12.6.7.2, „Hinzufügen eines LSP-Generierungsintervalls“.

Abschnitt 12.6.7.2

Hinzufügen eines LSP-Generierungsintervalls

Um ein LSP-Generierungsintervall zu einem IS-IS-Bereich hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie ein neues Intervall hinzu, indem Sie Folgendes eingeben:

   ```
   routing isis area name lsp-gen-interval is-type [ level-1-2 | level-1-only | level-2-only ]
   interval seconds
   ```

   Erläuterung:

   - *name* ist die eindeutige Bezeichnung für einen Routingprozess, der zu einem bestimmten Router gehört.
   - *level* ist der IS-Typ.
   - *seconds* ist das Mindestintervall in Sekunden, im Bereich von 1 bis 120. Der Standardwert ist 30.
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.6.7.3

Ein Intervall zur LSP-Generierung löschen

Um ein Intervall zur LSP-Generierung für einen IS-IS-Bereich zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die LDP-Schnittstelle, indem Sie Folgendes eingeben:

   ```
   no routing isis area name lsp-gen-interval is-type [ level-1-2 | level-1-only | level-2-only ]
   interval seconds
   ```

   Erläuterung:

   - *name* ist die eindeutige Bezeichnung für einen Routingprozess, der zu einem bestimmten Router gehört.
   - *level* ist der IS-Typ.
   - *seconds* ist das Mindestintervall in Sekunden, im Bereich von 1 bis 120. Die Voreinstellung ist 30.
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.6.8

SPF-Berechnungen verwalten

IS-IS nutzt den SPF-(Shortest Path First)-Algorithmus, um die besten Routen zu jedem bekannten Ziel im Netzwerk zu ermitteln. Wenn sich die Netzwerktopologie (nicht die externen Links) ändert, ist eine teilweise Neuberechnung erforderlich.

IS-IS kann so konfiguriert werden, dass die SPF-Berechnung alle 1 bis 120 Sekunden durchgeführt wird. Standardmäßig wird die SPF-Berechnung von IS-IS einmal pro Sekunde durchgeführt, was unter Umständen je nach Größe des Bereichs und der Anzahl der Topologieänderungen viel Rechnerleistung verbrauchen kann.

INHALT

- Abschnitt 12.6.8.1, „Eine Liste der SPF-Berechnungsintervalle anzeigen“

- Abschnitt 12.6.8.2, „Ein SPF-Berechnungsintervall hinzufügen“
- Abschnitt 12.6.8.3, „Ein SPF-Berechnungsintervall löschen“

Abschnitt 12.6.8.1
Eine Liste der SPF-Berechnungsintervalle anzeigen

Um eine Liste der SPF-Berechnungsintervalle, die für einen IS-IS-Bereich konfiguriert sind, anzuzeigen, geben Sie Folgendes ein:

```
show running-config routing isis area name spf-interval
```

Erläuterung:

- *name* ist die eindeutige Bezeichnung für einen Routingprozess, der zu einem bestimmten Router gehört.

Falls Intervalle konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config routing isis area Area_1 spf-interval | tab
ISTYPE        INTERVAL
-----------------------
level-1-only  60

 !
!
```

Falls keine Intervalle konfiguriert wurden, fügen Sie je nach Bedarf Intervalle hinzu. Weitere Informationen finden Sie unter Abschnitt 12.6.8.2, „Ein SPF-Berechnungsintervall hinzufügen“.

Abschnitt 12.6.8.2
Ein SPF-Berechnungsintervall hinzufügen

Um ein SPF-Berechnungsintervall zu einem IS-IS-Bereich hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie ein neues Intervall hinzu, indem Sie Folgendes eingeben:

   ```
   routing isis area name spf-interval is-type [ level-1-2 | level-1-only | level-2-only ] interval
   seconds
   ```

   Erläuterung:

   - *name* ist die eindeutige Bezeichnung für einen Routingprozess, der zu einem bestimmten Router gehört.
   - *level* ist der IS-Typ.
   - *seconds* ist das Mindestintervall in Sekunden, im Bereich von 1 bis 120. Die Voreinstellung ist 30.
3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.6.8.3
Ein SPF-Berechnungsintervall löschen

Um ein SPF-Berechnungsintervall für einen IS-IS-Bereich zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.

2. Löschen Sie die LDP-Schnittstelle, indem Sie Folgendes eingeben:

```
no routing isis area name spf-interval is-type [ level-1-2 | level-1-only | level-2-only ] interval seconds
```

Erläuterung:

- *name* ist die eindeutige Bezeichnung für einen Routingprozess, der zu einem bestimmten Router gehört.
- *level* ist der IS-Typ.
- *seconds* ist das Mindestintervall in Sekunden, im Bereich von 1 bis 120. Die Voreinstellung ist 30.

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.6.9

Die Lebensdauer von LSPs verwalten

IS-IS behält Link-State Packets (LSP) in der Link-State Database (LSDB) nur für eine kurze Zeit, sofern sie nicht aufgefrischt werden. Die maximale Aufbewahrungszeit ist standardmäßig auf 1200 Sekunden eingestellt. Sie kann jedoch bei Bedarf für verschiedene Routing-Typen in einem Bereich von 350 bis 65535 Sekunden angepasst werden.

Die Lebensdauer ist für jeden Bereich und jeden Routing-Typ im IS-IS-Netzwerk konfigurierbar.

HINWEIS
Informationen zum Konfigurieren des Auffrischungsintervalls für ein LSP finden Sie unter Abschnitt 12.6.10, „LSP-Auffrischungsintervalle verwalten“.

INHALT

- Abschnitt 12.6.9.1, „Eine Liste der LSP-Lebensdauerintervalle anzeigen“
- Abschnitt 12.6.9.2, „Hinzufügen eines LSP-Lebensdauerintervalls“
- Abschnitt 12.6.9.3, „Ein LSP-Lebensdauer-Intervall löschen“

Abschnitt 12.6.9.1

Eine Liste der LSP-Lebensdauerintervalle anzeigen

Um eine Liste der LSP-Lebensdauerintervalle, die für einen IS-IS-Bereich konfiguriert sind, anzuzeigen, geben Sie Folgendes ein:

```
show running-config routing isis area name max-lsp-lifetime
```

Erläuterung:

- *name* ist die eindeutige Bezeichnung für einen Routingprozess, der zu einem bestimmten Router gehört.

Falls Intervalle konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config routing isis area Area_1 max-lsp-lifetime | tab
ISTYPE        INTERVAL
-----------------------
level-1-only  60

 !
```

```
!
```

Falls keine Intervalle konfiguriert wurden, fügen Sie je nach Bedarf Intervalle hinzu. Weitere Informationen finden Sie unter Abschnitt 12.6.9.2, „Hinzufügen eines LSP-Lebensdauerintervalls“.

Abschnitt 12.6.9.2
Hinzufügen eines LSP-Lebensdauerintervalls

Um ein LSP-Lebensdauerintervall zu einem IS-IS-Bereich hinzuzufügen, gehen Sie wie folgt vor:

WICHTIG!
Das LSP-Lebensdauerintervall muss 300 Sekunden länger sein als das LSP-Aktualisierungsintervall. Weitere Informationen über das LSP-Aktualisierungsintervall finden Sie in Abschnitt 12.6.10, „LSP-Auffrischungsintervalle verwalten“.

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie ein neues Intervall hinzu, indem Sie Folgendes eingeben:

   ```
   routing isis area name max-lsp-lifetime is-type [ level-1-2 | level-1-only | level-2-only ]
   interval seconds
   ```

   Erläuterung:

   - *name* ist die eindeutige Bezeichnung für einen Routingprozess, der zu einem bestimmten Router gehört.
   - *level* ist der IS-Typ.
   - *seconds* ist das Mindestintervall in Sekunden, im Bereich von 1 bis 120. Der Standardwert ist 30.
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.6.9.3
Ein LSP-Lebensdauer-Intervall löschen

Um ein LSP-Lebensdauer-Intervall für einen IS-IS-Bereich zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die LDP-Schnittstelle, indem Sie Folgendes eingeben:

   ```
   no routing isis area name max-lsp-lifetime is-type [ level-1-2 | level-1-only | level-2-only ]
   interval seconds
   ```

   Erläuterung:

   - *name* ist die eindeutige Bezeichnung für einen Routingprozess, der zu einem bestimmten Router gehört.
   - *level* ist der IS-Typ.
   - *seconds* ist das Mindestintervall in Sekunden, im Bereich von 1 bis 120. Die Voreinstellung ist 30.
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.6.10

LSP-Auffrischungsintervalle verwalten

IS-IS behält Link-State Packets (LSP) in der Link-State Database (LSDB) nur für eine kurze Zeit, sofern sie nicht aufgefrischt werden. Standardmäßig bleiben LSP 1200 Sekunden in der LSDB (dies wird als *Lebensdauer* eines LSP bezeichnet), und sie werden alle 900 Sekunden aktualisiert.

Das Auffrischungsintervall ist für jeden Bereich und jeden Routing-Typ im IS-IS-Netzwerk konfigurierbar.

HINWEIS
Informationen zum Konfigurieren der Lebensdauer eines LSP finden Sie unter Abschnitt 12.6.9, „Die Lebensdauer von LSPs verwalten“.

INHALT

- Abschnitt 12.6.10.1, „Eine Liste der LSP-Aktualisierungsintervalle anzeigen“
- Abschnitt 12.6.10.2, „Hinzufügen eines LSP-Aktualisierungsintervalls“
- Abschnitt 12.6.10.3, „Ein LSP-Aktualisierungsintervall löschen“

Abschnitt 12.6.10.1

Eine Liste der LSP-Aktualisierungsintervalle anzeigen

Um eine Liste der LSP-Aktualisierungsintervalle, die für einen IS-IS-Bereich konfiguriert sind, anzuzeigen, geben Sie Folgendes ein:

```
show running-config routing isis area name lsp-refresh-interval
```

Erläuterung:

- *name* ist die eindeutige Bezeichnung für einen Routingprozess, der zu einem bestimmten Router gehört.

Falls Intervalle konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config routing isis area Area_1 lsp-refresh-interval | tab
ISTYPE        INTERVAL
-----------------------
level-1-only  60

 !
!
```

Falls keine Intervalle konfiguriert wurden, fügen Sie je nach Bedarf Intervalle hinzu. Weitere Informationen finden Sie unter Abschnitt 12.6.10.2, „Hinzufügen eines LSP-Aktualisierungsintervalls“.

Abschnitt 12.6.10.2

Hinzufügen eines LSP-Aktualisierungsintervalls

Um ein LSP-Aktualisierungsintervall zu einem IS-IS-Bereich hinzuzufügen, gehen Sie wie folgt vor:

WICHTIG!
Das LSP-Aktualisierungsintervall muss 300 Sekunden kürzer sein als das LSP-Lebensdauerintervall. Weitere Informationen über das LSP-Aktualisierungsintervall finden Sie in Abschnitt 12.6.9, „Die Lebensdauer von LSPs verwalten“.

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie ein neues Intervall hinzu, indem Sie Folgendes eingeben:

   ```
   routing isis area name lsp-refresh-interval is-type [ level-1-2 | level-1-only | level-2-only ]
   interval seconds
   ```

   Erläuterung:

   - *name* ist die eindeutige Bezeichnung für einen Routingprozess, der zu einem bestimmten Router gehört.
   - *level* ist der IS-Typ.
   - *seconds* ist das Mindestintervall in Sekunden, im Bereich von 1 bis 120. Der Standardwert ist 30.
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.6.10.3
Ein LSP-Aktualisierungsintervall löschen

Um ein LSP-Aktualisierungsintervall für einen IS-IS-Bereich zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die LDP-Schnittstelle, indem Sie Folgendes eingeben:

   ```
   no routing isis area name lsp-refresh-interval is-type [ level-1-2 | level-1-only | level-2-only ]
   interval seconds
   ```

   Erläuterung:

   - *name* ist die eindeutige Bezeichnung für einen Routingprozess, der zu einem bestimmten Router gehört.
   - *level* ist der IS-Typ.
   - *seconds* ist das Mindestintervall in Sekunden, im Bereich von 1 bis 120. Die Voreinstellung ist 30.
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.6.11
Verwalten von Network Entity Titles (NETs)

Network Entity Titles (NETs) definieren die Bereichsadresse und die System-ID für den Router. Datenverkehr, der von einem anderen Router mit derselben Bereichsadresse und System-ID empfangen wurde, wird an diesen Router weitergeleitet.

Der RUGGEDCOM ROX II unterstützt das IS-IS-Multihoming. Dieses Verfahren erlaubt, dass mehrere NETs für einen einzelnen Router definiert werden und ergänzt die Liste möglicher Datenverkehrsquellen.

Jeder NET besitzt einen Hexadezimalwert, der zwischen 8 und 20 Oktette lang sein kann, obwohl 10 Oktette üblich sind. Der Wert beinhaltet einen Authority and Format-Identifikator (AFI), eine Bereichskennung, einen System-Identifikator und einen Selektor. Nachstehend ein Beispiel für eine NET-Adresse:

```
0001.1921.6800.1001.00
```

- *49* ist der AFI. Verwenden Sie *49* für die private Adressierung.
- *0001* ist die Bereichskennung. In diesem Beispiel ist der Bereich *1*.

- *1921.6800.1001* ist der System-Identifikator. Es kann jede beliebige Nummer verwendet werden, jedoch handelt es sich bei dem System-Identifikator um eine modifizierte Form der IP-Adresse des Routers. Der System-Identifikator in diesem Beispiel wird beispielsweise in *192.168.1.1* übersetzt. Um die Adresse in die Gegenrichtung zu konvertieren, füllen Sie die IP-Adresse mit Nullen (0) auf und ordnen die Dezimalpunkte neu an, indem Sie drei zwei Byte lange Zahlen bilden.
- *00* ist der Selektor.

WICHTIG!
Der System-Identifikator muss im Netzwerk eindeutig sein.

INHALT

- Abschnitt 12.6.11.1, „Eine Liste der NETs anzeigen“
- Abschnitt 12.6.11.2, „Eine NET hinzufügen“
- Abschnitt 12.6.11.3, „Eine Network Entity Title löschen“

Abschnitt 12.6.11.1
Eine Liste der NETs anzeigen

Um eine Liste der für dynamische IS-IS-Routen konfigurierten Bereiche anzusehen, geben Sie Folgendes ein:

```
show running-config routing isis area name net
```

Erläuterung:

- *name* ist die eindeutige Bezeichnung für einen Routingprozess, der zu einem bestimmten Router gehört.

Falls NETs konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config routing isis area Area_1 net | tab
NET TITLE
--------------------------
49.0001.1921.6800.1001.00

 !
!
```

Falls keine NETs konfiguriert wurden, fügen Sie je nach Bedarf NETs hinzu. Weitere Informationen finden Sie unter Abschnitt 12.6.11.2, „Eine NET hinzufügen“.

Abschnitt 12.6.11.2
Eine NET hinzufügen

Um eine Network Entity Title (NET) für einen IS-IS-Bereich hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie die NET hinzu, indem Sie Folgendes eingeben:

   ```
   routing isis area name net title
   ```

   Erläuterung:

   - *name* ist die eindeutige Bezeichnung für einen Routingprozess, der zu einem bestimmten Router gehört.

- *title* ist die NET für den Router und besteht aus einer Bereichskennung aus 2 Oktetten, einer System-ID aus 3 Oktetten und einem Selektor aus 1 Oktett. Beispiel: 0001.1921.6800.1001.00

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.6.11.3
Eine Network Entity Title löschen

Um eine Network Entity Title (NET) für einen IS-IS-Bereich zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die NET, indem Sie Folgendes eingeben:

```
no routing isis area name net title
```

Erläuterung:

- *name* ist die eindeutige Bezeichnung für einen Routingprozess, der zu einem bestimmten Router gehört.
- *title* ist die NET für den Router und besteht aus einer Bereichskennung aus 2 Oktetten, einer System-ID aus 3 Oktetten und einem Selektor aus 1 Oktett. Beispiel: 0001.1921.6800.1001.00

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.6.12
Umverteilungsmetriken verwalten

Umverteilung im Allgemeinen ist die Ankündigung von Routen durch ein Protokoll, die über ein anderes dynamisches Routingprotokoll, eine statische Route oder einen direkt angeschlossenen Router erlernt wurden. Sie wird eingesetzt, um die Interoperabilität zwischen Netzwerken mit unterschiedlichen Routing-Protokollen zu fördern.

Die Umverteilung einer Route wird durch Definition einer Metrik für das Source-Routing-Protokoll erreicht. Da jedes Routing-Protokoll die Routen unterschiedlich berechnet, muss darauf geachtet werden, eine Metrik zu definieren, die vom Protokoll verstanden wird.

Es gibt zwei unterschiedlichen Metriken: interne und externe. Beiden Metriken kann ein Wert zwischen 0 und 63 zugewiesen werden. Um jedoch zu verhindern, dass externe Metriken mit internen Metriken konkurrieren, wird jeder externen Metrik automatisch der Wert 64 hinzugefügt. Damit liegen externe Metriken im Bereich von 64 bis 128, obwohl der definierte Wert nur im Bereich von 0 bis 63 liegt.

Für IS-IS gibt es keine vorgegebene Metrik. Für jedes Routing-Protokoll sollte eine Metrik definiert werden, andernfalls wird automatisch ein metrischer Wert von Null (0) verwendet.

INHALT

- Abschnitt 12.6.12.1, „Eine Liste der Umverteilungsmetriken anzeigen“
- Abschnitt 12.6.12.2, „Eine Umverteilungsmetrik hinzufügen“
- Abschnitt 12.6.12.3, „Eine Umverteilungsmetrik löschen“

Abschnitt 12.6.12.1
Eine Liste der Umverteilungsmetriken anzeigen

Um eine Liste der Umverteilungsmetriken für einen IS-IS-Bereich anzusehen, geben Sie Folgendes ein:

```
show running-config routing isis area name redistribute
```

Erläuterung:

- *name* ist die eindeutige Bezeichnung für einen Routingprozess, der zu einem bestimmten Router gehört.

Falls Metriken konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config routing isis area Area_1 redistribute | tab
                  METRIC
SOURCE  IS TYPE   TYPE      METRIC
-------------------------------------
bgp     level-1-2  internal  10

 !
!
```

Falls keine Umverteilungsmetriken konfiguriert wurden, fügen Sie je nach Bedarf Metriken hinzu. Weitere Informationen finden Sie unter Abschnitt 12.6.12.2, „Eine Umverteilungsmetrik hinzufügen".

Abschnitt 12.6.12.2
Eine Umverteilungsmetrik hinzufügen

Um für einen IS-IS-Bereich eine Umverteilungsmetrik hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie die Metrik hinzu, indem Sie Folgendes eingeben:

   ```
   routing isis area name redistribute source
   ```

   Erläuterung:

   - *name* ist die eindeutige Bezeichnung für einen Routingprozess, der zu einem bestimmten Router gehört.
   - *source* ist das Protokoll, das über die IS-IS-Route Pakete überträgt. Optionen sind u.a. bgp, connected, kernel, ospf, rip und static.
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
is-type { is-type }	**Zusammenfassung:** { level-1-only, level-2-only, level-1-2 } IS-Typ der IS-IS-Information, spezifiziert als "level-1-only", "level-2-only" oder "level-1-2". Gibt es keine Spezifizierung, wird der IS-Typ aus dem Bereich verwendet.
metric-type { metric-type }	**Zusammenfassung:** { internal, external } **Standard:** external Der äußere IS-IS-Metriktyp für umverteilte Routen. Voreinstellung ist "external".
metric { metric }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 0 und 16777214 Die Metrik für umverteilte Routen.

4. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.6.12.3

Eine Umverteilungsmetrik löschen

Um eine Umverteilungsmetrik für einen IS-IS-Bereich zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die Metrik, indem Sie Folgendes eingeben:

   ```
   no routing isis area name redistribute source
   ```

   Erläuterung:

   - *name* ist die eindeutige Bezeichnung für einen Routingprozess, der zu einem bestimmten Router gehört.
   - *source* ist das Protokoll, das über die IS-IS-Route Pakete überträgt. Optionen sind u.a. bgp, connected, kernel, ospf, rip und static.
3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.7

Verwalten des RIP

Das Routing Information-Protokoll (RIP) bestimmt den besten Pfad für das Leiten des IP-Datenverkehrs durch ein TCP/IP-Netzwerk in Abhängigkeit von der Anzahl an Hops zwischen zwei beliebigen Routern. Das Protokoll nutzt die zu einem vorhandenen Netzwerk kürzeste verfügbare Route als Route für das Senden von Paketen zu diesem Netzwerk.

Der RUGGEDCOM ROX II RIP Daemon ist eine RFC 1058 [http://tools.ietf.org/rfc/rfc1058.txt]-konforme Implementierung des RIP-Protokolls, die die RIP-Versionen 1 und 2 unterstützt. Die RIP-Version 1 ist auf veraltete klassenbasierte Netzwerke beschränkt, während die RIP-Version 2 Subnetzmasken sowie die einfache Authentifizierung unterstützt, um zu steuern, mit welchen Routern die Routen ausgetauscht werden.

RIP greift auf Netzwerk- und Nachbareinträge zu, um zu steuern, mit welchen Routern die Routen ausgetauscht werden. Ein Netzwerk ist entweder ein Subnetz oder eine Schnittstelle eines physischen (broadcastfähigen) Netzwerks. Jeder Router, der Bestandteil dieses Subnetzes bzw. mit dieser Schnittstelle verbunden ist, kann Routen austauschen. Ein Nachbar ist ein bestimmter Router, der anhand seiner IP-Adresse spezifiziert wird und mit dem Routen ausgetauscht werden. Bei Punkt-zu-Punkt-Verbindungen müssen Nachbareinträge zum Hinzufügen anderer Router verwendet werden, mit denen Routen ausgetauscht werden. Die maximal zulässige Anzahl an Hops zwischen zwei Punkten in einem RIP-Netzwerk liegt bei 15, wodurch die Netzwerkgröße beschränkt wird.

Verbindungsausfälle werden bei Verwendung von RIP letztlich bemerkt, obwohl es bei RIP nicht ungewöhnlich ist, dass es mehrere Minuten dauert, bis eine Dead-Route aus dem gesamten Netzwerk verschwunden ist. In großen Netzwerken kann es bei auftretenden Verbindungs- oder Routenänderungen über eine Stunde dauern, bis diese konvergiert sind. Für eine schnellere Konvergenz und Wiederherstellung wird OSPF empfohlen. Weitere Informationen über OSPF finden Sie in Abschnitt 12.9, „Verwalten von OSPF“.

Bei dem RIP handelt es sich um ein veraltetes Routing-Protokoll, das größtenteils durch OSPF abgelöst wurde.

HINWEIS
In komplexen vorhandenen Netzwerken können RIP, OSPF, BGP und IS-IS gleichzeitig auf demselben Router aktiv sein. In der Regel wird jedoch jeweils nur ein dynamisches Routingprotokoll verwendet.

INHALT

- Abschnitt 12.7.1, „Konfigurieren des RIP“

- Abschnitt 12.7.2, „Anzeigen des Status von dynamischen RIP-Routen“
- Abschnitt 12.7.3, „Präfix-Listen und -Einträge verwalten“
- Abschnitt 12.7.4, „Netzwerke verwalten“
- Abschnitt 12.7.5, „Netzwerk-IP-Adressen verwalten“
- Abschnitt 12.7.6, „Netzwerkschnittstellen verwalten“
- Abschnitt 12.7.7, „Nachbarn verwalten“
- Abschnitt 12.7.8, „Verteilung der Präfix-Liste verwalten“
- Abschnitt 12.7.9, „Schlüsselbunde und Schlüssel verwalten“
- Abschnitt 12.7.10, „Umverteilungsmetriken verwalten“
- Abschnitt 12.7.11, „Routing-Schnittstellen verwalten“

Abschnitt 12.7.1

Konfigurieren des RIP

Um das dynamische Routing mithilfe des Routing-Information-Protocol-(RIP)-Daemon zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***routing » rip*** und konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
enabled	Aktiviert das dynamische RIP-Routing-Protokoll
default-information-originate	Das Routenelement erstellt nur innerhalb des RIP eine statische Route. Dieses Element sollte nur von fortgeschrittenen Benutzern eingesetzt werden, die sich mit dem Routing Information Protocol (RIP) besonders gut auskennen. In den meisten Fällen empfiehlt es sich, eine statische Route anzulegen und diese im RIP mit dem "Redistribute Element" mit statischem Typ umzuverteilen.
default-metric { default-metric }	**Zusammenfassung:** Eine vorzeichenbehaftete 8-Bit-Ganzzahl zwischen 1 und 16 **Standard:** 1 Stellt die Standard-Metrik ein. Mit Ausnahme der angebundenen Routentypen wird die Standard-Metrik angekündigt, wenn eine Metrik nicht für eine umverteilte Route konfiguriert wurde. Bei angebundenen Routentypen ist die Standard-Metrik trotz des Werts dieses Parameters 1.
distance-default { distance-default }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 1 und 255 Legt den RIP-Standardabstand fest.
version { version }	**Zusammenfassung:** Eine vorzeichenbehaftete 8-Bit-Ganzzahl zwischen 1 und 2 Die RIP-Version so einstellen, dass Lesen und Senden zulässig ist. Die Version kann entweder 1 oder 2 sein. Das Deaktivieren von RIPv1 durch Festlegen der Version 2 wird NACHDRÜCKLICH empfohlen.

3. Konfigurieren Sie Präfixlisten. Weitere Informationen finden Sie unter Abschnitt 12.7.3.3, „Eine Präfixliste hinzufügen“.
4. Konfigurieren Sie ein Netzwerk. Weitere Informationen finden Sie unter Abschnitt 12.7.4.1, „Ein Netzwerk konfigurieren“.
5. Konfigurieren Sie die Präfixlisten-Verteilung. Weitere Informationen finden Sie unter Abschnitt 12.7.8.2, „Hinzufügen eines Präfixlisten-Verteilpfads“.

6. Konfigurieren Sie Schlüsselbunde. Weitere Informationen finden Sie unter Abschnitt 12.7.9.3, „Ein Schlüsselbund hinzufügen“.
7. Konfigurieren Sie Umverteilungsmetriken. Weitere Informationen finden Sie unter Abschnitt 12.7.10.2, „Eine Umverteilungsmetrik hinzufügen“.
8. Konfigurieren Sie Schnittstellen. Weitere Informationen finden Sie unter Abschnitt 12.7.11.2, „Eine Routing-Schnittstelle konfigurieren“.
9. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.7.2

Anzeigen des Status von dynamischen RIP-Routen

Um den Status der auf dem Gerät konfigurierten dynamischen RIP-Routen anzuzeigen, geben Sie Folgendes ein:

```
show routing status rip route
```

Sofern RIP-Routen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show routing status rip route | tab
NETWORK          TYPE       SUB TYPE   NEXT HOP     METRIC  FROM         TAG  TI
-------------------------------------------------------------------------------
192.168.0.0/24   connected  interface  0.0.0.0      1       self         0
192.168.5.0/24   rip        normal     192.168.0.3  2       192.168.0.3  0    02
192.168.6.0/24   rip        normal     192.168.0.3  2       192.168.0.3  0    02
192.168.50.0/24  connected  interface  0.0.0.0      1       self         0
192.168.60.0/24  connected  interface  0.0.0.0      1       self         0
```

Diese Liste liefert die folgenden Informationen:

Parameter	Beschreibung
network	**Zusammenfassung:** Eine Zeichenkette Das Netzwerk.
type	**Zusammenfassung:** Eine Zeichenkette Der Routentyp.
sub-type	**Zusammenfassung:** Eine Zeichenkette Der Routen-Subtyp.
next-hop	**Zusammenfassung:** Eine Zeichenkette Der nächste Hop.
metric	**Zusammenfassung:** Eine Zeichenkette Der metrische Wert.
from	**Zusammenfassung:** Eine Zeichenkette Woher diese Route kommt.
tag	**Zusammenfassung:** Eine Zeichenkette Variable.
time	**Zusammenfassung:** Eine Zeichenkette Die Aktualisierungszeit der Route.

Um den Status der auf dem Gerät konfigurierten RIP-Schnittstellen anzuzeigen, geben Sie Folgendes ein:

```
show routing status rip interface
```

Falls RIP-Schnittstellen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show routing status rip interface | tab
                                                    NEXT
NAME          NETWORK           TYPE       SUB TYPE   HOP      METRIC  FROM  TAG  TIME
-------------------------------------------------------------------------------------
switch.1112
              192.168.11.0/24   connected  interface  0.0.0.0  1       self  0
```

Diese Liste liefert die folgenden Informationen:

Parameter	Beschreibung
network	**Zusammenfassung:** Eine Zeichenkette Das Netzwerk.
type	**Zusammenfassung:** Eine Zeichenkette Der Routentyp.
sub-type	**Zusammenfassung:** Eine Zeichenkette Der Routen-Subtyp.
next-hop	**Zusammenfassung:** Eine Zeichenkette Nächster Hop.
metric	**Zusammenfassung:** Eine Zeichenkette Der metrische Wert.
from	**Zusammenfassung:** Eine Zeichenkette Woher diese Route kommt.
tag	**Zusammenfassung:** Eine Zeichenkette Variable.
time	**Zusammenfassung:** Eine Zeichenkette Die Aktualisierungszeit der Route.

Falls keine dynamischen RIP-Routen konfiguriert wurden, konfigurieren Sie RIP und fügen Sie nach Bedarf Routen hinzu. Weitere Informationen über das Konfigurieren von RIP finden Sie in Abschnitt 12.7.1, „Konfigurieren des RIP“.

Abschnitt 12.7.3

Präfix-Listen und -Einträge verwalten

Nachbarn können Präfix-Listen zugeordnet werden, die dem RIP-Daemon die Filterung eingehender oder abgehender Routen auf Grund der Einträge *allow* und *deny* in der Präfix-Liste ermöglichen.

INHALT

- Abschnitt 12.7.3.1, „Eine Liste der Präfixeinträge anzeigen“
- Abschnitt 12.7.3.2, „Eine Liste der Präfixeinträge anzeigen“
- Abschnitt 12.7.3.3, „Eine Präfixliste hinzufügen“
- Abschnitt 12.7.3.4, „Einen Präfixeintrag hinzufügen“

- Abschnitt 12.7.3.5, „Eine Präfixliste löschen“
- Abschnitt 12.7.3.6, „Einen Präfixeintrag löschen“

Abschnitt 12.7.3.1
Eine Liste der Präfixeinträge anzeigen

Um eine Liste der Präfixeinträge für dynamische RIP-Routen anzusehen, geben Sie Folgendes ein:

```
show running-config routing rip filter prefix-list
```

Falls Präfixlisten konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config routing rip filter prefix-list | tab
NAME                 DESCRIPTION  SEQ  ACTION  SUBNET           LE  GE
-------------------------------------------------------------------------
list-permit-lan-22   -
                                  100  permit  192.168.33.0/24  -   -
list-withdraw-lan-11 -
                                  100  permit  192.168.33.0/24  -   -
                                  200  permit  192.168.33.0/24  32  -

!
```

Falls keine Präfixlisten konfiguriert wurden, fügen Sie je nach Bedarf Listen hinzu. Weitere Informationen finden Sie unter Abschnitt 12.7.3.3, „Eine Präfixliste hinzufügen“.

Abschnitt 12.7.3.2
Eine Liste der Präfixeinträge anzeigen

Um eine Liste von Einträgen für dynamische RIP-Präfixlisten anzuzeigen, geben Sie Folgendes ein:

```
show running-config routing rip filter prefix-list name entry
```

Erläuterung:

- *name* ist die Bezeichnung der Präfixliste

Falls Einträge konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config routing rip filter prefix-list test entry | tab
SEQ  ACTION  SUBNET           LE  GE
-------------------------------------------
5    permit  192.168.40.0/24  32  -
6    deny    192.168.5.21/32    -   -

 !
!
```

Falls keine Einträge konfiguriert wurden, fügen Sie je nach Bedarf Einträge hinzu. Weitere Informationen finden Sie unter Abschnitt 12.7.3.4, „Einen Präfixeintrag hinzufügen“.

Abschnitt 12.7.3.3
Eine Präfixliste hinzufügen

Um eine Präfixliste für dynamische RIP-Routen hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie die Liste hinzu, indem Sie Folgendes eingeben:

   ```
   routing rip filter prefix-list name
   ```

   Erläuterung:

   - *name* ist die Bezeichnung der Präfixliste
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
description { description }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 1024 Zeichen Die Beschreibung der Präfixliste.

4. Fügen Sie nach Bedarf Präfixeinträge hinzu. Weitere Informationen finden Sie unter Abschnitt 12.7.3.4, „Einen Präfixeintrag hinzufügen“.
5. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.7.3.4
Einen Präfixeintrag hinzufügen

Um einen Eintrag in die Präfixliste eines dynamischen RIP hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den Eintrag hinzu, indem Sie Folgendes eingeben:

   ```
   routing rip filter prefix-list name entry number
   ```

   Erläuterung:

   - *name* ist die Bezeichnung der Präfixliste
   - *number* ist die Sequenznummer für den Eintrag
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
action { action }	**Zusammenfassung:** { deny, permit } **Standard:** permit Der Vorgang, der ausgeführt wird.
subnet { subnet }	**Zusammenfassung:** Eine Zeichenkette mit 9 bis 18 Zeichen Die IPv4-Netzwerkadresse und das Präfix. Dieser Parameter ist obligatorisch.
le { le }	**Zusammenfassung:** Eine vorzeichenlose 8-Bit-Ganzzahl zwischen 1 und 32 Die maximale Präfixlänge, die zu erreichen ist.
ge { ge }	**Zusammenfassung:** Eine vorzeichenlose 8-Bit-Ganzzahl zwischen 1 und 32 Die minimale Präfixlänge, die zu erreichen ist.

4. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.7.3.5
Eine Präfixliste löschen

Um eine Präfixliste für dynamische RIP-Routen zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.

   HINWEIS
   Beim Löschen einer Präfixliste werden gleichzeitig alle zugehörigen Präfixe entfernt.

2. Löschen Sie die Liste, indem Sie Folgendes eingeben:

   ```
   no routing rip filter prefix-list name
   ```

   Erläuterung:

   - *name* ist die Bezeichnung der Präfixliste

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.7.3.6
Einen Präfixeintrag löschen

Um einen Eintrag in der Präfixliste eines dynamischen RIP zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den Eintrag, indem Sie Folgendes eingeben:

   ```
   no routing rip filter prefix-list name entry number
   ```

   Erläuterung:

   - *name* ist die Bezeichnung der Präfixliste
   - *number* ist die Sequenznummer für den Eintrag

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.7.4
Netzwerke verwalten

Im Gegensatz zu den Nachbarn, bei denen es sich um spezifische Router handelt, mit denen Routen ausgetauscht werden, sind Netzwerke Gruppen von Routern, die entweder Teil eines bestimmten Subnetzes sind oder mit einer bestimmten Netzwerkschnittstelle verbunden sind. Sie können gleichzeitig als Nachbarn genutzt werden.

HINWEIS
Bei Punkt-zu-Punkt-Verbindungen legen Sie anstelle eines Netzwerks Nachbarn fest. Weitere Informationen finden Sie unter Abschnitt 12.7.7.2, „Einen Nachbarn hinzufügen“.

HINWEIS
RIP v1 sendet in seinen Updates keine Subnetzmaskeninformationen. Die definierten Netzwerke sind auf die klassischen Netzwerke (d. h. Klasse A, B und C) beschränkt.

HINWEIS
Wenn Nachbarn, aber keine Netzwerke angegeben sind, empfängt der Router Routing-Informationen von seinen Nachbarn, leitet aber keine Routen zu ihnen. Weitere Informationen über Nachbarn finden Sie unter Abschnitt 12.7.7, „Nachbarn verwalten“.

INHALT

- Abschnitt 12.7.4.1, „Ein Netzwerk konfigurieren“
- Abschnitt 12.7.4.2, „Nachverfolgen von Befehlen“

Abschnitt 12.7.4.1

Ein Netzwerk konfigurieren

Um ein Netzwerk für das RIP-Protokoll zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie eine oder mehrere Netzwerk-IP-Adressen hinzu. Weitere Informationen finden Sie unter Abschnitt 12.7.5.2, „Eine Netzwerk-IP-Adresse hinzufügen“.
3. Fügen Sie eine oder mehrere Netzwerkschnittstellen hinzu. Weitere Informationen finden Sie unter Abschnitt 12.7.6.2, „Eine Netzwerkschnittstelle hinzufügen“.
4. Fügen Sie einen oder mehrere Nachbarn hinzu. Weitere Informationen finden Sie unter Abschnitt 12.7.7.2, „Einen Nachbarn hinzufügen“.

Abschnitt 12.7.4.2

Nachverfolgen von Befehlen

Netzwerkbefehle lassen sich mithilfe von Event Trackern, die unter ***global » tracking*** konfiguriert werden, nachverfolgen. Weitere Informationen über Event Tracker finden Sie in Abschnitt 12.5, „Event-Tracker verwalten“.

Ein Netzwerkbefehl wird in Abhängigkeit vom Status des Event Trackers aktiviert. Der Parameter `apply-when` bestimmt, wann der Befehl aktiviert wird. Beispiel: Wenn der Parameter `apply-when` auf **down**gesetzt ist, wird der Netzwerkbefehl aktiv (und kündigt dadurch das Netzwerk den RIP-Peers eines Routers an), wenn das nachverfolgte Ziel nicht verfügbar ist.

Um einen Befehl für ein RIP-Netzwerk nachzuverfolgen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***routing » rip » distribute-prefix-list » {direction} {interface} » track***, wobei *{direction}* die Richtung (ein- oder ausgehend) ist, in die Routing-Updates gefiltert werden, und *{interface}* die Bezeichnung der Schnittstelle ist.
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
event { event }	**Zusammenfassung:** Eine Zeichenkette Wählt ein Ereignis zum Tracken. Die "distribute-prefix-list" nur dann eingesetzt, wenn das getrackte Ereignis sich im Klarzustand befindet. Dieser Parameter ist obligatorisch.
apply-when { apply-when }	**Zusammenfassung:** { up, down } **Standard:** up

Parameter	Beschreibung
	Wendet die "distribute-prefix-list" an, wenn das getrackte Ereignis verfügbar ("UP") oder nicht verfügbar ("DOWN") wird.

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.7.5
Netzwerk-IP-Adressen verwalten

Dieser Abschnitt beschreibt, wie Sie IP-Adressen für RIP-Netzwerke verwalten können.

INHALT

- Abschnitt 12.7.5.1, „Eine Liste der Netzwerk-IP-Adressen anzeigen“
- Abschnitt 12.7.5.2, „Eine Netzwerk-IP-Adresse hinzufügen“
- Abschnitt 12.7.5.3, „Eine Netzwerk-IP-Adresse löschen“

Abschnitt 12.7.5.1
Eine Liste der Netzwerk-IP-Adressen anzeigen

Um eine Liste der für ein RIP-Netzwerk konfigurierten IP-Adressen anzusehen, geben Sie Folgendes ein:

```
show running-config routing rip network ip
```

Falls Adressen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config routing rip network ip
routing rip
 network ip 192.168.33.0/24
 !
!
```

Falls keine IP-Adressen konfiguriert wurden, fügen Sie je nach Bedarf Adressen hinzu. Weitere Informationen finden Sie unter Abschnitt 12.7.5.2, „Eine Netzwerk-IP-Adresse hinzufügen“.

Abschnitt 12.7.5.2
Eine Netzwerk-IP-Adresse hinzufügen

Um eine IP-Adresse für ein RIP-Netzwerk hinzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den Nachbarn hinzu, indem Sie Folgendes eingeben:

   ```
   routing rip network ip address
   ```

   Erläuterung:

   - *`address`* ist die IP-Subnetzadresse und das Präfix für das Netzwerk

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.7.5.3
Eine Netzwerk-IP-Adresse löschen

Um eine IP-Adresse aus einem RIP-Netzwerk zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die IP-Adresse, indem Sie Folgendes eingeben:

   ```
   no routing rip network ip address
   ```

   Erläuterung:

   - *address* ist die IP-Subnetzadresse und das Präfix für das Netzwerk
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.7.6
Netzwerkschnittstellen verwalten

Dieser Abschnitt beschreibt, wie Sie von RIP-Netzwerken benutzte Schnittstellen verwalten können.

INHALT

- Abschnitt 12.7.6.1, „Eine Liste der Netzwerkschnittstellen anzeigen“
- Abschnitt 12.7.6.2, „Eine Netzwerkschnittstelle hinzufügen“
- Abschnitt 12.7.6.3, „Eine Netzwerkschnittstelle löschen“

Abschnitt 12.7.6.1
Eine Liste der Netzwerkschnittstellen anzeigen

Um eine Liste der für ein RIP-Netzwerk konfigurierten Schnittstellen anzusehen, geben Sie Folgendes ein:

```
show running-config routing rip network interface
```

Falls Schnittstellen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config routing rip network interface
routing rip
 network interface switch.4084
 !
!
```

Falls keine Schnittstellen konfiguriert wurden, fügen Sie je nach Bedarf Schnittstellen hinzu. Weitere Informationen finden Sie unter Abschnitt 12.7.7.2, „Einen Nachbarn hinzufügen“.

Abschnitt 12.7.6.2
Eine Netzwerkschnittstelle hinzufügen

Um für ein RIP-Netzwerk eine Schnittstelle hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den Nachbarn hinzu, indem Sie Folgendes eingeben:

   ```
   routing rip network interface name
   ```

   Erläuterung:

   - *name* ist die Bezeichnung der Schnittstelle
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.7.6.3
Eine Netzwerkschnittstelle löschen

Um eine Schnittstelle in einem RIP-Netzwerk zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie das Netzwerk durch Eingabe von:

   ```
   no routing rip network interface name
   ```

   Erläuterung:

   - *name* ist die Bezeichnung der Schnittstelle
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.7.7
Nachbarn verwalten

Nachbarn sind andere Router, mit denen Routen ausgetauscht werden.

INHALT

- Abschnitt 12.7.7.1, „Eine Liste der Nachbarn anzeigen“
- Abschnitt 12.7.7.2, „Einen Nachbarn hinzufügen“
- Abschnitt 12.7.7.3, „Einen Nachbarn löschen“

Abschnitt 12.7.7.1
Eine Liste der Nachbarn anzeigen

Um eine Liste der für ein RIP-Netzwerk konfigurierten Nachbarn anzusehen, geben Sie Folgendes ein:

```
show running-config routing rip network neighbor
```

Falls Nachbarn konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config routing rip network neighbor
routing rip
 network neighbor 192.168.33.2
 !
!
```

Falls keine Nachbarn konfiguriert wurden, fügen Sie je nach Bedarf Nachbarn hinzu. Weitere Informationen finden Sie unter Abschnitt 12.7.7.2, „Einen Nachbarn hinzufügen“.

Abschnitt 12.7.7.2
Einen Nachbarn hinzufügen

Um zu einem RIP-Netzwerk einen Nachbarn hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den Nachbarn hinzu, indem Sie Folgendes eingeben:

   ```
   routing rip network neighbor address
   ```

   Erläuterung:

   - *address* ist die IP-Adresse des Nachbarn
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.7.7.3
Einen Nachbarn löschen

Um einen Nachbarn in einem RIP-Netzwerk zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie das Netzwerk durch Eingabe von:

   ```
   no routing rip network neighbor address
   ```

   Erläuterung:

   - *address* ist die IP-Adresse des Nachbarn
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.7.8
Verteilung der Präfix-Liste verwalten

Dieser Abschnitt beschreibt, wie Sie die Verteilung von Präfix-Listen verwalten können.

INHALT

- Abschnitt 12.7.8.1, „Eine Liste der Präfixlisten-Verteilerpfade anzeigen“
- Abschnitt 12.7.8.2, „Hinzufügen eines Präfixlisten-Verteilpfads“

- Abschnitt 12.7.8.3, „Einen Präfixlisten-Verteilpfad löschen“

Abschnitt 12.7.8.1
Eine Liste der Präfixlisten-Verteilerpfade anzeigen

Um eine Liste der Präfixlisten-Verteilerpfade für dynamische RIP-Routen anzusehen, geben Sie Folgendes ein:

```
show running-config routing rip distribute-prefix-list
```

Falls Verteilerpfade konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config routing rip distribute-prefix-list
routing rip
 distribute-prefix-list out ""
  prefix-list list-permit-lan-22
 !
!
```

Falls keine Präfixlisten-Verteilerpfade konfiguriert wurden, fügen Sie je nach Bedarf Verteilerpfade hinzu. Weitere Informationen finden Sie unter Abschnitt 12.7.8.2, „Hinzufügen eines Präfixlisten-Verteilpfads“.

Abschnitt 12.7.8.2
Hinzufügen eines Präfixlisten-Verteilpfads

Um einen Präfixlisten-Verteilpfad für dynamische RIP-Routen hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den Pfad hinzu, indem Sie Folgendes eingeben:

   ```
   routing rip distribute-prefix-list direction interface
   ```

   Erläuterung:

   - *direction* ist die Richtung (ein- oder ausgehend), in die Routing-Updates gefiltert werden.
   - *interface* ist die Bezeichnung der Schnittstelle. Dieser Parameter ist optional.
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
prefix-list { prefix-list }	**Zusammenfassung:** Eine Zeichenkette Die Bezeichnung der Präfixliste. Dieser Parameter ist obligatorisch.

4. Konfigurieren Sie bei Bedarf einen Event Tracker, um die Netzwerkbefehle zu beobachten. Weitere Informationen finden Sie unter Abschnitt 12.7.4.2, „Nachverfolgen von Befehlen“.
5. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.7.8.3
Einen Präfixlisten-Verteilpfad löschen

Um einen Präfixlisten-Verteilpfad für dynamische RIP-Routen zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den Pfad, indem Sie Folgendes eingeben:

   ```
   no routing rip distribute-prefix-list direction interface
   ```

   Erläuterung:

   - *direction* ist die Richtung (ein- oder ausgehend), in die Routing-Updates gefiltert werden.
   - *interface* ist die Bezeichnung der Schnittstelle Dieser Parameter ist optional.
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.7.9

Schlüsselbunde und Schlüssel verwalten

Schlüsselbunde sind eine Anzahl Schlüssel (oder gemeinsame Geheimnisse), mit denen die Kommunikation über ein dynamisches IP-Netzwerk authentifiziert werden kann. Nur Router mit dem gleichen Schlüssel können Mitteilungen senden und empfangen.

Es können mehrere Schlüsselbunde für verschiedene Schnittstellengruppen konfiguriert werden und die Gültigkeit jedes Schlüssels in einem Schlüsselbund kann separat konfiguriert werden.

INHALT

- Abschnitt 12.7.9.1, „Eine Liste der Schlüsselbunde (Key Chains) anzeigen“
- Abschnitt 12.7.9.2, „Eine Liste der Schlüssel anzeigen“
- Abschnitt 12.7.9.3, „Ein Schlüsselbund hinzufügen“
- Abschnitt 12.7.9.4, „Hinzufügen eines Schlüssels“
- Abschnitt 12.7.9.5, „Ein Schlüsselbund (Key Chain) löschen“
- Abschnitt 12.7.9.6, „Einen Schlüssel löschen“

Abschnitt 12.7.9.1

Eine Liste der Schlüsselbunde (Key Chains) anzeigen

Um eine Liste der Schlüsselbunde für dynamische RIP-Routen anzusehen, geben Sie Folgendes ein:

```
show running-config routing rip key-chain
```

Falls Schlüsselbunde konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config routing rip key-chain
routing rip
 key-chain key-1
  key 1
   key-string RUGGEDCOM
   accept-lifetime start 2013-01-01T01:01:01-00:00
   accept-lifetime expire 2022-01-01T01:01:01-00:00
   send-lifetime start 2013-01-01T01:01:01-00:00
   send-lifetime expire 2022-01-01T01:01:01-00:00
  !
 !
!
```

Falls keine Schlüsselbunde konfiguriert wurden, fügen Sie je nach Bedarf Schlüsselbunde hinzu. Weitere Informationen finden Sie unter Abschnitt 12.7.9.3, „Ein Schlüsselbund hinzufügen“.

Abschnitt 12.7.9.2
Eine Liste der Schlüssel anzeigen

Um eine Liste der Schlüssel in einem Schlüsselbund anzuzeigen, geben Sie Folgendes ein:

```
show running-config routing rip rip key-chain name key
```

Erläuterung:

- *name* ist die Bezeichnung des Schlüsselbunds

Falls Schlüssel konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config routing rip key-chain key
routing rip
 key-chain key-1
  key 1
   key-string RUGGEDCOM
   accept-lifetime start 2013-01-01T01:01:01-00:00
   accept-lifetime expire 2022-01-01T01:01:01-00:00
   send-lifetime start 2013-01-01T01:01:01-00:00
   send-lifetime expire 2022-01-01T01:01:01-00:00
  !
 !
!
```

Falls keine Schlüssel konfiguriert wurden, fügen Sie je nach Bedarf Schlüssel hinzu. Für weitere Informationen siehe Abschnitt 12.7.9.4, „Hinzufügen eines Schlüssels“.

Abschnitt 12.7.9.3
Ein Schlüsselbund hinzufügen

Um ein Schlüsselbund für dynamisches RIP-Routing hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den Pfad hinzu, indem Sie Folgendes eingeben:

   ```
   routing rip key-chain name
   ```

   Erläuterung:

   - *name* ist die Bezeichnung des Schlüsselbunds
3. Konfigurieren Sie einen oder mehrere Schlüssel für den Schlüsselbund. Für weitere Informationen siehe Abschnitt 12.7.9.4, „Hinzufügen eines Schlüssels“.
4. Konfigurieren Sie eine Routing-Schnittstelle, um den Schlüsselbund zu Authentifizierungszwecken zu verwenden. Für weitere Informationen siehe Abschnitt 12.7.11.2, „Eine Routing-Schnittstelle konfigurieren“.
5. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.7.9.4

Hinzufügen eines Schlüssels

Schlüssel (oder gemeinsame Geheimnisse) werden zur Authentifizierung der Kommunikation über ein RIP-Netzwerk verwendet. Zur Aufrechterhaltung der Netzwerkstabilität wird jedem Schlüssel ein Accept-Lifetime- und ein Send-Lifetime-Parameter zugewiesen.

Der *Accept*-Lifetime-Parameter ist der Zeitraum, in dem der Schlüssel vom Gerät akzeptiert wird.

Der *Send*-Lifetime-Parameter ist der Zeitraum, in dem der Schlüssel anderen Geräten gesendet werden kann.

Dies wird als "Hitless Authentication Key Rollover" bezeichnet; ein Verfahren für die nahtlose Aktualisierung von Authentifizierungsschlüsseln, ohne dass ein Rücksetzen von Netzwerksitzungen erforderlich wird.

Um einen Schlüssel zu einem Schlüsselbund hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den Schlüssel hinzu, indem Sie Folgendes eingeben:

   ```
   routing rip key-chain name key id
   ```

   Erläuterung:

   - *name* ist die Bezeichnung des Schlüsselbunds
   - *id* ist die ID des Schlüssels
3. Konfigurieren Sie die Einstellung für die Bezeichnung des Schlüsselbunds mithilfe der folgenden Parameter:

Parameter	Beschreibung
key-string { key-string }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 1024 Zeichen Legt die Schlüsselzeichenkette fest.

4. Konfigurieren Sie die Accept-Lifetime-Einstellungen mithilfe der folgenden Parameter:

Parameter	Beschreibung
start { start }	**Zusammenfassung:** Eine Zeichenkette Die Anfangszeit, in der der Schlüssel als gültig gilt. **HINWEIS** *Die Start-Zeit kann nicht konfiguriert werden, solange die Expire-Zeit nicht konfiguriert ist,*
expire { expire }	**Zusammenfassung:** { infinite } oder eine Zeichenkette Expire-Zeit. **HINWEIS** *Die Expire-Zeit kann nicht konfiguriert werden, solange die Start-Zeit nicht konfiguriert ist,*

5. Konfigurieren Sie die Send-Lifetime-Einstellungen mithilfe der folgenden Parameter:

Parameter	Beschreibung
start { start }	**Zusammenfassung:** Eine Zeichenkette Legt die Zeitdauer fest, in der der Schlüssel am Schlüsselbund als gültig gilt.

Parameter	Beschreibung
	HINWEIS *Die Start-Zeit kann nicht konfiguriert werden, solange die Expire-Zeit nicht konfiguriert ist,*
expire { expire }	**Zusammenfassung:** { infinite } oder eine Zeichenkette Der Zeitpunkt, zu dem der Schlüssel abläuft. **HINWEIS** *Die Expire-Zeit kann nicht konfiguriert werden, solange die Start-Zeit nicht konfiguriert ist,*

6. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.7.9.5
Ein Schlüsselbund (Key Chain) löschen

Um ein Schlüsselbund (Key Chain) für dynamisches RIP-Routing zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie das Schlüsselbund durch Eingabe von:

```
no routing rip key-chain name
```

Erläuterung:

- *`name`* ist der Name des Schlüsselbunds

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.7.9.6
Einen Schlüssel löschen

Um einen Schlüssel aus einem Schlüsselbund zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den Schlüssel, indem Sie Folgendes eingeben:

```
no routing rip key-chain name key id
```

Erläuterung:

- *`name`* ist die Bezeichnung des Schlüsselbunds
- *`id`* ist die ID des Schlüssels

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.7.10

Umverteilungsmetriken verwalten

Die Umverteilungsmetriken dienen zur Umverteilung von Routing-Informationen von anderen Routing-Protokollen, statischen Routen oder vom Kernel verwalteten Routen. Routen für Subnetze, die direkt mit dem Router verbunden sind, aber kein Teil des RIP-Netzwerks sind, können ebenfalls mitgeteilt werden.

INHALT

- Abschnitt 12.7.10.1, „Eine Liste der Umverteilungsmetriken anzeigen“
- Abschnitt 12.7.10.2, „Eine Umverteilungsmetrik hinzufügen“
- Abschnitt 12.7.10.3, „Eine Umverteilungsmetrik löschen“

Abschnitt 12.7.10.1

Eine Liste der Umverteilungsmetriken anzeigen

Um eine Liste der Umverteilungsmetriken für dynamische RIP-Routen anzusehen, geben Sie Folgendes ein:

```
show running-config routing rip redistribute
```

Falls Metriken konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config routing rip redistribute
routing rip
 redistribute bgp
  no metric
 !
!
```

Falls keine Umverteilungsmetriken konfiguriert wurden, fügen Sie je nach Bedarf Metriken hinzu. Weitere Informationen finden Sie unter Abschnitt 12.7.10.2, „Eine Umverteilungsmetrik hinzufügen“.

Abschnitt 12.7.10.2

Eine Umverteilungsmetrik hinzufügen

Um für dynamische RIP-Routen eine Umverteilungsmetrik hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie die Metrik hinzu, indem Sie Folgendes eingeben:

   ```
   routing rip redistribute [ bgp | ospf | connected | static | kernel ]
   ```

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.7.10.3

Eine Umverteilungsmetrik löschen

Um eine Umverteilungsmetrik für dynamische RIP-Routen zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.

2. Löschen Sie die Metrik durch Eingabe von:

```
no routing rip redistribute [ bgp | ospf | connected | static | kernel ]
```

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.7.11

Routing-Schnittstellen verwalten

Dieser Abschnitt beschreibt, wie Sie Schnittstellen für RIP-Routen verwalten können.

INHALT

- Abschnitt 12.7.11.1, „Eine Liste der Routing-Schnittstellen anzeigen“
- Abschnitt 12.7.11.2, „Eine Routing-Schnittstelle konfigurieren“

Abschnitt 12.7.11.1

Eine Liste der Routing-Schnittstellen anzeigen

Um eine Liste der für ein RIP-Netzwerk konfigurierten Routing-Schnittstellen anzusehen, geben Sie Folgendes ein:

```
show running-config routing rip interface
```

Eine Tabelle oder Liste ähnlich dem folgenden Beispiel wird angezeigt:

```
ruggedcom# show running-config routing rip interface | tab
                   KEY                      RECEIVE  SEND     SPLIT
IFNAME       MODE  CHAIN  STRING  PASSIVE  VERSION  VERSION  HORIZON
-------------------------------------------------------------------------
dummy0       -     -      -       -        -        -        yes
fe-cm-1      -     -      -       -        -        -        yes
switch.0001  -     -      -       -        -        -        yes
```

Abschnitt 12.7.11.2

Eine Routing-Schnittstelle konfigurieren

Um eine Routing-Schnittstelle für ein RIP-Netzwerk zu konfigurieren, gehen Sie wie folgt vor:

HINWEIS
Das Open Shortest Path First (OSPF) erkennt Router-Schnittstellen als passiv oder aktiv an und sendet OSPF-Nachrichten auf aktiven Schnittstellen und ignoriert passive Schnittstellen.

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***routing » rip » interface » {name}***, wobei *{name}* die Bezeichnung der Schnittstelle ist.
3. Konfigurieren Sie die Authentifizierungseinstellungen, indem Sie die folgenden Befehle eingeben:

Parameter	Beschreibung
mode { mode }	**Zusammenfassung:** { md5-rfc, md5-old-ripd, text, none } Der Authentifizierungsmodus.

Parameter	Beschreibung
key-chain { key-chain }	**Zusammenfassung:** Eine Zeichenkette Der Schlüsselbund zur Authentifizierung.
string { string }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 16 Zeichen Die Zeichenkette zur Authentifizierung.

4. Konfigurieren Sie die Schnittstelleneinstellungen, indem Sie die folgenden Befehle eingeben:

Parameter	Beschreibung
{ ifname }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 32 Zeichen Der Name der Schnittstelle.
passive	Die festgelegte Schnittstelle ist in den passiven Modus versetzt. Im passiven Modus werden alle empfangenen Pakete normal verarbeitet und RIPd sendet weder Multicast- noch Unicast-RIP-Pakete, außer an RIP-Nachbarn, die mit einem Nachbarelement spezifiziert wurden.
receive-version { receive-version }	**Zusammenfassung:** { 1, 2, 1,2, 2,1 } Die Version von RIP-Paketen, die an dieser Schnittstelle angenommen werden. Standardmäßig werden Pakete der Version 1 und Version 2 angenommen.
send-version { send-version }	**Zusammenfassung:** { 1, 2, 1,2, 2,1 } Die RIP-Version, mit der Pakete zu senden sind. Standardmäßig werden Pakete der Version 2 gesendet.
split-horizon { split-horizon }	**Zusammenfassung:** { yes, no, poisoned-reverse } **Standard:** yes Ein geteilter Horizont.
mode { mode }	**Zusammenfassung:** { md5-rfc, md5-old-ripd, text, none } Der Authentifizierungsmodus.
key-chain { key-chain }	**Zusammenfassung:** Eine Zeichenkette Der Schlüsselbund zur Authentifizierung.
string { string }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 16 Zeichen Die Zeichenkette zur Authentifizierung.

5. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.8

BGP verwalten

Das Border Gateway Protocol (BGP) ist entsprechend der Definition von RFC 4271 [http://tools.ietf.org/rfc/rfc4271.txt] ein robustes und skalierbares Routing-Protokoll. BGP ist für die Verwaltung einer Routing-Tabelle mit bis zu 90.000 Routen ausgelegt. Daher wird es in großen Netzwerken oder unter Netzwerkgruppen mit gemeinsamen Verwaltungs- und Routingregeln verwendet. Das externe BGP (eBGP) dient zum Austausch von Routen zwischen verschiedenen autonomen Systemen (AS). Das interne BGP (iBGP) dient zum Austausch von Routen innerhalb eines autonomen Systems (AS).

BGP wird vom bgpd-Daemon verwendet, um die Kommunikation mit anderen Routern zu steuern. Der Daemon bestimmt zudem, an welche Router er den Verkehr für jede bekannte Netzwerkroute weiterleiten möchte.

HINWEIS
In komplexen vorhandenen Netzwerken können RIP, OSPF, BGP und IS-IS gleichzeitig auf demselben Router aktiv sein. In der Regel wird jedoch nur ein dynamisches Routingprotokoll zur Zeit verwendet.

INHALT

- Abschnitt 12.8.1, „Konfigurieren von BGP“
- Abschnitt 12.8.2, „Anzeigen des Status von dynamischen BGP-Routen“
- Abschnitt 12.8.3, „Routen-Karten verwalten“
- Abschnitt 12.8.4, „Vorgelagerte und ausgegliederte autonome Systempfadfilter verwalten“
- Abschnitt 12.8.5, „Präfix-Listen und -Einträge verwalten“
- Abschnitt 12.8.6, „Autonome Systempfade und Einträge verwalten“
- Abschnitt 12.8.7, „Nachbarn verwalten“
- Abschnitt 12.8.8, „Netzwerke verwalten“
- Abschnitt 12.8.9, „Sammeladressen verwalten“
- Abschnitt 12.8.10, „Optionen für Sammeladressen verwalten“
- Abschnitt 12.8.11, „Umverteilungsmetriken verwalten“

Abschnitt 12.8.1

Konfigurieren von BGP

Um das dynamische Routing mit BGP zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***routing » bgp*** und konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
enabled	Aktiviert BGP.
as-id { as-id }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 1 und 65535 ID des autonomen Systems.
always-compare-med	Immer MED von verschiedenen Nachbarn vergleichen.
default-local-preference { default-local-preference }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl **Standard:** 100 Standardwert der lokalen Einstellungen.
deterministic-med	Wählt den Pfad "best-MED" unter den Pfaden, die von der benachbarten AS angekündigt werden.
router-id { router-id }	**Zusammenfassung:** Eine Zeichenkette mit 7 bis 15 Zeichen Router-ID für BGP.

3. Konfigurieren Sie autonome Systempfadfilter. Weitere Informationen finden Sie unter Abschnitt 12.8.6.3, „Einen autonomen Systempfadfilter hinzufügen“.
4. Konfigurieren Sie Präfixlistenfilter. Weitere Informationen finden Sie unter Abschnitt 12.8.5.3, „Eine Präfixliste hinzufügen“.

5. Konfigurieren Sie Route-Map-Filter. Weitere Informationen finden Sie unter Abschnitt 12.8.3.3, „Einen Route-Map-Filter hinzufügen“.
6. Konfigurieren Sie ein Netzwerk. Weitere Informationen finden Sie unter Abschnitt 12.8.8.2, „Ein Netzwerk hinzufügen“.
7. Konfigurieren Sie IP-Adressen für Nachbarn. Weitere Informationen finden Sie unter Abschnitt 12.8.7.2, „Einen Nachbarn hinzufügen“.
8. Konfigurieren Sie Sammeladressen. Weitere Informationen finden Sie unter Abschnitt 12.8.9.2, „Eine Sammeladresse hinzufügen“.
9. Konfigurieren Sie Umverteilungsmetriken. Weitere Informationen finden Sie unter Abschnitt 12.8.11.2, „Eine Umverteilungsmetrik hinzufügen“.
10. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.8.2

Anzeigen des Status von dynamischen BGP-Routen

Um den Status der dynamischen BGP-Routen anzuzeigen, geben Sie Folgendes ein:

```
show routing status bgp route
```

Sofern BGP-Routen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show routing status bgp route | tab
                                                                LOCAL               AS
NETWORK       ADDRESS      SELECTED  INTERNAL  METRIC  PREFERENCE  WEIGHT  PATH  ORIGIN
-------------------------------------------------------------------------------------------
192.168.1.0
              192.168.1.2  true      true      0       100         0             IGP
192.168.6.0
              2.0.0.1      true      false     0                   0       200   IGP
192.168.12.0
              192.168.1.2  true      true      0       100         0             IGP
192.168.13.0
              0.0.0.0      true      false     0                   32768         IGP
```

Die Liste liefert die folgenden Informationen:

Parameter	Beschreibung
network	**Zusammenfassung:** Eine Zeichenkette Netzwerk.
next-hop	**Zusammenfassung:** Eine Zeichenkette Adresse des nächsten Hop.
selected	**Zusammenfassung:** { true, false } Für diese Route ausgewählter nächster Hop.
internal	**Zusammenfassung:** { true, false } Interne Route.
metric	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl Metrischer Wert.
local-preference	**Zusammenfassung:** Eine Zeichenkette

Parameter	Beschreibung
	Lokale Einstellungen.
weight	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl Gewicht.
as-path	**Zusammenfassung:** Eine Zeichenkette Pfad.
origin	**Zusammenfassung:** Eine Zeichenkette Ursprungsstelle.

Um den Status des dynamischen BGP-Nachbarn anzuzeigen, geben Sie Folgendes ein:

```
show routing status bgp neighbor
```

Falls BGP-Nachbarn konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show routing status bgp neighbor | tab
                                                                    PREFIX
                              LOCAL              AS
ID          VERSION  AS    MSGRCVD  MSGSENT  UPTIME    STATE       RECEIVED  NETWORK        NEXT HOP
  SELECTED  INTERNAL  METRIC  PREFERENCE  WEIGHT  PATH  ORIGIN
-------------------------------------------------------------------------------------------------------
13.13.13.2  4        2122  982      984      16:18:04  Established  2
                                                                              13.13.13.0/30  13.13.13.1
  true      false     0                  32768         IGP
                                                                              192.168.12.0   13.13.13.1
  true      false     2                  32768         Unspecified
```

Die Liste liefert die folgenden Informationen:

Parameter	Beschreibung
id	**Zusammenfassung:** Eine Zeichenkette Nachbar-Adresse.
version	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl BGP-Version.
as	**Zusammenfassung:** Eine Zeichenkette Entfernte AS-Nummer.
msgrcvd	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl Anzahl erhaltener BGP-Nachrichten.
msgsent	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl Anzahl gesendeter BGP-Nachrichten.
uptime	**Zusammenfassung:** Eine Zeichenkette Klarzeit des Peers.
state	**Zusammenfassung:** Eine Zeichenkette Verbindungszustand mit diesem Nachbarn.
prefix-received	**Zusammenfassung:** Eine Zeichenkette Anzahl der von diesem Nachbarn empfangenen Präfixe (Netzwerke).

Parameter	Beschreibung
network	**Zusammenfassung:** Eine Zeichenkette

Parameter	Beschreibung
	Netzwerk.
next-hop	**Zusammenfassung:** Eine Zeichenkette Adresse des nächsten Hop.
selected	**Zusammenfassung:** { true, false } Für diese Route ausgewählter nächster Hop.
internal	**Zusammenfassung:** { true, false } Interne Route.
metric	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl Metrischer Wert.
local-preference	**Zusammenfassung:** Eine Zeichenkette Lokale Einstellungen.
weight	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl Gewicht.
as-path	**Zusammenfassung:** Eine Zeichenkette Pfad.
origin	**Zusammenfassung:** Eine Zeichenkette Ursprungsstelle.

Falls keine dynamischen BGP-Routen konfiguriert wurden, konfigurieren Sie BGP und fügen Sie nach Bedarf Routen hinzu. Weitere Informationen über das Konfigurieren von BGP finden Sie in Abschnitt 12.8.1, „Konfigurieren von BGP“.

Abschnitt 12.8.3

Routen-Karten verwalten

Routen-Karten sind sequentielle Anweisungen für die Filterung der Routen, die bestimmte Kriterien erfüllen. Erfüllt eine Route die Kriterien der angewandten Routen-Karte, so kann sie entweder aus der Routing-Tabelle ausgeschlossen oder gegen Umverteilung gesperrt werden.

Jede Routen-Karte erfordert eine fortlaufende Nummer (z. B. 10, 20, 30 usw.), mit der mehrere Routen-Karten nacheinander abgearbeitet werden können, bis ein Treffer gefunden wird. Es wird empfohlen, fortlaufende Nummern in 10er-Schritten anzulegen, falls später eine neue Routen-Karte zwischen zwei vorhandene Karten eingefügt werden muss.

INHALT

- Abschnitt 12.8.3.1, „Eine Liste der Route-Map-Filter anzeigen“
- Abschnitt 12.8.3.2, „Eine Liste der Einträge im Route-Map-Filter anzeigen“
- Abschnitt 12.8.3.3, „Einen Route-Map-Filter hinzufügen“
- Abschnitt 12.8.3.4, „Einen Eintrag für einen Route-Map-Filter hinzufügen“
- Abschnitt 12.8.3.5, „Einen Route-Map-Filter löschen“
- Abschnitt 12.8.3.6, „Einen Eintrag im Route-Map-Filter löschen“
- Abschnitt 12.8.3.7, „Konfigurieren von Übereinstimmungsregeln“

- Abschnitt 12.8.3.8, „Konfigurieren eines Satzes“

Abschnitt 12.8.3.1
Eine Liste der Route-Map-Filter anzeigen

Um eine Liste der Route-Map-Filter für jedes dynamische BGP anzuzeigen, geben Sie Folgendes ein:

```
show running-config routing bgp filter route-map
```

Falls Filter konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config routing bgp filter route-map | tab
                        ON
                        MATCH  AS    PREFIX  PREFIX  PREFIX                              LOCAL
                  NEXT          ORIGINATOR
TAG  SEQ  ACTION  CALL  GOTO    PATH  LIST    LIST    METRIC  PEER  ORIGIN  AS  IP  PREFERENCE
 OPERATION  VALUE  HOP   ORIGIN  ID          WEIGHT
-------------------------------------------------------------------------------------------
map
     10   permit  -     -      -     -       -       -       -       -     -       -   -   -
 -          -      -     -       -           -

!
```

Falls keine Filter konfiguriert wurden, fügen Sie je nach Bedarf Filter hinzu. Weitere Informationen finden Sie unter Abschnitt 12.8.6.3, „Einen autonomen Systempfadfilter hinzufügen“.

Abschnitt 12.8.3.2
Eine Liste der Einträge im Route-Map-Filter anzeigen

Um eine Liste der Einträge im Route-Map-Filter für jedes BGP anzuzeigen, geben Sie Folgendes ein:

```
show running-config routing bgp filter route-map tag entry
```

Erläuterung:

- *tag* ist die Variable für den Route-Map-Filter

Falls Einträge konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config routing bgp filter route-map map entry | tab
                   ON
                   MATCH  AS    PREFIX  PREFIX  PREFIX                                  LOCAL
             NEXT          ORIGINATOR
SEQ  ACTION  CALL  GOTO    PATH  LIST    LIST    LIST    METRIC  PEER  ORIGIN  AS  IP  PREFERENCE
 OPERATION  VALUE  HOP   ORIGIN  ID          WEIGHT  AS
-----------------------------------------------------------------------------------------------
10   permit  -     -      -     -       -       -       -       -     -       -   -   -          -
      -      -     -       -           -

 !
!
```

Falls keine Filter konfiguriert wurden, fügen Sie je nach Bedarf Filter hinzu. Weitere Informationen finden Sie unter Abschnitt 12.8.6.3, „Einen autonomen Systempfadfilter hinzufügen“.

Abschnitt 12.8.3.3

Einen Route-Map-Filter hinzufügen

Um für dynamische BGP-Routen einen Route-Map-Filter hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den neuen Filter hinzu, indem Sie Folgendes eingeben:

   ```
   routing bgp filter route-map tag
   ```

   Erläuterung:

   - *tag* ist die Variable für den Route-Map-Filter
3. Fügen Sie einen oder mehrere Einträge hinzu. Für weitere Informationen siehe Abschnitt 12.8.3.4, „Einen Eintrag für einen Route-Map-Filter hinzufügen“.
4. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.8.3.4

Einen Eintrag für einen Route-Map-Filter hinzufügen

Um einen Eintrag für einen Route-Map-Filter hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den neuen Filter hinzu, indem Sie Folgendes eingeben:

   ```
   routing bgp filter route-map tag entry number
   ```

   Erläuterung:

   - *tag* ist die Variable für den Route-Map-Filter
   - *number* ist die Sequenznummer für den Eintrag
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
action { action }	**Zusammenfassung:** { deny, permit } **Standard:** permit Vorgang.
call { call }	**Zusammenfassung:** Eine Zeichenkette Springt nach "match+set" zu einer anderen Route-Map.
on-match-goto { on-match-goto }	**Zusammenfassung:** Eine Zeichenkette Zu diesem übereinstimmenden Eintrag gehen.

4. Konfigurieren Sie die Übereinstimmungsregeln für den Route-Map-Filter. Weitere Informationen finden Sie unter Abschnitt 12.8.3.7, „Konfigurieren von Übereinstimmungsregeln“.
5. Konfigurieren Sie einen Datensatz für den Route-Map-Filter. Weitere Informationen finden Sie unter Abschnitt 12.8.3.8, „Konfigurieren eines Satzes“.
6. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.8.3.5
Einen Route-Map-Filter löschen

Um einen Route-Map-Filter für dynamische BGP-Routen zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den Filterschlüssel, indem Sie Folgendes eingeben:

   ```
   no routing bgp filter route-map tag
   ```

   Erläuterung:

   - *tag* ist die Variable für den Route-Map-Filter
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.8.3.6
Einen Eintrag im Route-Map-Filter löschen

Um einen Eintrag im Route-Map-Filter zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den Filterschlüssel, indem Sie Folgendes eingeben:

   ```
   no routing bgp filter route-map tag entry number
   ```

   Erläuterung:

   - *tag* ist die Variable für den Route-Map-Filter
   - *number* ist die Sequenznummer für den Eintrag
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.8.3.7
Konfigurieren von Übereinstimmungsregeln

Um Übereinstimmungsregeln für einen Eintrag im Route-Map-Filter zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***routing » bgp » filter » route-map » {tag} » entry » {number} » match***, wobei *{tag}* die Variable für den Route-Map-Filter und *{number}* die Sequenznummer für den Eintrag ist.
3. Konfigurieren Sie je nach Bedarf die folgenden Parameter:

Parameter	Beschreibung
as-path { as-path }	**Zusammenfassung:** Eine Zeichenkette BGP-AS-Pfadfilter abgleichen.
metric { metric }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Routen-Metrik abgleichen.
peer { peer }	**Zusammenfassung:** Eine Zeichenkette mit 7 bis 15 Zeichen

Parameter	Beschreibung
	Dieser Parameter wird nicht unterstützt und sämtliche Werte werden vom System ignoriert.
origin { origin }	**Zusammenfassung:** { egp, igp, incomplete } BGP-Ursprungscode abgleichen.

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.8.3.8
Konfigurieren eines Satzes

Um Übereinstimmungsregeln für einen Eintrag im Route-Map-Filter zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***routing » bgp » filter » route-map » {tag} » entry » {number} » set***, wobei *{tag}* die Variable für den Route-Map-Filter und *{number}* die Sequenznummer für den Eintrag ist.
3. Konfigurieren Sie je nach Bedarf die folgenden Parameter:

Parameter	Beschreibung
local-preference { local-preference }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Lokale Einstellungen.
next-hop { next-hop }	**Zusammenfassung:** { peer } oder eine Zeichenkette mit 7 bis 15 Zeichen Die Adresse des nächsten Hops (xxx.xxx.xxx.xxx/xx oder Peer zur Verwendung der Peer-Adresse).
origin { origin }	**Zusammenfassung:** { egp, igp, incomplete } Der Ursprungscode.
originator-id { originator-id }	**Zusammenfassung:** Eine Zeichenkette mit 7 bis 15 Zeichen Dieser Parameter wird nicht unterstützt und sämtliche Werte werden vom System ignoriert.
weight { weight }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Gewicht.

4. Fügen Sie vorangestellte und/oder ausgeschlossene autonome Systempfade hinzu. Weitere Informationen finden Sie unter Abschnitt 12.8.4.3, „Einen vorgelagerten autonomen Systempfadfilter hinzufügen“ und/oder Abschnitt 12.8.4.4, „Einen ausgegliederten autonomen Systempfadfilter hinzufügen“.
5. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.8.4

Vorgelagerte und ausgegliederte autonome Systempfadfilter verwalten

Dieser Abschnitt beschreibt, wie Sie vorgelagerte und ausgegliederte autonome Systempfadfilter konfigurieren und verwalten können.

INHALT

- Abschnitt 12.8.4.1, „Eine Liste der vorgelagerten autonomen Systempfadfilter anzeigen“
- Abschnitt 12.8.4.2, „Eine Liste der ausgegliederten autonomen Systempfade anzeigen“
- Abschnitt 12.8.4.3, „Einen vorgelagerten autonomen Systempfadfilter hinzufügen“
- Abschnitt 12.8.4.4, „Einen ausgegliederten autonomen Systempfadfilter hinzufügen“
- Abschnitt 12.8.4.5, „Einen vorgelagerten autonomen Systempfadfilter löschen“
- Abschnitt 12.8.4.6, „Einen ausgegliederten autonomen Systempfadfilter löschen“

Abschnitt 12.8.4.1

Eine Liste der vorgelagerten autonomen Systempfadfilter anzeigen

Um eine Liste der vorgelagerten autonomen Systempfadfilter, die für einen BGP-Route-Map-Eintrag konfiguriert wurden, anzuzeigen, geben Sie Folgendes ein:

```
show running-config routing bgp filter route-map name entry number set as-path prepend
```

Erläuterung:

- *name* ist die Bezeichnung der Route-Map
- *number* ist die Eintragsnummer

Falls Filter konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config routing bgp filter route-map route entry 10 set as-path prepend
routing bgp
 filter route-map route
  entry 10
   set as-path prepend 120
   !
  !
 !
!
```

Falls keine vorgelagerten autonomen Systempfadfilter konfiguriert wurden, fügen Sie je nach Bedarf Filter hinzu. Weitere Informationen finden Sie unter Abschnitt 12.8.4.3, „Einen vorgelagerten autonomen Systempfadfilter hinzufügen“.

Abschnitt 12.8.4.2

Eine Liste der ausgegliederten autonomen Systempfade anzeigen

Um eine Liste der ausgegliederten autonomen Systempfadfilter, die für einen BGP-Route-Map-Eintrag konfiguriert wurden, anzuzeigen, geben Sie Folgendes ein:

```
show running-config routing bgp filter route-map name entry number set as-path exclude
```

Erläuterung:

- *name* ist die Bezeichnung der Route-Map
- *number* ist die Eintragsnummer

Falls Filter konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config routing bgp filter route-map route entry 10 set as-path exclude
routing bgp
 filter route-map route
  entry 10
   set as-path exclude 110
   !
  !
 !
!
```

Falls keine ausgegliederten autonomen Systempfadfilter konfiguriert wurden, fügen Sie je nach Bedarf Filter hinzu. Weitere Informationen finden Sie unter Abschnitt 12.8.4.4, „Einen ausgegliederten autonomen Systempfadfilter hinzufügen“.

Abschnitt 12.8.4.3

Einen vorgelagerten autonomen Systempfadfilter hinzufügen

Um einen vorgelagerten autonomen Systempfadfilter zu einem BGP-Route-Map-Eintrag hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den Pfad hinzu, indem Sie Folgendes eingeben:

   ```
   routing bgp filter route-map name entry number set as-path prepend path
   ```

   Erläuterung:

   - *name* ist die Bezeichnung der Route-Map
   - *number* ist die Eintragsnummer
   - *path* ist die Nummer für den autonomen Systempfad
3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.8.4.4

Einen ausgegliederten autonomen Systempfadfilter hinzufügen

Um einen ausgegliederten autonomen Systempfadfilter zu einem BGP-Route-Map-Eintrag hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den Pfad hinzu, indem Sie Folgendes eingeben:

   ```
   routing bgp filter route-map name entry number set as-path exclude path
   ```

   Erläuterung:

- *name* ist die Bezeichnung der Route-Map
- *number* ist die Eintragsnummer
- *path* ist die Nummer für den autonomen Systempfad

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.8.4.5
Einen vorgelagerten autonomen Systempfadfilter löschen

Um einen vorgelagerten autonomen Systempfadfilter aus einem BGP-Route-Map-Eintrag zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie das Netzwerk, indem Sie Folgendes eingeben:

```
no routing bgp filter route-map name entry number set as-path prepend path
```

Erläuterung:

- *name* ist die Bezeichnung der Route-Map
- *number* ist die Eintragsnummer
- *path* ist die Nummer für den autonomen Systempfad

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.8.4.6
Einen ausgegliederten autonomen Systempfadfilter löschen

Um einen ausgegliederten autonomen Systempfadfilter aus einem BGP-Route-Map-Eintrag zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie das Netzwerk, indem Sie Folgendes eingeben:

```
no routing bgp filter route-map name entry number set as-path exclude path
```

Erläuterung:

- *name* ist die Bezeichnung der Route-Map
- *number* ist die Eintragsnummer
- *path* ist die Nummer für den autonomen Systempfad

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.8.5

Präfix-Listen und -Einträge verwalten

Nachbarn können Präfix-Listen zugeordnet werden, die dem BGP-Daemon die Filterung eingehender oder abgehender Routen auf Grund der Einträge *allow* und *deny* in der Präfix-Liste ermöglichen.

INHALT

- Abschnitt 12.8.5.1, „Eine Liste der Präfixeinträge anzeigen“
- Abschnitt 12.8.5.2, „Eine Liste der Präfixeinträge anzeigen“
- Abschnitt 12.8.5.3, „Eine Präfixliste hinzufügen“
- Abschnitt 12.8.5.4, „Einen Präfixeintrag hinzufügen“
- Abschnitt 12.8.5.5, „Eine Präfixliste löschen“
- Abschnitt 12.8.5.6, „Einen Präfixeintrag löschen“

Abschnitt 12.8.5.1

Eine Liste der Präfixeinträge anzeigen

Um eine Liste der Präfixeinträge für dynamische BGP-Routen anzusehen, geben Sie Folgendes ein:

```
routing bgp filter prefix-list
```

Falls Präfixlisten konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config routing bgp filter prefix-list | tab
NAME                  DESCBGPTION  SEQ  ACTION  SUBNET           LE  GE
-------------------------------------------------------------------------
list-permit-lan-22    -
                                   100  permit  192.168.33.0/24  -   -
list-withdraw-lan-11  -
                                   100  permit  192.168.33.0/24  -   -
                                   200  permit  192.168.33.0/24  32  -

!
```

Falls keine Präfixlisten konfiguriert wurden, fügen Sie je nach Bedarf Listen hinzu. Weitere Informationen finden Sie unter Abschnitt 12.8.5.3, „Eine Präfixliste hinzufügen“.

Abschnitt 12.8.5.2

Eine Liste der Präfixeinträge anzeigen

Um eine Liste von Einträgen für dynamisches BGP, OSPF oder BGP-Präfixlisten anzuzeigen, geben Sie Folgendes ein:

```
routing bgp filter prefix-list name entry
```

Erläuterung:

- *name* ist die Bezeichnung der Präfixliste

Falls Einträge konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config routing bgp filter prefix-list test entry | tab
SEQ  ACTION  SUBNET           LE  GE
```

```
-------------------------------------------
5    permit  192.168.40.0/24  32  -
6    deny    192.168.5.21/32     -   -

 !
!
```

Falls keine Einträge konfiguriert wurden, fügen Sie je nach Bedarf Einträge hinzu. Weitere Informationen finden Sie unter Abschnitt 12.8.5.4, „Einen Präfixeintrag hinzufügen“.

Abschnitt 12.8.5.3
Eine Präfixliste hinzufügen

Um eine Präfixliste für dynamische BGP-Routen hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie die Liste hinzu, indem Sie Folgendes eingeben:

   ```
   routing bgp filter prefix-list name
   ```

   Erläuterung:

   - *name* ist die Bezeichnung der Präfixliste
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
description { description }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 1024 Zeichen Die Beschreibung der Präfixliste.

4. Fügen Sie nach Bedarf Präfixeinträge hinzu. Weitere Informationen finden Sie unter Abschnitt 12.8.5.4, „Einen Präfixeintrag hinzufügen“.
5. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.8.5.4
Einen Präfixeintrag hinzufügen

Um einen Eintrag in die Präfixliste eines dynamischen BGP hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den Eintrag hinzu, indem Sie Folgendes eingeben:

   ```
   routing bgp filter prefix-list name entry number
   ```

   Erläuterung:

   - *name* ist die Bezeichnung der Präfixliste
   - *number* ist die Sequenznummer für den Eintrag
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
action { action }	**Zusammenfassung:** { deny, permit } **Standard:** permit

Parameter	Beschreibung
	Vorgang.
subnet { subnet }	**Zusammenfassung:** Eine Zeichenkette mit 9 bis 18 Zeichen Netzwerk (xxx.xxx.xxx.xxx/xx). Dieser Parameter ist obligatorisch.
le { le }	**Zusammenfassung:** Eine vorzeichenlose 8-Bit-Ganzzahl zwischen 1 und 32 Die maximale Präfixlänge, um IP-Adresse im Subnetz anzupassen.
ge { ge }	**Zusammenfassung:** Eine vorzeichenlose 8-Bit-Ganzzahl zwischen 1 und 32 Die minimale Präfixlänge, um IP-Adresse im Subnetz anzupassen.

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.8.5.5
Eine Präfixliste löschen

Um eine Präfixliste für dynamische BGP-Routen zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.

   HINWEIS
   Beim Löschen einer Präfixliste werden gleichzeitig alle zugehörigen Präfixe entfernt.

2. Löschen Sie die Liste, indem Sie Folgendes eingeben:

   ```
   no routing bgp filter prefix-list name
   ```

   Erläuterung:

   - *`name`* ist die Bezeichnung der Präfixliste

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.8.5.6
Einen Präfixeintrag löschen

Um einen Eintrag in der Präfixliste eines dynamischen BGP zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den Eintrag, indem Sie Folgendes eingeben:

   ```
   no routing bgp filter prefix-list name entry number
   ```

   Erläuterung:

   - *`name`* ist die Bezeichnung der Präfixliste
   - *`number`* ist die Sequenznummer für den Eintrag

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.8.6

Autonome Systempfade und Einträge verwalten

Dieser Abschnitt beschreibt, wie Sie autonome Systempfade und Einträge für dynamische BGP-Routen konfigurieren können.

INHALT

- Abschnitt 12.8.6.1, „Eine Liste der autonomen Systempfade anzeigen“
- Abschnitt 12.8.6.2, „Eine Liste der autonomen Systempfadeinträge anzeigen“
- Abschnitt 12.8.6.3, „Einen autonomen Systempfadfilter hinzufügen“
- Abschnitt 12.8.6.4, „Hinzufügen eines Eintrags für einen autonomen Systempfadfilter“
- Abschnitt 12.8.6.5, „Einen autonomen Systempfadfilter löschen“
- Abschnitt 12.8.6.6, „Einen Eintrag für einen autonomen Systempfadfilter löschen“

Abschnitt 12.8.6.1

Eine Liste der autonomen Systempfade anzeigen

Um eine Liste der autonomen Systempfadfilter für dynamische BGP-Routen anzusehen, geben Sie Folgendes ein:

```
show running-config routing bgp filter as-path
```

Falls Filter konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config routing bgp filter as-path | tab
NAME              ACTION  MATCH
----------------------------------
filter-allow-120
                  permit  120

!
```

Falls keine Filter konfiguriert wurden, fügen Sie je nach Bedarf Filter hinzu. Weitere Informationen finden Sie unter Abschnitt 12.8.6.3, „Einen autonomen Systempfadfilter hinzufügen“.

Abschnitt 12.8.6.2

Eine Liste der autonomen Systempfadeinträge anzeigen

Um eine Liste der Einträge für einen autonomen Systempfadfilter anzusehen, geben Sie Folgendes ein:

```
show running-config routing bgp filter as-path name entry
```

Erläuterung:

- *name* ist die Bezeichnung des autonomen Systempfadfilters

Falls Einträge konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config routing bgp filter as-path filter-allow-120 entry | tab
ACTION  MATCH
---------------
permit  120

 !
```

```
!
```

Falls keine Filter konfiguriert wurden, fügen Sie je nach Bedarf Filter hinzu. Weitere Informationen finden Sie unter Abschnitt 12.8.6.3, „Einen autonomen Systempfadfilter hinzufügen“.

Abschnitt 12.8.6.3

Einen autonomen Systempfadfilter hinzufügen

Um einen autonomen Systempfadfilter für dynamische BGP-Routen hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den neuen Filter hinzu, indem Sie Folgendes eingeben:

   ```
   routing bgp filter as-path name
   ```

   Erläuterung:

   - *name* ist die Bezeichnung des autonomen Systempfadfilters
3. Fügen Sie einen oder mehrere Einträge hinzu. Für weitere Informationen siehe Abschnitt 12.8.6.4, „Hinzufügen eines Eintrags für einen autonomen Systempfadfilter“.
4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.8.6.4

Hinzufügen eines Eintrags für einen autonomen Systempfadfilter

Erstellen Sie einen Eintrag für einen autonomen Systempfadfilter, der mit einem String- oder Integer-Wert im AS-Pfad übereinstimmt, und führen Sie anschließend eine Aktion aus. Die Übereinstimmungskriterien werden mithilfe regulärer Ausdrücke definiert.

Um einen Eintrag für einen autonomen Systempfadfilter hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den neuen Filter hinzu, indem Sie Folgendes eingeben:

   ```
   routing bgp filter as-path name entry action match
   ```

   Erläuterung:

   - *name* ist die Bezeichnung des autonomen Systempfadfilters.
   - *action* ist die Aktion.
   - *match* ist der reguläre Ausdruck, der mit dem autonomen Systempfadfilter übereinstimmt. Weitere Informationen über reguläre Ausdrücke finden Sie in Abschnitt 2.5.7, „Verwenden von regulären Ausdrücken“.
3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.8.6.5

Einen autonomen Systempfadfilter löschen

Um einen autonomen Systempfadfilter für dynamische BGP-Routen zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den Filterschlüssel, indem Sie Folgendes eingeben:

   ```
   no routing bgp filter as-path name
   ```

   Erläuterung:

   - *name* ist die Bezeichnung des autonomen Systempfadfilters
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.8.6.6

Einen Eintrag für einen autonomen Systempfadfilter löschen

Um einen Eintrag für einen autonomen Systempfadfilter zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den Filterschlüssel, indem Sie Folgendes eingeben:

   ```
   no routing bgp filter as-path name entry action match
   ```

   Erläuterung:

   - *name* ist die Bezeichnung des autonomen Systempfadfilters
   - *action* ist die Aktion
   - *match* ist der reguläre Ausdruck, der mit dem autonomen Systempfadfilter übereinstimmt
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.8.7

Nachbarn verwalten

Nachbarn sind andere Router, mit denen Routen ausgetauscht werden. Damit BGP funktionieren kann, müssen ein oder mehrere Nachbarn angegeben werden.

HINWEIS
Wenn Nachbarn, aber keine Netzwerke angegeben sind, empfängt der Router BGP-Routing-Informationen von seinen Nachbarn, leitet aber keine Routen zu ihnen. Weitere Informationen über Netzwerke finden Sie unter Abschnitt 12.8.8, „Netzwerke verwalten“.

INHALT

- Abschnitt 12.8.7.1, „Eine Liste der Nachbarn anzeigen“
- Abschnitt 12.8.7.2, „Einen Nachbarn hinzufügen“
- Abschnitt 12.8.7.3, „Konfigurieren der Verteilung von Präfixlisten“
- Abschnitt 12.8.7.4, „Nachverfolgen von Befehlen für BGP-Nachbarn“
- Abschnitt 12.8.7.5, „Einen Nachbarn löschen“

Abschnitt 12.8.7.1
Eine Liste der Nachbarn anzeigen

Um eine Liste der für ein BGP-Netzwerk konfigurierten Nachbarn anzusehen, geben Sie Folgendes ein:

```
show running-config routing bgp neighbor
```

Falls Nachbarn konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config routing bgp neighbor
routing bgp
 neighbor 192.168.123.3
  remote-as 100
  no ebgp-multihop
  no maximum-prefix
  no next-hop-self
  no password
  no route-map in
  no route-map out
  no soft-reconfiguration
  no weight
 !
!
```

Falls keine Nachbarn konfiguriert wurden, fügen Sie je nach Bedarf Nachbarn hinzu. Weitere Informationen finden Sie unter Abschnitt 12.8.7.2, „Einen Nachbarn hinzufügen“.

Abschnitt 12.8.7.2
Einen Nachbarn hinzufügen

Um einem BGP-Netzwerk einen Nachbarn hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den Nachbarn hinzu, indem Sie Folgendes eingeben:

   ```
   routing bgp neighbor address
   ```

   Erläuterung:

   - *address* ist die IP-Adresse des Nachbarn
3. Konfigurieren Sie die Route Map-Einstellungen mithilfe der folgenden Parameter:

Parameter	Beschreibung
in { in }	**Zusammenfassung:** Eine Zeichenkette Route-Map auf eingehende Routen anwenden.
out { out }	**Zusammenfassung:** Eine Zeichenkette Route-Map auf ausgehende Routen anwenden.

4. Konfigurieren Sie die Neighbor-Einstellungen mithilfe der folgenden Parameter:

Parameter	Beschreibung
remote-as { remote-as }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 1 und 65535 Ein BGP-Nachbar. Dieser Parameter ist obligatorisch.
ebgp-multihop { ebgp-multihop }	**Zusammenfassung:** Eine vorzeichenlose 8-Bit-Ganzzahl zwischen 1 und 255

Parameter	Beschreibung
	Die maximale Hop-Zählung. Dadurch sind EBGP-Nachbarn an nicht direkt verbundenen Netzwerken zulässig.
maximum-prefix { maximum-prefix }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 1 und 4294967295 Die maximale Präfixnummer, die von diesem Peer angenommen wird.
next-hop-self	Deaktiviert die Berechnung des nächsten Hops für diesen Nachbarn.
password { password }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 1024 Zeichen Passwort.
update-source { update-source }	**Zusammenfassung:** Eine Zeichenkette mit 7 bis 15 Zeichen IP-Quelladresse von Routing-Updates.
disable-connected-check	Deaktiviert die Verbindungsüberprüfung beim Einrichten einer eBGP-Peering-Sitzung mit einem Single-Hop-Peer, der eine Loopback-Schnittstelle verwendet.
soft-reconfiguration	Soft-Rekonfiguration je Nachbar.
weight { weight }	**Zusammenfassung:** Eine vorzeichenlose 16-Bit-Ganzzahl Das Standardgewicht für Routen von diesem Nachbarn.

5. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.8.7.3
Konfigurieren der Verteilung von Präfixlisten

Um die Verteilung von Präfixlisten für einen Nachbarn in einem BGP-Netzwerk zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Übernehmen Sie die gewünschte Präfixliste in die gewählte Routenrichtung, indem Sie Folgendes eingeben:

   ```
   routing bgp neighbor address distribute-prefix-list [ in | out ] prefix-list prefix
   ```

   Erläuterung:

   - *`address`* ist die Adresse des gewählten Nachbarn
   - *`prefix`* ist die gewählte BGP-Präfixliste
3. Konfigurieren Sie bei Bedarf einen Event Tracker, um die Netzwerkbefehle zu beobachten. Weitere Informationen finden Sie unter Abschnitt 12.8.7.4, „Nachverfolgen von Befehlen für BGP-Nachbarn“.
4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.8.7.4
Nachverfolgen von Befehlen für BGP-Nachbarn

Netzwerkbefehle lassen sich mithilfe von Event Trackern, die unter ***global » tracking*** konfiguriert werden, nachverfolgen. Weitere Informationen über Event Tracker finden Sie in Abschnitt 12.5, „Event-Tracker verwalten“.

Ein Netzwerkbefehl wird in Abhängigkeit vom Status des Event Trackers aktiviert. Der Parameter `apply-when` bestimmt, wann der Befehl aktiviert wird. Beispiel: Wenn der Parameter `apply-when` auf **`down`**gesetzt ist,

wird der Netzwerkbefehl aktiv (und kündigt dadurch das Netzwerk den BGP-Peers eines Routers an), wenn das nachverfolgte Ziel nicht verfügbar ist.

Um einen Befehl für einen BGP-Nachbarn nachzuverfolgen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***routing » dynamic » bgp » neighbor » {address}***, wobei *{address}* die IP-Subnetzadresse und das Präfix für den Nachbarn ist.
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
event { event }	**Zusammenfassung:** Eine Zeichenkette Markiert das Tracken eines Ereignisses, wobei die "distribute-prefix-list" nur anzuwenden ist, wenn das getrackte Ereignis verfügbar ("UP") wird. Dieser Parameter ist obligatorisch.
apply-when { apply-when }	**Zusammenfassung:** { up, down } **Standard:** up Wendet die "distribute-prefix-list" an, wenn das getrackte Ereignis verfügbar ("UP") oder nicht verfügbar ("DOWN") wird.

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.8.7.5
Einen Nachbarn löschen

Um einen Nachbarn in einem BGP-Netzwerk zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie das Netzwerk durch Eingabe von:

```
no routing bgp neighbor address
```

Erläuterung:

- *`address`* ist die IP-Adresse des Nachbarn

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.8.8
Netzwerke verwalten

Im Gegensatz zu den Nachbarn, bei denen es sich um spezifische Router handelt, mit denen Routen ausgetauscht werden, sind Netzwerke Gruppen von Routern, die entweder Teil eines bestimmten Subnetzes sind oder mit einer bestimmten Netzwerkschnittstelle verbunden sind. Sie können gleichzeitig als Nachbarn genutzt werden.

HINWEIS
Bei Punkt-zu-Punkt-Verbindungen legen Sie anstelle eines Netzwerks Nachbarn fest. Weitere Informationen finden Sie unter Abschnitt 12.8.7.2, „Einen Nachbarn hinzufügen“.

HINWEIS
Netze für das BGP-Protokoll benötigen keinen gültigen Eintrag in der Routing-Tabelle. Da BGP ein breiteres Gateway-Protokoll ist, wird in der Regel eine allgemeinere Netzwerkspezifikation eingegeben. Wenn zum Beispiel ein geroutetes Netz innerhalb des autonomen Systems (AS) aus vielen verschiedenen Subnetzen der Klasse C (/24) des Bereichs 192.168.0.0/16 bestand, ist es effizienter, die eine Netzspezifikation der Klasse B, 192.168.0.0/16, seinen BGP-Nachbarn anzukündigen.

HINWEIS
Wenn Nachbarn, aber keine Netzwerke angegeben sind, empfängt der Router Routing-Informationen von seinen Nachbarn, kündigt ihnen aber keine Routen an. Weitere Informationen über Nachbarn finden Sie unter Abschnitt 12.8.7, „Nachbarn verwalten“.

INHALT

- Abschnitt 12.8.8.1, „Eine Liste der Netzwerke anzeigen“
- Abschnitt 12.8.8.2, „Ein Netzwerk hinzufügen“
- Abschnitt 12.8.8.3, „Nachverfolgen von Befehlen für ein BGP-Netzwerk“
- Abschnitt 12.8.8.4, „Ein Netzwerk löschen“

Abschnitt 12.8.8.1

Eine Liste der Netzwerke anzeigen

Um eine Liste der für das BGP-Protokoll konfigurierten Netzwerke anzusehen, geben Sie Folgendes ein:

```
show running-config routing bgp network
```

Falls Netzwerke konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config routing bgp network
routing bgp
 network 192.168.12.0/24
 !
 network 192.168.123.0/24
 !
!
```

Falls keine Netzwerke konfiguriert wurden, fügen Sie nach Bedarf Netzwerke hinzu. Weitere Informationen finden Sie unter Abschnitt 12.8.8.2, „Ein Netzwerk hinzufügen“.

Abschnitt 12.8.8.2

Ein Netzwerk hinzufügen

Um ein neues Netzwerk zum BGP-Protokoll hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie das Netzwerk hinzu, indem Sie Folgendes eingeben:

   ```
   routing bgp network address
   ```

   Erläuterung:

   - *address* ist die IP-Subnetzadresse und das Präfix für das Netzwerk

3. Konfigurieren Sie bei Bedarf einen Event Tracker, um die Netzwerkbefehle zu beobachten. Für weitere Informationen siehe Abschnitt 12.8.8.3, „Nachverfolgen von Befehlen für ein BGP-Netzwerk“.
4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.8.8.3
Nachverfolgen von Befehlen für ein BGP-Netzwerk

Netzwerkbefehle lassen sich mithilfe von Event Trackern, die unter ***global » tracking*** konfiguriert werden, nachverfolgen. Weitere Informationen über Event Tracker finden Sie in Abschnitt 12.5, „Event-Tracker verwalten“.

Ein Netzwerkbefehl wird in Abhängigkeit vom Status des Event Trackers aktiviert. Der Parameter `apply-when` bestimmt, wann der Befehl aktiviert wird. Beispiel: Wenn der Parameter `apply-when` auf **`down`**gesetzt ist, wird der Netzwerkbefehl aktiv (und kündigt dadurch das Netzwerk den BGP-Peers eines Routers an), wenn das nachverfolgte Ziel nicht verfügbar ist.

Um einen Befehl für ein BGP-Netzwerk nachzuverfolgen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***routing » bgp » network » {address} » track***, wobei *{address}* die IP-Subnetzadresse und das Präfix für das Netzwerk ist.
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
event { event }	**Zusammenfassung:** Eine Zeichenkette Ein Ereignis wählen. Dieser Parameter ist obligatorisch.
apply-when { apply-when }	**Zusammenfassung:** { up, down } **Standard:** up Das Netzwerk wird angekündigt, wenn das getrackte Ereignis verfügbar ("UP") wird, bzw. die Ankündigung des Netzwerks beendet wird, wenn das getrackte Ereignis nicht verfügbar ("DOWN") wird.

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.8.8.4
Ein Netzwerk löschen

Um ein für das BGP-Protokoll konfiguriertes Netzwerk zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie das Netzwerk durch Eingabe von:

```
no routing bgp network address
```

Erläuterung:

- *`address`* ist die IP-Subnetzadresse und das Präfix für das Netzwerk

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.8.9
Sammeladressen verwalten

Dieser Abschnitt beschreibt, wie mehrere Adressen in einer einzelnen dynamischen BGP-Route zusammengeführt werden können.

INHALT

- Abschnitt 12.8.9.1, „Eine Liste der Sammeladressen anzeigen“
- Abschnitt 12.8.9.2, „Eine Sammeladresse hinzufügen“
- Abschnitt 12.8.9.3, „Eine Sammeladresse löschen“

Abschnitt 12.8.9.1
Eine Liste der Sammeladressen anzeigen

Um eine Liste der Sammeladressen für dynamische BGP-Routen anzusehen, geben Sie Folgendes ein:

```
show running-config routing bgp aggregate-address
```

Falls Adressen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config routing bgp aggregate-address
routing bgp
 aggregate-address 11.11.0.0/16
  options summary-only
  !
 !
!
```

Falls keine Sammeladressen konfiguriert wurden, fügen Sie je nach Bedarf Adressen hinzu. Weitere Informationen finden Sie unter Abschnitt 12.8.9.2, „Eine Sammeladresse hinzufügen“.

Abschnitt 12.8.9.2
Eine Sammeladresse hinzufügen

Um eine Sammeladresse für dynamische BGP-Routen hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den Pfad hinzu, indem Sie Folgendes eingeben:

   ```
   routing bgp aggregate-address address
   ```

   Erläuterung:

   - *address* ist die Subnetzadresse und das Präfix für die Sammeladresse
3. Bei Bedarf konfigurieren Sie Optionen für die Adresse. Für weitere Informationen siehe Abschnitt 12.8.10.2, „Eine Option für Sammeladressen hinzufügen“.
4. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.8.9.3
Eine Sammeladresse löschen

Um eine Sammeladresse für dynamische BGP-Routen zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die Adresse, indem Sie Folgendes eingeben:

   ```
   no routing bgp aggregate-address address
   ```

   Erläuterung:

   - *address* ist die Subnetzadresse und das Präfix für die Sammeladresse
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.8.10
Optionen für Sammeladressen verwalten

Dieser Abschnitt beschreibt, wie die Optionen `as-set` und `summary-only` für BGP-Sammeladressen eingestellt werden.

INHALT

- Abschnitt 12.8.10.1, „Eine Liste der Optionen für Sammeladressen anzeigen“
- Abschnitt 12.8.10.2, „Eine Option für Sammeladressen hinzufügen“
- Abschnitt 12.8.10.3, „Eine Option für Sammeladressen löschen“

Abschnitt 12.8.10.1
Eine Liste der Optionen für Sammeladressen anzeigen

Um eine Liste der Optionen für Sammeladressen anzusehen, geben Sie Folgendes ein:

```
routing bgp aggregate-address address options
```

Falls Optionen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config routing bgp aggregate-address 11.11.0.0/16 options
routing bgp
 aggregate-address 11.11.0.0/16
  options summary-only
  !
 !
!
```

Falls keine Optionen konfiguriert wurden, fügen Sie je nach Bedarf Optionen hinzu. Weitere Informationen finden Sie unter Abschnitt 12.8.10.2, „Eine Option für Sammeladressen hinzufügen“.

Abschnitt 12.8.10.2
Eine Option für Sammeladressen hinzufügen

Um eine Option für Sammeladressen hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den Pfad hinzu, indem Sie Folgendes eingeben:

   ```
   routing bgp aggregate-address address options [ summary-only | as-set ]
   ```

   Erläuterung:

   - *address* ist die Subnetzadresse und das Präfix für die Sammeladresse
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.8.10.3
Eine Option für Sammeladressen löschen

Um eine Option für Sammeladressen zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die Option, indem Sie Folgendes eingeben:

   ```
   no routing bgp aggregate-address address options [ summary-only | as-set ]
   ```

   Erläuterung:

   - *address* ist die Subnetzadresse und das Präfix für die Sammeladresse
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.8.11
Umverteilungsmetriken verwalten

Die Umverteilungsmetriken dienen zur Umverteilung von Routing-Informationen von anderen Routing-Protokollen, statischen Routen oder vom Kernel verwalteten Routen. Routen für Subnetze, die direkt mit dem Router verbunden sind, aber kein Teil des BGP-Netzwerks sind, können ebenfalls mitgeteilt werden.

INHALT

- Abschnitt 12.8.11.1, „Eine Liste der Umverteilungsmetriken anzeigen“
- Abschnitt 12.8.11.2, „Eine Umverteilungsmetrik hinzufügen“
- Abschnitt 12.8.11.3, „Eine Umverteilungsmetrik löschen“

Abschnitt 12.8.11.1
Eine Liste der Umverteilungsmetriken anzeigen

Um eine Liste der Umverteilungsmetriken für dynamische BGP-Routen anzusehen, geben Sie Folgendes ein:

```
show running-config routing bgp redistribute
```

Falls Metriken konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config routing bgp redistribute
routing bgp
 redistribute rip
  no metric
 !
!
```

Falls keine Umverteilungsmetriken konfiguriert wurden, fügen Sie je nach Bedarf Metriken hinzu. Weitere Informationen finden Sie unter Abschnitt 12.8.11.2, „Eine Umverteilungsmetrik hinzufügen“.

Abschnitt 12.8.11.2
Eine Umverteilungsmetrik hinzufügen

Um für dynamische BGP-Routen eine Umverteilungsmetrik hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie die Metrik hinzu, indem Sie Folgendes eingeben:

   ```
   routing bgp redistribute [ rip | ospf | connected | static | kernel ] metric metric
   ```

   Erläuterung:

   - *metric* ist die Metrik für umverteilte Routen
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.8.11.3
Eine Umverteilungsmetrik löschen

Um eine Umverteilungsmetrik für dynamische BGP-Routen zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die Metrik durch Eingabe von:

   ```
   no routing bgp redistribute [ rip | ospf | connected | static | kernel ]
   ```
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.9
Verwalten von OSPF

Das Open Shortest Path First-Protokoll (OSPF) bestimmt den besten Pfad für das Leiten des IP-Datenverkehrs durch ein TCP/IP-Netzwerk in Abhängigkeit von Verbindungskosten und -qualität. Im Gegensatz zum statischen Routing werden beim OSPF Verbindungsausfälle und sonstige Veränderungen der Netzwerktopologie berücksichtigt. OSPF unterscheidet sich auch dahingehend von RIP, da es weniger Router-zu-Router-Aktualisierungsverkehr bereitstellt.

Bei dem RUGGEDCOM ROX II OSPF Daemon (ospfd) handelt es sich um eine RFC 2178 [http://tools.ietf.org/html/rfc2178]-konforme Implementierung der OSPF-Version 2. Der Deamon verwendet Opaque LSA-Erweiterungen

(RFC 2370 [http://tools.ietf.org/html/rfc2370]) und ABR-Typ-Erweiterungen (RFC 3509 [http://tools.ietf.org/html/rfc3509]).

Ein OSPF-Netzwerkdesign beinhaltet die Partitionierung eines Netzwerks in mehrere eigenständige Bereiche. Die Bereiche werden zur Minimierung von Routerverkehr innerhalb eines Bereichs und zur besseren Verwaltung und Senkung der Anzahl angekündigter Routen gewählt. Jedem Bereich werden Bereichsnummern zugeordnet. Alle Router im Bereich werden als Area-Router bezeichnet. Wenn zwischen zwei Bereichen Datenverkehr übermittelt wird, dann wird ein Router mit Verbindungen in jeden Bereich als Area-Border-Router ausgewählt und dient als Gateway.

HINWEIS
Der Parameter `router-id` *legt die ID des Routers fest. Standardmäßig ist dies die höchste dem Router zugewiesene IP. Eine manuelle Konfiguration dieses Werts wird empfohlen, um eine Änderung der ID beim Hinzufügen zum bzw. beim Löschen aus dem Router zu vermeiden. Bei der Wahl des Master-Routers wird die ID als einer der Werte herangezogen, um den Gewinner zu wählen. Durch eine feste ID werden unerwartete Änderungen bei der Wahl des Master-Routers vermieden.*

HINWEIS
In komplexen vorhandenen Netzwerken können RIP, OSPF, BGP und IS-IS gleichzeitig auf demselben Router aktiv sein. In der Regel wird jedoch jeweils nur ein dynamisches Routingprotokoll verwendet.

HINWEIS
Es können bestimmte Routen für Virtual Routing and Forwarding (VRF)-Schnittstellen konfiguriert werden. Weitere Informationen über VRF finden Sie in Abschnitt 12.11, „Verwalten von VRF (Virtual Routing and Forwarding)“.

INHALT

- Abschnitt 12.9.1, „OSPF-Grundlagen“
- Abschnitt 12.9.2, „Konfigurieren des OSPF“
- Abschnitt 12.9.3, „Anzeigen des Status von dynamischen OSPF-Routen“
- Abschnitt 12.9.4, „Präfix-Listen und -Einträge verwalten“
- Abschnitt 12.9.5, „Bereiche verwalten“
- Abschnitt 12.9.6, „Routen-Karten verwalten“
- Abschnitt 12.9.7, „Filter für eingehende Routen verwalten“
- Abschnitt 12.9.8, „Umverteilungsmetriken verwalten“
- Abschnitt 12.9.9, „Routing-Schnittstellen verwalten“
- Abschnitt 12.9.10, „Message Digest Keys verwalten“

Abschnitt 12.9.1
OSPF-Grundlagen

Wenn ein OSPF-konfigurierter Router seinen Betrieb aufnimmt, gibt er ein *Hello*-Paket aus. Router mit demselben OSPF-Bereich, Hello-Interval- und Dead-Interval-Timer kommunizieren miteinander und werden als Nachbarn bezeichnet.

Nach dem Erkennen seiner Nachbarn tauscht ein Router so genannte Link State Advertisements aus, um die Netzwerktopologie zu bestimmen.

Alle 30 Minuten (voreingestellt) muss die gesamte Topologie des Netzwerks an alle Router im Bereich gesendet werden.

Falls die Verbindungsraten zu niedrig, die Verbindungen zu stark ausgelastet sind oder zu viele Routen existieren, werden bestimmte Routen möglicherweise nicht erneut bekanntgegeben und als veraltet eingestuft.

Die Unterteilung des Netzwerks in kleinere Bereiche zur Senkung der Anzahl an Routen innerhalb eines Bereichs oder die Senkung der Anzahl der anzukündigenden Routen kann zur Vermeidung dieses Problems beitragen.

In Netzwerken mit gemeinsamen Zugriff (d.h. durch Switches oder Hubs angebundene Router) wird ein Designated-Router und ein Backup-Designated-Router gewählt, um Routenänderungen von den Subnetzen im Bereich zu empfangen. Sobald ein Designated-Router gewählt ist, werden alle Änderungen des Routing-Zustands an den Designated-Router gesendet, der die resultierenden Änderungen anschließend an alle Router sendet.

Die Wahl wird in Abhängigkeit der Priorität entschieden, die der Schnittstelle der einzelnen Router zugewiesen ist. Die höchste Priorität gewinnt. Falls die Priorität gebunden ist, gewinnt die höchste Router-ID.

Abschnitt 12.9.2

Konfigurieren des OSPF

Um das dynamische Routing mithilfe des Open-Shortest-Path-First-(OSPF)-Daemon zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***routing » ospf*** und konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
enabled	Aktiviert das dynamische OSPF-Routing-Protokoll.
abr-type { abr-type }	**Zusammenfassung:** { cisco, ibm, shortcut, standard } **Standard:** cisco Der Typ OSPF ABR.
auto-cost-reference-bandwidth { auto-cost-reference-bandwidth }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 1 und 4294967 **Standard:** 100 Berechnet die OSPF-Schnittstellenkosten entsprechend der Bandbreite [1-4294967 Mbit/s]
compatible-rfc1583	Sorgt für Kompatibilität mit dem obsoleten RFC1583 OSPF (aktuell ist RFC2178)
default-information-originate	Kündigt die voreingestellte Route an.
default-metric { default-metric }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 0 und 16777214 Die Standard-Metrik der "Redistribute"-Routen.
distance { distance }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 1 und 255 Die administrative Distanz.
opaque-lsa	Aktiviert die Opaque-LSA-Funktion (RFC2370).
passive-default	**Zusammenfassung:** { true, false } **Standard:** true Passiver Standardwert für eine neue Schnittstelle.
refresh-timer { refresh-timer }	**Zusammenfassung:** Eine vorzeichenlose 16-Bit-Ganzzahl zwischen 10 und 1800 **Standard:** 10 Der Refresh-Timer.
router-id { router-id }	**Zusammenfassung:** Eine Zeichenkette mit 7 bis 15 Zeichen

Parameter	Beschreibung
	Die Router-ID für OSPF.

3. Konfigurieren Sie Präfixlistenfilter. Weitere Informationen finden Sie unter Abschnitt 12.9.4.3, „Hinzufügen einer Präfixliste“.
4. Konfigurieren Sie Bereiche. Weitere Informationen finden Sie unter Abschnitt 12.9.5.2, „Hinzufügen eines Bereichs“.
5. Konfigurieren Sie Route-Map-Filter. Weitere Informationen finden Sie unter Abschnitt 12.9.6.3, „Hinzufügen eines Route-Map-Filters“.
6. Konfigurieren Sie Umverteilungsmetriken. Weitere Informationen finden Sie unter Abschnitt 12.9.8.2, „Hinzufügen einer Umverteilungsmetrik“.
7. Konfigurieren Sie Schnittstellen. Weitere Informationen finden Sie unter Abschnitt 12.9.9.2, „Eine Routing-Schnittstelle konfigurieren“.
8. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.9.3

Anzeigen des Status von dynamischen OSPF-Routen

Um den Status der auf dem Gerät konfigurierten dynamischen OSPF-Routen anzuzeigen, geben Sie Folgendes ein:

```
show routing status ospf route network
```

Sofern OSPF-Routen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show routing status ospf route network | tab
ID              DISCARD  INTER AREA  COST  AREA     HOW
-------------------------------------------------------------------------------
192.168.1.0/24  no       intra area  10    0.0.0.0
                                                    directly attached to fe-1-2
192.168.2.0/24  no       intra area  10    0.0.0.0
                                                    directly attached to fe-1-4
```

Diese Liste liefert die folgenden Informationen:

Parameter	Beschreibung
id	**Zusammenfassung:** Eine Zeichenkette Netzwerkpräfix.
destination	**Zusammenfassung:** Eine Zeichenkette Ziel (Netzwerk oder Verwerfen).
path-type	**Zusammenfassung:** Eine Zeichenkette Pfadtyp (inter-area oder intra-area).
cost	**Zusammenfassung:** Eine Zeichenkette Kosten.
area	**Zusammenfassung:** Eine Zeichenkette Bereich.

Um den Status des auf dem Gerät konfigurierten dynamischen OSPF-Nachbarn anzuzeigen, geben Sie Folgendes ein:

```
show routing status ospf neighbor
```

Falls ein OSPF-Nachbar konfiguriert wurde, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show routing status ospf neighbor
                                                                                DEAD
ID           ADDRESS         INTERFACE                   PRIORITY  STATE        TIME
-------------------------------------------------------------------------------------
21.21.21.21  192.168.212.21  switch.0212:192.168.212.22  1         Full/Backup  31.249s
```

Diese Liste liefert die folgenden Informationen:

Parameter	Beschreibung
id	**Zusammenfassung:** Eine Zeichenkette Nachbar-ID.
address	**Zusammenfassung:** Eine Zeichenkette Adresse.
interface	**Zusammenfassung:** Eine Zeichenkette Schnittstelle.
priority	**Zusammenfassung:** Eine Zeichenkette Priorität.
state	**Zusammenfassung:** Eine Zeichenkette Status.
dead-time	**Zusammenfassung:** Eine Zeichenkette Totzeit.

Um den Status der auf dem Gerät konfigurierten dynamischen OSPF-Datenbank anzuzeigen, geben Sie Folgendes ein:

```
show routing status ospf database
```

Falls ein OSPF-Nachbar konfiguriert wurde, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show routing status ospf database
 router
                                                    LINK
ID           AREA     ADV ROUTER   AGE   SEQNUM      COUNT
-----------------------------------------------------------
21.21.21.21  0.0.0.0  21.21.21.21  1307  0x80000017  2
22.22.22.22  0.0.0.0  22.22.22.22  614   0x8000001c  1
22.22.22.22  0.0.0.1  22.22.22.22  1364  0x8000000e  1

 net
ID              AREA     ADV ROUTER   AGE  SEQNUM
-----------------------------------------------------
192.168.212.22  0.0.0.0  22.22.22.22  584  0x80000009

 summary
ID             AREA     ADV ROUTER   AGE   SEQNUM      ROUTE
-------------------------------------------------------------------------
192.168.22.0   0.0.0.0  22.22.22.22  1354  0x80000008  192.168.22.0/24
192.168.21.0   0.0.0.1  22.22.22.22  1434  0x80000009  192.168.21.0/24
192.168.212.0  0.0.0.1  22.22.22.22  44    0x80000008  192.168.212.0/24

 as-external
                                          METRIC
```

Diese Liste liefert die folgenden Informationen:

Über den Router:

Parameter	Beschreibung
area	**Zusammenfassung:** Eine Zeichenkette Bereich.

Über das Netz:

Parameter	Beschreibung
area	**Zusammenfassung:** Eine Zeichenkette Bereichskennung.

Über die Zusammenfassung:

Parameter	Beschreibung
area	**Zusammenfassung:** Eine Zeichenkette Bereichskennung.

Falls keine dynamischen OSPF-Routen konfiguriert wurden, konfigurieren Sie OSPF und fügen Sie nach Bedarf Routen hinzu. Weitere Informationen über das Konfigurieren von OSPF finden Sie in Abschnitt 12.9.2, „Konfigurieren des OSPF“.

Abschnitt 12.9.4

Präfix-Listen und -Einträge verwalten

Nachbarn können Präfix-Listen zugeordnet werden, die dem OSPF-Daemon die Filterung eingehender oder abgehender Routen auf Grund der Einträge *allow* und *deny* in der Präfix-Liste ermöglichen.

INHALT

- Abschnitt 12.9.4.1, „Eine Liste der Präfixlisten anzeigen“
- Abschnitt 12.9.4.2, „Eine Liste der Präfixeinträge anzeigen“
- Abschnitt 12.9.4.3, „Hinzufügen einer Präfixliste“
- Abschnitt 12.9.4.4, „Hinzufügen eines Präfixeintrags“
- Abschnitt 12.9.4.5, „Eine Präfixliste löschen“
- Abschnitt 12.9.4.6, „Einen Präfixeintrag löschen“

Abschnitt 12.9.4.1

Eine Liste der Präfixlisten anzeigen

Um eine Liste von Präfixlisten für dynamische OSPF-Routen anzuzeigen, geben Sie Folgendes ein:

- **Bei Standard-OSPF-Routen**

```
routing ospf filter prefix-list
```

- **Bei VRF-Routen über OSPF**

```
routing ospf vrf vrf filter prefix-list
```

Erläuterung:

- *vrf* ist die Bezeichnung der gewählten VRF

Falls Präfixlisten konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config routing ospf filter prefix-list | tab
NAME                  DESCOSPFTION  SEQ  ACTION  SUBNET           LE  GE
-------------------------------------------------------------------------
list-permit-lan-22    -
                                    100  permit  192.168.33.0/24  -   -
list-withdraw-lan-11  -
                                    100  permit  192.168.33.0/24  -   -
                                    200  permit  192.168.33.0/24  32  -

!
```

Falls keine Präfixlisten konfiguriert wurden, fügen Sie je nach Bedarf Listen hinzu. Weitere Informationen finden Sie unter Abschnitt 12.9.4.3, „Hinzufügen einer Präfixliste“.

Abschnitt 12.9.4.2

Eine Liste der Präfixeinträge anzeigen

Um eine Liste von Einträgen für dynamische OSPF, Standard-OSPF und OSPF-Präfixlisten anzuzeigen, geben Sie Folgendes ein:

- **Bei Standard-OSPF-Routen**

  ```
  routing ospf filter prefix-list name entry
  ```

- **Bei VRF-Routen über OSPF**

  ```
  routing ospf vrf vrf filter prefix-list name entry
  ```

Erläuterung:

- *vrf* ist die Bezeichnung der gewählten VRF
- *name* ist die Bezeichnung der Präfixliste

Falls Einträge konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config routing ospf filter prefix-list test entry | tab
SEQ  ACTION  SUBNET           LE  GE
-----------------------------------------
5    permit  192.168.40.0/24  32  -
6    deny    192.168.5.21/32     -   -

 !
!
```

Falls keine Einträge konfiguriert wurden, fügen Sie je nach Bedarf Einträge hinzu. Weitere Informationen finden Sie unter Abschnitt 12.9.4.4, „Hinzufügen eines Präfixeintrags“.

Abschnitt 12.9.4.3

Hinzufügen einer Präfixliste

Um dynamischen OSPF-Routen eine Präfixliste hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie die Liste hinzu, indem Sie Folgendes eingeben:

- **Bei Standard-OSPF-Routen**

  ```
  routing ospf filter prefix-list name
  ```

- **Bei VRF-Routen über OSPF**

  ```
  routing ospf vrf vrf filter prefix-list name
  ```

  Erläuterung:

  - *vrf* ist die Bezeichnung der gewählten VRF
  - *name* ist die Bezeichnung der Präfixliste

3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
description { description }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 1024 Zeichen Die Beschreibung der Präfixliste.

4. Fügen Sie nach Bedarf Präfixeinträge hinzu. Weitere Informationen finden Sie unter Abschnitt 12.9.4.4, „Hinzufügen eines Präfixeintrags“.
5. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.9.4.4

Hinzufügen eines Präfixeintrags

Um einen Eintrag in der Präfixliste eines dynamischen OSPF hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den Eintrag hinzu, indem Sie Folgendes eingeben:

   - **Bei Standard-OSPF-Routen**

     ```
     routing ospf filter prefix-list name entry number
     ```

   - **Bei VRF-Routen über OSPF**

     ```
     routing ospf vrf vrf filter prefix-list name entry number
     ```

     Erläuterung:

     - *vrf* ist die Bezeichnung der gewählten VRF
     - *name* ist die Bezeichnung der Präfixliste
     - *number* ist die Sequenznummer für den Eintrag

3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
action { action }	**Zusammenfassung:** { deny, permit } **Standard:** permit Vorgang.
subnet { subnet }	**Zusammenfassung:** Eine Zeichenkette mit 9 bis 18 Zeichen Netzwerk (xxx.xxx.xxx.xxx/xx). Dieser Parameter ist obligatorisch.
le { le }	**Zusammenfassung:** Eine vorzeichenlose 8-Bit-Ganzzahl zwischen 1 und 32

Parameter	Beschreibung
	Die maximale Präfixlänge, um IP-Adresse im Subnetz anzupassen.
ge { ge }	**Zusammenfassung:** Eine vorzeichenlose 8-Bit-Ganzzahl zwischen 1 und 32 Die minimale Präfixlänge, um IP-Adresse im Subnetz anzupassen.

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.9.4.5
Eine Präfixliste löschen

Um eine Präfixliste für dynamische OSPF-Routen zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.

   HINWEIS
   Beim Löschen einer Präfixliste werden gleichzeitig alle zugehörigen Präfixe entfernt.

2. Löschen Sie die Liste, indem Sie Folgendes eingeben:
   - **Bei Standard-OSPF-Routen**

     ```
     no routing ospf filter prefix-list name
     ```

   - **Bei VRF-Routen über OSPF**

     ```
     no routing ospf vrf vrf filter prefix-list name
     ```

   Erläuterung:
   - *`vrf`* ist die Bezeichnung der gewählten VRF
   - *`name`* ist die Bezeichnung der Präfixliste
3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.9.4.6
Einen Präfixeintrag löschen

Um einen Eintrag in der Präfixliste eines dynamischen OSPF zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den Eintrag, indem Sie Folgendes eingeben:
   - **Bei Standard-OSPF-Routen**

     ```
     no routing ospf filter prefix-list name entry number
     ```

   - **Bei VRF-Routen über OSPF**

     ```
     no routing ospf vrf vrf filter prefix-list name entry number
     ```

   Erläuterung:
   - *`vrf`* ist die Bezeichnung der gewählten VRF
   - *`name`* ist die Bezeichnung der Präfixliste

- *number* ist die Sequenznummer für den Eintrag

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.9.5
Bereiche verwalten

Netzwerkbereiche legen die Regionen fest, in denen Routen an andere Router verteilt werden. Die Subnetze an einem bestimmten Router können dessen OSPF-Bereich hinzugefügt werden. Der Router bietet diese Subnetze dann allen Routern in seinem Bereich an.

OSPF-Bereiche müssen so eingerichtet sein, dass ein einzelner Verbindungsausfall nicht dazu führen kann, dass das Netzwerk in zwei getrennte Netzwerke aufgespalten wird.

Ein Router kann mehreren Bereichen angehören und als Gateway zwischen Bereichen fungieren. Sind in einem Netzwerk mehrere Bereiche vorhanden, ist Bereich Null (0) der Backbone-Bereich. Jeder Bereich muss einen Router besitzen, der ihn mit Bereich Null (0) verbindet.

INHALT

- Abschnitt 12.9.5.1, „Eine Liste der Bereiche anzeigen“
- Abschnitt 12.9.5.2, „Hinzufügen eines Bereichs“
- Abschnitt 12.9.5.3, „Einen Bereich löschen“

Abschnitt 12.9.5.1
Eine Liste der Bereiche anzeigen

Um eine Liste von Bereichen, die für dynamische OSPF-Routen konfiguriert wurden, anzuzeigen, geben Sie Folgendes ein:

- **Bei Standard-OSPF-Routen**

```
show running-config routing ospf area
```

- **Bei VRF-Routen über OSPF**

```
show running-config routing ospf vrf vrf area
```

Erläuterung:

- *vrf* ist die Bezeichnung der gewählten VRF

Falls Bereiche konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config routing ospf area | tab
AREA     NETWORK
--------------------------
0.0.0.0  192.168.12.0/24

!
```

Falls keine Bereiche konfiguriert wurden, fügen Sie je nach Bedarf Bereiche hinzu. Weitere Informationen finden Sie unter Abschnitt 12.9.5.2, „Hinzufügen eines Bereichs“.

Abschnitt 12.9.5.2
Hinzufügen eines Bereichs

Um einen Bereich für dynamische OSPF-Routen hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den Bereich hinzu, indem Sie Folgendes eingeben:
   - **Bei Standard-OSPF-Routen**
     ```
     routing ospf area id network/prefix
     ```
   - **Bei VRF-Routen über OSPF**
     ```
     routing ospf vrf vrf area id network/prefix
     ```

   Erläuterung:
   - *vrf* ist die Bezeichnung der gewählten VRF
   - *id* ist die ID für den OSPF-Bereich Die ID muss das Format *A.B.C.D* aufweisen.
   - *network/prefix* ist das Netzwerk und das Präfix für den OSPF-Bereich
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
shortcut { shortcut }	**Zusammenfassung:** { default, disable, enable } **Standard:** default Legt den Shortcut-Modus des Bereichs fest. Mögliche Optionen sind: • Default: Wenn der Area Border Router (ABR) über eine aktive Backbone-Verbindung verfügt, wird der Bereich nicht für das Shortcutting verwendet und der ABR legt im Router-LSA für diesen Bereich kein neues Bit (S-Bit) fest. Das Gegenteil ist wahr, wenn der ABR über keine aktive Backbone-Verbindung verfügt. • Enable: Wenn der Area Border Router (ABR) über eine aktive Backbone-Verbindung verfügt, legt er im Router-LSA für diesen Bereich ein neues Bit (S-Bit) fest und verwendet es für das Shortcutting. Andere ABR im Bereich müssen ebenfalls das neue Bit melden. Wenn der Area Border Router (ABR) jedoch über keine aktive Backbone-Verbindung verfügt, verwendet er den Bereich bedingungslos für das Shortcutting und legt im Router-LSA für diesen Bereich das neue Bit fest. • Disable: Der ABR verwendet diesen Bereich nicht für das Shortcutting oder legt das neue Bit (S-Bit) im dafür erzeugten Router-LSA fest.

4. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.9.5.3
Einen Bereich löschen

Um einen Bereich für dynamische OSPF-Routen zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den Bereich, indem Sie Folgendes eingeben:
   - **Bei Standard-OSPF-Routen**
     ```
     no routing ospf area id network/prefix
     ```
   - **Bei VRF-Routen über OSPF**
     ```
     no routing ospf vrf vrf area id network/prefix
     ```

Erläuterung:

- *vrf* ist die Bezeichnung der gewählten VRF
- *id* ist die ID für den gewählten OSPF-Bereich Die ID muss das Format *A.B.C.D* aufweisen.
- *network/prefix* ist das Netzwerk und das Präfix für den gewählten OSPF-Bereich

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.9.6

Routen-Karten verwalten

Routen-Karten sind sequentielle Anweisungen für die Filterung der Routen, die bestimmte Kriterien erfüllen. Erfüllt eine Route die Kriterien der angewandten Routen-Karte, so kann sie entweder aus der Routing-Tabelle ausgeschlossen oder gegen Umverteilung gesperrt werden. In RUGGEDCOM ROX II werden Routen-Karten konfiguriert, um Routen anhand ihres metrischen Werts, der die Kosten der Route bestimmt, zu filtern. Sobald ein Treffer gefunden ist, wird die zugehörige Aktion ausgeführt.

Jede Routen-Karte erfordert eine fortlaufende Nummer (z. B. 10, 20, 30 usw.), mit der mehrere Routen-Karten nacheinander abgearbeitet werden können, bis ein Treffer gefunden wird. Es wird empfohlen, fortlaufende Nummern in 10er-Schritten anzulegen, falls später eine neue Routen-Karte zwischen zwei vorhandene Karten eingefügt werden muss.

INHALT

- Abschnitt 12.9.6.1, „Eine Liste der Route-Map-Filter anzeigen“
- Abschnitt 12.9.6.2, „Anzeigen einer Liste der Einträge für einen Route-Map-Filter“
- Abschnitt 12.9.6.3, „Hinzufügen eines Route-Map-Filters“
- Abschnitt 12.9.6.4, „Einen Eintrag für einen Route-Map-Filter hinzufügen“
- Abschnitt 12.9.6.5, „Einen Route-Map-Filter löschen“
- Abschnitt 12.9.6.6, „Löschen eines Eintrags im Route-Map-Filter“
- Abschnitt 12.9.6.7, „Konfigurieren von Übereinstimmungsregeln“

Abschnitt 12.9.6.1

Eine Liste der Route-Map-Filter anzeigen

Um eine Liste der Route-Map-Filter für dynamische OSPF-Routen anzuzeigen, geben Sie Folgendes ein:

- **Bei Standard-OSPF-Routen**

```
show running-config routing ospf filter route-map
```

- **Bei VRF-Routen über OSPF**

```
show running-config routing ospf vrf vrf filter route-map
```

Erläuterung:

- *vrf* ist die Bezeichnung der gewählten VRF

Falls Filter konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config routing ospf filter route-map | tab
```

```
                       ON
                       MATCH  AS     PREFIX  PREFIX  PREFIX                                LOCAL
                  NEXT          ORIGINATOR
TAG  SEQ  ACTION  CALL  GOTO   PATH  LIST    LIST    LIST    METRIC  PEER  ORIGIN  AS  IP  PREFERENCE
 OPERATION  VALUE  HOP   ORIGIN  ID          WEIGHT
-------------------------------------------------------------------------------------------
map
     10   permit  -     -      -     -       -       -       -       -     -       -   -   -
 -          -      -     -       -           -

!
```

Falls keine Filter konfiguriert wurden, fügen Sie je nach Bedarf Filter hinzu. Weitere Informationen finden Sie unter Abschnitt 12.9.6.3, „Hinzufügen eines Route-Map-Filters“.

Abschnitt 12.9.6.2

Anzeigen einer Liste der Einträge für einen Route-Map-Filter

Um eine Liste der Einträge für einen Route-Map-Filter anzuzeigen, geben Sie Folgendes ein:

- **Bei Standard-OSPF-Routen**

  ```
  show running-config routing ospf filter route-map tag entry
  ```

- **Bei VRF-Routen über OSPF**

  ```
  show running-config routing ospf vrf vrf filter route-map tag entry
  ```

Erläuterung:

- *vrf* ist die Bezeichnung der gewählten VRF
- *tag* ist die Variable für den Route-Map-Filter

Falls Einträge konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config routing ospf filter route-map map entry | tab
                   ON
                   MATCH  AS     PREFIX  PREFIX  PREFIX                                LOCAL
              NEXT          ORIGINATOR
SEQ  ACTION   CALL  GOTO   PATH  LIST    LIST    LIST    METRIC  PEER  ORIGIN  AS  IP  PREFERENCE
 OPERATION  VALUE  HOP   ORIGIN  ID          WEIGHT  AS
-------------------------------------------------------------------------------------------
10   permit  -     -      -     -       -       -       -       -     -       -   -   -           -
      -      -     -       -           -

 !
!
```

Falls keine Filter konfiguriert wurden, fügen Sie je nach Bedarf Filter hinzu. Weitere Informationen finden Sie unter Abschnitt 12.9.6.4, „Einen Eintrag für einen Route-Map-Filter hinzufügen“.

Abschnitt 12.9.6.3

Hinzufügen eines Route-Map-Filters

Um einen Route-Map-Filter für dynamische OSPF-Routen hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den neuen Filter hinzu, indem Sie Folgendes eingeben:

- **Bei Standard-OSPF-Routen**

  ```
  routing ospf filter route-map tag
  ```

- **Bei VRF-Routen über OSPF**

  ```
  routing ospf vrf vrf filter route-map tag
  ```

  Erläuterung:

  - *vrf* ist die Bezeichnung der gewählten VRF
  - *tag* ist die Variable für den Route-Map-Filter

3. Fügen Sie einen oder mehrere Einträge hinzu. Weitere Informationen finden Sie unter Abschnitt 12.9.6.4, „Einen Eintrag für einen Route-Map-Filter hinzufügen“.
4. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.9.6.4

Einen Eintrag für einen Route-Map-Filter hinzufügen

Um einen Eintrag für einen Route-Map-Filter hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den neuen Filter hinzu, indem Sie Folgendes eingeben:

   - **Bei Standard-OSPF-Routen**

     ```
     routing ospf filter route-map tag entry number
     ```

   - **Bei VRF-Routen über OSPF**

     ```
     routing ospf vrf vrf filter route-map tag entry number
     ```

     Erläuterung:

     - *vrf* ist die Bezeichnung der gewählten VRF
     - *tag* ist die Variable für den Route-Map-Filter
     - *number* ist die Sequenznummer für den Eintrag

3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
action { action }	**Zusammenfassung:** { deny, permit } **Standard:** permit Vorgang.
call { call }	**Zusammenfassung:** Eine Zeichenkette Springt nach "match+set" zu einer anderen Route-Map.
on-match-goto { on-match-goto }	**Zusammenfassung:** Eine Zeichenkette Zu diesem übereinstimmenden Eintrag gehen.

Parameter	Beschreibung
metric { metric }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Metrischer Wert.
metric-type { metric-type }	**Zusammenfassung:** Eine vorzeichenbehaftete 8-Bit-Ganzzahl zwischen 1 und 2

Parameter	Beschreibung
	Externer Routentyp.

4. Konfigurieren Sie die Übereinstimmungsregeln für den Route-Map-Filter. Weitere Informationen finden Sie unter Abschnitt 12.9.6.7, „Konfigurieren von Übereinstimmungsregeln".
5. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.9.6.5
Einen Route-Map-Filter löschen

Um einen Route-Map-Filter für dynamische OSPF-Routen zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den Filterschlüssel, indem Sie Folgendes eingeben:
   - **Bei Standard-OSPF-Routen**
     ```
     no routing ospf filter route-map tag
     ```
   - **Bei VRF-Routen über OSPF**
     ```
     no routing ospf vrf vrf filter route-map tag
     ```

   Erläuterung:
   - *`vrf`* ist die Bezeichnung der gewählten VRF
   - *`tag`* ist die Variable für den Route-Map-Filter
3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.9.6.6
Löschen eines Eintrags im Route-Map-Filter

Um einen Eintrag im Route-Map-Filter zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den Filterschlüssel, indem Sie Folgendes eingeben:
   - **Bei Standard-OSPF-Routen**
     ```
     no routing ospf filter route-map tag entry number
     ```
   - **Bei VRF-Routen über OSPF**
     ```
     no routing ospf vrf vrf filter route-map tag entry number
     ```

   Erläuterung:
   - *`vrf`* ist die Bezeichnung der gewählten VRF
   - *`tag`* ist die Variable für den Route-Map-Filter
   - *`number`* ist die Sequenznummer für den Eintrag
3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.9.6.7
Konfigurieren von Übereinstimmungsregeln

Um Übereinstimmungsregeln für einen Eintrag im Route-Map-Filter zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu:
   - **Bei Standard-OSPF-Routen**
     routing » dynamic » ospf » filter » route-map » {tag} » entry » {number} » match
   - **Bei VRF-Routen über OSPF**
     routing » dynamic » ospf » vrf » {vrf} » filter » route-map » {tag} » entry » {number} » match

   Erläuterung:
   - *{vrf}* ist die gewählte VRF
   - *{tag}* ist die Variable für den Route-Map-Filter
   - *{number}* ist die Sequenznummer für den Eintrag
3. Konfigurieren Sie je nach Bedarf die folgenden Parameter:

Parameter	Beschreibung
prefix-list { prefix-list }	**Zusammenfassung:** Eine Zeichenkette Die Bezeichnung der Präfixliste.

Parameter	Beschreibung
prefix-list { prefix-list }	**Zusammenfassung:** Eine Zeichenkette Die Bezeichnung der Präfixliste.

Parameter	Beschreibung
ifname { ifname }	**Zusammenfassung:** Eine Zeichenkette Der Schnittstellenname.

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.9.7
Filter für eingehende Routen verwalten

Ankündigungen eingehender Routen können durch Zuweisung eines oder mehrerer Routen-Filter gefiltert werden. Dies kann hilfreich sein, wenn bestimmte OSPF-Routen aus der Routing-Tabelle ausgeschlossen werden sollen.

HINWEIS
Weitere Informationen über Routen-Filter finden Sie unter Abschnitt 12.9.6, „Routen-Karten verwalten“.

INHALT

- Abschnitt 12.9.7.1, „Liste der Filter für eingehende Routen anzeigen“
- Abschnitt 12.9.7.2, „Hinzufügen eines Filters für eingehende Routen“

- Abschnitt 12.9.7.3, „Einen Filter für eingehende Routen löschen“

Abschnitt 12.9.7.1
Liste der Filter für eingehende Routen anzeigen

Um eine Liste der Filter, die für eingehende, angekündigte Routen konfiguriert wurden, anzuzeigen, geben Sie Folgendes ein:

- **Bei Standard-OSPF-Routen**

```
show running-config routing ospf incoming-route-filter
```

- **Bei VRF-Routen über OSPF**

```
show running-config routing ospf vrf vrf incoming-route-filter
```

Erläuterung:

- *vrf* ist die Bezeichnung der gewählten VRF

Falls Filter für Routen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config routing ospf incoming-route-filter
routing ospf
 incoming-route-filter ospf_route_1
 !
!
```

Falls keine Filter für Routen konfiguriert wurden, fügen Sie je nach Bedarf Filter hinzu. Weitere Informationen finden Sie unter Abschnitt 12.9.7.2, „Hinzufügen eines Filters für eingehende Routen“.

Abschnitt 12.9.7.2
Hinzufügen eines Filters für eingehende Routen

Um einen Routenfilter für eingehende angekündigte Routen hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Stellen Sie sicher, dass eine Route-Map konfiguriert wurde. Weitere Informationen finden Sie unter Abschnitt 12.9.6, „Routen-Karten verwalten“.
3. Erstellen Sie einen neuen Filter für eingehende Routen, indem Sie Folgendes eingeben:
   - **Bei Standard-OSPF-Routen**

```
routing ospf incoming-route-filter route-map
```

   - **Bei VRF-Routen über OSPF**

```
routing ospf vrf vrf incoming-route-filter route-map
```

   Erläuterung:
   - *vrf* ist die Bezeichnung der gewählten VRF
   - *route-map* ist die Bezeichnung der Route-Map
4. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.9.7.3
Einen Filter für eingehende Routen löschen

Um einen Routenfilter, der für eingehende angekündigte Routen konfiguriert ist, zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die Adresse, indem Sie Folgendes eingeben:
   - **Bei Standard-OSPF-Routen**
     ```
     no routing ospf incoming-route-filter route-map
     ```
   - **Bei VRF-Routen über OSPF**
     ```
     no routing ospf vrf vrf incoming-route-filter route-map
     ```

   Erläuterung:
   - *vrf* ist die Bezeichnung der gewählten VRF
   - *route-map* ist die Bezeichnung der Route-Map
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.9.8
Umverteilungsmetriken verwalten

Die Umverteilungsmetriken dienen zur Umverteilung von Routing-Informationen von anderen Routing-Protokollen, statischen Routen oder vom Kernel verwalteten Routen. Routen für Subnetze, die direkt mit dem Router verbunden sind, aber kein Teil der OSPF-Bereiche sind, können ebenfalls mitgeteilt werden.

INHALT

- Abschnitt 12.9.8.1, „Anzeigen Liste mit Umverteilungsmetriken“
- Abschnitt 12.9.8.2, „Hinzufügen einer Umverteilungsmetrik“
- Abschnitt 12.9.8.3, „Eine Umverteilungsmetrik löschen“

Abschnitt 12.9.8.1
Anzeigen Liste mit Umverteilungsmetriken

Um für dynamische OSPF-Routen eine Liste mit Umverteilungsmetriken anzuzeigen, geben Sie Folgendes ein:

- **Bei Standard-OSPF-Routen**
  ```
  routing ospf redistribute
  ```
- **Bei VRF-Routen über OSPF**
  ```
  routing ospf vrf vrf redistribute
  ```

Erläuterung:

- *vrf* ist die Bezeichnung der gewählten VRF

Wenn Metriken konfiguriert wurden, wird eine Tabelle oder Liste ähnlich der Folgenden angezeigt:

```
ruggedcom# show running-config routing ospf redistribute
```

```
routing ospf
 redistribute bgp
  no metric-type
  no metric
 !
!
```

Wenn keine Umverteilungsmetriken konfiguriert wurden, fügen Sie nach Bedarf eine Metrik hinzu. Für weitere Informationen siehe Abschnitt 12.9.8.2, „Hinzufügen einer Umverteilungsmetrik“.

Abschnitt 12.9.8.2
Hinzufügen einer Umverteilungsmetrik

Um eine Umverteilungsmetrik für dynamische OPF-Routen hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie die Metrik hinzu, indem Sie Folgendes eingeben:
   - **Bei Standard-OSPF-Routen**

     ```
     routing ospf redistribute [  bgp |  rip |  connected |  static |  kernel ]
     ```

   - **Bei VRF-Routen über OSPF**

     ```
     routing ospf vrf vrf redistribute [  bgp |  rip |  connected |  static |  kernel ]
     ```

   Erläuterung:
   - *vrf* ist die Bezeichnung der gewählten VRF
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
metric-type { metric-type }	**Zusammenfassung:** Eine vorzeichenbehaftete 8-Bit-Ganzzahl zwischen 1 und 2 **Standard:** 2 Der äußere OSPF-Metriktyp für umverteilte Routen.
metric { metric }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 0 und 16777214 Die Metrik für umverteilte Routen.
route-map { route-map }	**Zusammenfassung:** Eine Zeichenkette Die Bezeichnung der Route-Map.

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.9.8.3
Eine Umverteilungsmetrik löschen

Um eine Umverteilungsmetrik für dynamische OPF-Routen zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die Metrik, indem Sie Folgendes eingeben:
   - **Bei Standard-OSPF-Routen**

     ```
     no routing ospf redistribute [  bgp |  rip |  connected |  static |  kernel ]
     ```

- **Bei VRF-Routen über OSPF**

```
no routing ospf vrf vrf redistribute [  bgp |  rip |  connected |  static |  kernel ]
```

Erläuterung:

- *vrf* ist die Bezeichnung der gewählten VRF

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.9.9

Routing-Schnittstellen verwalten

Dieser Abschnitt beschreibt, wie Sie Schnittstellen für OSPF-Routen verwalten können.

INHALT

- Abschnitt 12.9.9.1, „Eine Liste der Routing-Schnittstellen anzeigen“
- Abschnitt 12.9.9.2, „Eine Routing-Schnittstelle konfigurieren“

Abschnitt 12.9.9.1

Eine Liste der Routing-Schnittstellen anzeigen

Um eine Liste der Routing-Schnittstellen für ein OSPF-Netzwerk anzuzeigen, geben Sie Folgendes ein:

- **Bei Standard-OSPF-Routen**

```
show running-config routing ospf interface
```

- **Bei VRF-Routen über OSPF**

```
show running-config routing ospf vrf vrf interface
```

Erläuterung:

- *vrf* ist die Bezeichnung der gewählten VRF

Eine Tabelle oder Liste ähnlich dem folgenden Beispiel wird angezeigt:

```
ruggedcom# show running-config routing ospf interface | tab
                                          MINIMAL
                                  DEAD    HELLO       HELLO                       RETRANSMIT
 TRANSMIT  KEY
IFNAME       AUTHENTICATION  COST  INTERVAL  MULTIPLIER  INTERVAL  PRIORITY  PASSIVE  INTERVAL    DELAY
     ID   MD5
-------------------------------------------------------------------------------------------------
dummy0       -               -     40        -           10        1         true     5           1
fe-cm-1      -               -     40        -           10        1         true     5           1
switch.0001  -               -     40        -           10        1         true     5           1
```

Abschnitt 12.9.9.2

Eine Routing-Schnittstelle konfigurieren

Um eine Routing-Schnittstelle für ein OSPF-Netzwerk zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.

2. Navigieren Sie zu:
   - **Bei Standard-OSPF-Routen**
     routing » dynamic » ospf » interface » {name}
   - **Bei VRF-Routen über OSPF**
     routing » dynamic » ospf » vrf » {vrf} » interface » {name}

   Erläuterung:
   - *{vrf}* ist die gewählte VRF
   - *{name}* ist die Bezeichnung der Schnittstelle
3. Konfigurieren Sie die Einstellungen für das "Dead Interval", indem Sie die folgenden Befehle eingeben:

HINWEIS
Für einen stabilen Betrieb ist es empfehlenswert, dass der Wert `dead-interval` *mindestens vier mal so groß ist wie der Wert "Number of Hellos per Second".*

HINWEIS
Kleinere Werte von `dead-intervall` *und* `minimal-hello-multiplier` *tragen dazu bei, dass Veränderungen in Netzwerkrouten schneller umgesetzt werden, wenn sich die Topologie des Netzwerks ändert. Ferner vergrößert sich die Belastung für Router und Links durch höheren Verkehr, der durch den Anstieg der Nachrichten verursacht wird.*

Kleinere Werte sorgen zudem für Beschränkungen bei der Anzahl der Routen, die innerhalb eines OSPF-Netzwerkbereichs verteilt werden können, ebenso wie der Betrieb über langsamere Links.

WICHTIG!
Die Werte für `dead-interval` *und Number of Hellos per Second müssen bei jedem Router in einem OSPF-Netzwerkbereich identisch sein.*

Parameter	Beschreibung
dead-interval { dead-interval }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 1 und 65535 **Standard:** 40 Die Dauer, bevor ein Router für tot erachtet wird (in Sekunden).
minimal-hello-multiplier { minimal-hello-multiplier }	**Zusammenfassung:** Eine vorzeichenlose 8-Bit-Ganzzahl zwischen 1 und 10 Die Häufigkeit, wie oft eine "Hello"-Nachricht innerhalb einer Sekunde gesendet werden kann.

4. Konfigurieren Sie die Schnittstelleneinstellungen, indem Sie die folgenden Befehle eingeben:

HINWEIS
Bei aktiven Netzwerkschnittstellen ist die Linkerkennung automatisch aktiviert. Sie sorgt dafür, dass bei Ausfall einer Schnittstelle der entsprechende Routing-Daemon benachrichtigt wird und keine Subnetze mit dieser Schnittstelle mehr ankündigt. Der Routing-Daemon kündigt das Subnetz wieder an, sobald der Link wiederhergestellt ist. Dadurch können Routing-Daemons Linkausfälle schneller erkennen, da der Router für das Timeout nicht auf das ***Dead Interval*** *warten muss. Durch die Linkerkennung wird auch das Starten und Stoppen des Ankündigens von* ***wiederverteilten*** *Routen basierend auf dem Status ihrer Schnittstellen-Links verursacht.*

HINWEIS
Die Linkkosten legen fest, welche Route verwendet werden soll, wenn mehrere Links ein vorgegebenes Ziel erreichen können. Standardmäßig ordnet OSPF allen Links die gleichen Kosten zu, sofern keine zusätzlichen Informationen über die Links vorhanden sind. Bei jeder Schnittstelle

wird der Wert 10 Mbit angenommen, sofern nicht vom für die Schnittstelle eingestellten Parameter `auto-cost-bandwidth` *anders angegeben. Weitere Informationen zur* `auto-cost-bandwidth` *finden Sie unter Abschnitt 7.1.1, „Kalkulation für routingfähige Schnittstellen konfigurieren“.*

Standardmäßig beträgt die OSPF-Referenzbandbreite für die Berechnung der Linkkosten 100 Mbit. Die Referenzbandbreite dividiert durch die Linkbandbreite ergibt die Standardkosten für einen Link; dieser Wert ist standardmäßig 10. Wenn jedem Link eine spezifische Bandbreite zugeordnet wird, wird dies bei den Kosten berücksichtigt.

Unter OSPF können jeder routingfähigen Schnittstelle manuell Linkkosten zugeordnet werden. Dies sollte durchgeführt werden, wenn die Geschwindigkeit des Links nicht als Methode zum Auswählen des besten Links verwendet werden soll.

Parameter	Beschreibung
{ ifname }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 32 Zeichen Schnittstellen-Name.
authentication { authentication }	**Zusammenfassung:** { message-digest, null } Der Authentifizierungstyp an dieser Schnittstelle.
cost { cost }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 1 und 65535 Die Link-Kosten. Sind sie nicht eingestellt, werden die Kosten anhand der Referenzbandbreite dividiert durch die Schnittstellenbandbreite berechnet.
hello-interval { hello-interval }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 1 und 65535 **Standard:** 10 Die Zeit (in Sekunden) zwischen dem Senden der "Hello“-Pakete.
priority { priority }	**Zusammenfassung:** Eine vorzeichenlose 8-Bit-Ganzzahl zwischen 0 und 255 **Standard:** 1 Schnittstellenpriorität.
passive	**Zusammenfassung:** { true, false } **Standard:** true Gibt an, ob eine Schnittstelle aktiv oder passiv ist. Passive Schnittstellen senden keine LSA an andere Router und gehören nicht zu einem OSPF-Bereich.
retransmit-interval { retransmit-interval }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 1 und 65535 **Standard:** 5 Zeit (in Sekunden) zwischen der erneuten Übertragung von Ankündigungen zu Verbindungsunterbrechungen.
transmit-delay { transmit-delay }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 1 und 65535 **Standard:** 1 Die Link-Status-Übertragungsverzögerung (in Sekunden).
dead-interval { dead-interval }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 1 und 65535 **Standard:** 40 Die Dauer, bevor ein Router für tot erachtet wird (in Sekunden).
minimal-hello-multiplier { minimal-hello-multiplier }	**Zusammenfassung:** Eine vorzeichenlose 8-Bit-Ganzzahl zwischen 1 und 10 Die Häufigkeit, wie oft eine "Hello“-Nachricht innerhalb einer Sekunde gesendet werden kann.

5. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.9.10

Message Digest Keys verwalten

Message Digest Keys verwenden den MD5-Algorithmus, um OSPF-Nachbarn zu authentifizieren und zu verhindern, dass nicht autorisierte Router dem OSPF-Netzwerk beitreten. Durch Aktivieren der Authentifizierung und Konfigurieren eines gemeinsamen Schlüssels auf allen Routern können nur Router, die den gleichen Authentifizierungsschlüssel besitzen, Ankündigungen innerhalb des OSPF-Netzwerks senden und empfangen.

Mithilfe einer ID für jeden Schlüssel kann der Router mehrere Passwörter verwenden und wiederholte Angriffe verhindern, bei denen OSPF-Pakete erfasst, modifiziert und an einen Router übertragen werden. Um Passwörter zu ändern, legen Sie einfach einen neuen Schlüssel an und löschen den alten Schlüssel.

WICHTIG!
Der Router kann Routing-Informationen nur mit Nachbarn teilen, die dasselbe Authentifizierungsverfahren und dasselbe Passwort verwenden.

HINWEIS
Die Authentifizierung erfordert einen kleinen Mehraufwand, da die Nachrichten verschlüsselt werden. Sie wird nicht für vollständig private Netzwerke mit kontrolliertem Zugriff empfohlen.

INHALT

- Abschnitt 12.9.10.1, „Eine Liste der Message Digest Keys anzeigen“
- Abschnitt 12.9.10.2, „Hinzufügen eines Message Digest Key“
- Abschnitt 12.9.10.3, „Einen Message Digest Key löschen“

Abschnitt 12.9.10.1

Eine Liste der Message Digest Keys anzeigen

Um eine Liste der Message Digest Keys für eine OSPF-Routing-Schnittstelle anzuzeigen, geben Sie Folgendes ein:

- **Bei Standard-OSPF-Routen**

```
show running-config routing ospf interface name message-digest-key
```

- **Bei VRF-Routen über OSPF**

```
show running-config routing ospf interface name message-digest-key
```

Erläuterung:

- *vrf* ist die Bezeichnung der gewählten VRF
- *name* ist die Bezeichnung der Routing-Schnittstelle

Falls Schlüssel konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config routing ospf interface switch.0001 message-digest-key
routing ospf
 interface switch.0001
  message-digest-key 1
   md5 RUGGEDCOM
  !
 !
!
```

Falls keine Message Digest Keys konfiguriert wurden, fügen Sie je nach Bedarf Schlüssel hinzu. Weitere Informationen finden Sie unter Abschnitt 12.9.10.2, „Hinzufügen eines Message Digest Key“.

Abschnitt 12.9.10.2
Hinzufügen eines Message Digest Key

Um einen Message Digest Key einer OSPF-Routing-Schnittstelle hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den Schlüssel hinzu, indem Sie Folgendes eingeben:
   - **Bei Standard-OSPF-Routen**
     ```
     routing ospf interface name message-digest-key id
     ```
   - **Bei VRF-Routen über OSPF**
     ```
     routing ospf vrf vrf interface name message-digest-key id
     ```

   Erläuterung:
   - *vrf* ist die Bezeichnung der gewählten VRF
   - *name* ist die Bezeichnung der Routing-Schnittstelle
   - *id* ist die ID für den Message Digest Key
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.9.10.3
Einen Message Digest Key löschen

Um einen Message Digest Key aus einer OSPF-Routing-Schnittstelle zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den Schlüssel, indem Sie Folgendes eingeben:
   - **Bei Standard-OSPF-Routen**
     ```
     no routing ospf interface name message-digest-key id
     ```
   - **Bei VRF-Routen über OSPF**
     ```
     no routing ospf vrf vrf interface name message-digest-key id
     ```

   Erläuterung:
   - *vrf* ist die Bezeichnung der gewählten VRF
   - *name* ist die Bezeichnung der Routing-Schnittstelle
   - *id* ist die ID für den Message Digest Key
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.10

MPLS verwalten

MPLS (Multi-Protocol Label Switching) findet zwischen Layer 2 und Layer 3 des OSI-(Open Systems Interconnection)-Modells statt und stellt einen Mechanismus für den Datenverkehr für jedes beliebige Netzwerkschichtprotokoll bereit. MPLS trifft Weiterleitungsentscheidungen anhand von Labels, wobei die Labels in Ziel-IP-Netzwerken abgebildet werden. MPLS-Verkehr ist verbindungsorientiert, da er über vorkonfigurierte LSPs (Label Switch Paths) läuft, die mit dem dynamischen LDP (Label Distribution Protocol) oder durch statische Label-Bindings aufgebaut werden.

INHALT

- Abschnitt 12.10.1, „Status des IP Binding anzeigen“
- Abschnitt 12.10.2, „Status der Forwarding-Tabelle anzeigen“
- Abschnitt 12.10.3, „MPLS aktivieren/deaktivieren“
- Abschnitt 12.10.4, „MPLS-Schnittstellen verwalten“
- Abschnitt 12.10.5, „Statisches Label Binding verwalten“
- Abschnitt 12.10.6, „Statische Crossconnects verwalten“
- Abschnitt 12.10.7, „LDP verwalten“

Abschnitt 12.10.1

Status des IP Binding anzeigen

Um den Status des IP Binding im Gerät anzusehen, geben Sie Folgendes ein:

```
show mpls status ip-binding
```

Falls IP Binding konfiguriert wurde, wird eine Tabelle ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show mpls status ip-binding
                  LOCAL                    REMOTE
PREFIX            LABEL     NEXT HOP       LABEL
-------------------------------------------------
1.1.1.1/32        17        192.168.10.1   imp-null
2.2.2.2/32        18        192.168.10.1   imp-null
3.3.3.3/32        imp-null
4.4.4.4/32        imp-null
5.5.5.5/32        19        192.168.20.2   imp-null
6.6.6.6/32        20        192.168.20.2   imp-null
10.200.16.0/20    16
172.30.128.0/19   imp-null
192.168.10.0/24   imp-null
192.168.20.0/24   imp-null
192.168.100.0/24  21        192.168.10.1   imp-null
192.168.200.0/24  22        192.168.20.2   imp-null
```

Diese Tabelle liefert die folgenden Informationen:

Parameter	Beschreibung
prefix	**Zusammenfassung:** Eine Zeichenkette Das Präfix der Zieladresse.
local-label	**Zusammenfassung:** Eine Zeichenkette

Parameter	Beschreibung
	Das eingehende (lokale) Label.
next-hop	**Zusammenfassung:** Eine Zeichenkette Der Router des nächsten Ziel-Hops.
remote-label	**Zusammenfassung:** Eine Zeichenkette Das entfernte Label

Abschnitt 12.10.2
Status der Forwarding-Tabelle anzeigen

Um den Status der Forwarding-Tabelle im Gerät anzusehen, geben Sie Folgendes ein:

```
show mpls status forwarding-table
```

Eine Tabelle oder Liste ähnlich dem folgenden Beispiel wird angezeigt:

```
ruggedcom# show mpls status forwarding-table
LOCAL  OUTGOING                    OUTGOING
LABEL  LABEL     PREFIX            INTERFACE    NEXT HOP      UPTIME
-------------------------------------------------------------------------
17     Pop       1.1.1.1/32        switch.0010  192.168.10.1  01:04:31
18     Pop       2.2.2.2/32        switch.0010  192.168.10.1  01:04:31
19     Pop       5.5.5.5/32        switch.0020  192.168.20.2  01:04:33
20     Pop       6.6.6.6/32        switch.0020  192.168.20.2  01:04:33
21     Pop       192.168.100.0/24  switch.0010  192.168.10.1  01:04:31
22     Pop       192.168.200.0/24  switch.0020  192.168.20.2  01:04:33
```

Diese Tabelle oder Liste liefert die folgenden Informationen:

Parameter	Beschreibung
local-label	**Zusammenfassung:** Eine Zeichenkette Das eingehende (lokale) Label
outgoing-label	**Zusammenfassung:** Eine Zeichenkette Das ausgehende (entfernte) Label.
prefix	**Zusammenfassung:** Eine Zeichenkette Das Präfix der Zieladresse.
outgoing-interface	**Zusammenfassung:** Eine Zeichenkette Die ausgehende Schnittstelle.
next-hop	**Zusammenfassung:** Eine Zeichenkette Der Router des nächsten Ziel-Hops.
uptime	**Zusammenfassung:** Eine Zeichenkette Die Zeit, in der dieser Eintrag "up" war.

Abschnitt 12.10.3
MPLS aktivieren/deaktivieren

Um das MPLS-Routing zu aktivieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Zum Aktivieren oder Deaktivieren von MPLS geben Sie die folgenden Befehle ein:

   Aktivieren

   ```
   mpls enable
   ```

   Deaktivieren

   ```
   no mpls enable
   ```
3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.10.4

MPLS-Schnittstellen verwalten

Dieser Abschnitt beschreibt, wie Sie die MPLS-Schnittstellen verwalten können.

INHALT

- Abschnitt 12.10.4.1, „Status der MPLS-Schnittstellen anzeigen“
- Abschnitt 12.10.4.2, „Eine Liste der MPLS-Schnittstellen anzeigen“
- Abschnitt 12.10.4.3, „Eine MPLS-Schnittstelle aktivieren/deaktivieren“

Abschnitt 12.10.4.1

Status der MPLS-Schnittstellen anzeigen

Um den Status der MPLS-Schnittstellen im Gerät anzusehen, geben Sie Folgendes ein:

```
show mpls status interfaces
```

Falls MPLS-Schnittstellen im Gerät aktiviert wurden, wird eine Tabelle ähnlich dem folgenden Beispiel angezeigt:

```
show mpls status interfaces
MPLS
INTERFACES    STATUS
--------------------
switch.0010   yes
switch.0020   yes
```

Diese Tabelle liefert die folgenden Informationen:

Parameter	Beschreibung
mpls-interfaces	**Zusammenfassung:** Eine Zeichenkette Die Schnittstelle, die für MPLS aktiviert wurde.
status	**Zusammenfassung:** Eine Zeichenkette Der Betriebszustand.

Falls keine MPLS-Schnittstellen aktiviert wurden, aktivieren Sie Schnittstellen je nach Bedarf. Weitere Informationen über die Aktivierung von MPLS-Schnittstellen finden Sie unter Abschnitt 12.10.4.3, „Eine MPLS-Schnittstelle aktivieren/deaktivieren“.

Abschnitt 12.10.4.2
Eine Liste der MPLS-Schnittstellen anzeigen

Um eine Liste der MPLS-Schnittstellen anzusehen, geben Sie Folgendes ein:

```
show running-config mpls interface-mpls
```

Falls Schnittstellen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config mpls interface-mpls | tab
IFNAME     ENABLED
---------------------
fe-cm-1     false
switch.0001  false
switch.0010  true
switch.0020  false

!
```

Erläuterung:

- *IFNAME* ist die Bezeichnung der Schnittstelle
- *ENABLED* bezeichnet den Status des MPLS-Betriebs an der Schnittstelle

Falls keine MPLS-Schnittstellen konfiguriert wurden, fügen Sie je nach Bedarf Schnittstellen hinzu. Weitere Informationen über die Aktivierung von MPLS-Schnittstellen finden Sie unter Abschnitt 12.10.4.3, „Eine MPLS-Schnittstelle aktivieren/deaktivieren“.

Abschnitt 12.10.4.3
Eine MPLS-Schnittstelle aktivieren/deaktivieren

Um eine MPLS-Schnittstelle zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Aktivieren oder deaktivieren Sie die MLPS-Schnittstelle, indem Sie Folgendes eingeben:

   Aktivieren

   ```
   mpls interface-mpls interface enable
   ```

   Deaktivieren

   ```
   no mpls interface-mpls interface enable
   ```

   Erläuterung:

   - *interface* ist die Bezeichnung der Schnittstelle
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.10.5

Statisches Label Binding verwalten

Dieser Abschnitt beschreibt, wie Sie Label für IPv4- oder Netzwerk-Präfixe belegen können.

INHALT

- Abschnitt 12.10.5.1, „Den Status statischer Label Bindings anzeigen“
- Abschnitt 12.10.5.2, „Eine Liste der statischen Label anzeigen“
- Abschnitt 12.10.5.3, „Hinzufügen eines statischen Labels“
- Abschnitt 12.10.5.4, „Ein statisches Label“

Abschnitt 12.10.5.1

Den Status statischer Label Bindings anzeigen

Um den Status aller konfigurierten statischen Label Bindings anzusehen, geben Sie Folgendes ein:

```
show mpls status static-binding
```

Falls statische Label Bindings konfiguriert wurden, wird eine Tabelle ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show mpls status static-binding
                  IN     OUT
IP ADDRESS        LABEL  LABEL  NEXTHOP
-----------------------------------------------
192.168.20.0/24   90     101    192.168.10.2
192.168.200.0/24  95     100    192.168.10.2
```

Diese Tabelle liefert die folgenden Informationen:

Parameter	Beschreibung
ip-address	**Zusammenfassung:** Eine Zeichenkette Das Präfix der Zieladresse.
in-label	**Zusammenfassung:** Eine Zeichenkette Das eingehende (lokale) Label.
out-label	**Zusammenfassung:** Eine Zeichenkette Das ausgehende (entfernte) Label.
nexthop	**Zusammenfassung:** Eine Zeichenkette Der Router des nächsten Ziel-Hops.

Falls keine statischen Label Bindings konfiguriert wurden, fügen Sie je nach Bedarf Bindings hinzu. Weitere Informationen über das Konfigurieren statischer Bindings finden Sie unter Abschnitt 12.10.5.3, „Hinzufügen eines statischen Labels“.

Abschnitt 12.10.5.2

Eine Liste der statischen Label anzeigen

Um eine Liste der statischen Label anzusehen, geben Sie Folgendes ein:

```
show running-config mpls static-mpls binding [ ipv4 | ipv6 ]
```

Falls statische Label konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config mpls static-mpls binding ipv4
mpls
 static-mpls
  binding
   ipv4
    dest-address 192.168.52.52/32
     next-hop  192.168.10.2
     out-label 16
    !
   !
  !
 !
!
```

Falls keine statischen Label konfiguriert sind, fügen Sie je nach Bedarf Labels hinzu. Weitere Informationen über das Hinzufügen statischer Label finden Sie unter Abschnitt 12.10.5.3, „Hinzufügen eines statischen Labels“.

Abschnitt 12.10.5.3
Hinzufügen eines statischen Labels

Um ein statisches Label hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie ein statisches Label hinzu, indem Sie Folgendes eingeben:

   ```
   mpls static-mpls binding [ ipv4 | ipv6 ] dest-address address
   ```

   Erläuterung:

   - *address* ist die Zieladresse und das Zielpräfix.
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
in-label { in-label }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 16 und 1048575 Das eingehende Label: Ganzzahl 16 -> 1048575.
next-hop { next-hop }	**Zusammenfassung:** Eine Zeichenkette mit 7 bis 15 Zeichen Die IP-Adresse für den Router des nächsten Ziel-Hops. **HINWEIS** *Das ausgehende Label (out-label) des Ziels muss ebenfalls festgelegt werden.*
out-label { out-label }	**Zusammenfassung:** { explicit-null, implicit-null } oder eine vorzeichenlose 32-Bit-Ganzzahl zwischen 16 und 1048575 Das ausgehende Label: • *implicit null* - Das Label hat einen Wert von 3, d. h. der vorletzte (next-to-last) Router führt eine Pop-Operation durch und leitet das restliche Paket an den ausgehenden Router weiter. Das Penultimate Hop Popping (PHP) reduziert die Anzahl der Label-Suchläufe, die vom ausgehenden Router durchgeführt werden müssen. • *explicit null* - Das Label hat den Wert 0, d. h. anstelle einer Pop-Operation leitet der vorletzte (next-to-last) Router ein IPv4-Paket mit einem ausgehenden MPLS-Label von 0 an den ausgehenden Router weiter

Parameter	Beschreibung
	HINWEIS *Der nächste Ziel-Hop muss ebenfalls festgelegt werden.*

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.10.5.4
Ein statisches Label

Um ein statisches Label zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie ein statisches Label, indem Sie Folgendes eingeben:

```
no mpls static-mpls binding [ ipv4 | ipv6 ] dest-address address
```

   Erläuterung:

   - *`address`* ist die Zieladresse und das Zielpräfix.

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.10.6
Statische Crossconnects verwalten

Konfigurieren Sie statische MPLS-Crossconnects, wenn das Gerät der MPLS-Core-Router ist. Crossconnects bauen LSPs (Label Switch Paths) auf, wenn in benachbarten Routern kein LDP (Label Distribution Protocol) implementiert ist. Der Eintrag für statische Crossconnects wird in der Label Forwarding Information Base (LFIB) hinzugefügt. Damit ist in der Label Information Base (LIB) kein Label Binding erforderlich.

INHALT

- Abschnitt 12.10.6.1, „Status der statischen Crossconnects anzeigen“
- Abschnitt 12.10.6.2, „Eine Liste der statischen Crossconnects anzeigen“
- Abschnitt 12.10.6.3, „Einen statischen Crossconnect hinzufügen“
- Abschnitt 12.10.6.4, „Einen statischen Crossconnect löschen“

Abschnitt 12.10.6.1
Status der statischen Crossconnects anzeigen

Um den Status aller konfigurierten statischen Crossconnects anzusehen, geben Sie Folgendes ein:

```
show mpls status static-crossconnect
```

Falls statische Crossconnects konfiguriert wurden, wird eine Tabelle ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show mpls status static-crossconnect
LOCAL  OUTGOING  OUTGOING
LABEL  LABEL     INTERFACE    NEXT HOP
-------------------------------------------
200    205       switch.0010  192.168.10.2
215    250       switch.0010  192.168.10.2
```

Diese Tabelle liefert die folgenden Informationen:

Parameter	Beschreibung
local-label	**Zusammenfassung:** Eine Zeichenkette Das eingehende (lokale) Label.
outgoing-label	**Zusammenfassung:** Eine Zeichenkette Das ausgehende (entfernte) Label.
outgoing-interface	**Zusammenfassung:** Eine Zeichenkette Die ausgehende Schnittstelle.
next-hop	**Zusammenfassung:** Eine Zeichenkette Der Router des nächsten Ziel-Hops.

Falls keine statischen Crossconnects konfiguriert wurden, fügen Sie je nach Bedarf Crossconnects hinzu. Weitere Informationen über das Hinzufügen statischer Crossconnects finden Sie unter Abschnitt 12.10.6.3, „Einen statischen Crossconnect hinzufügen“.

Abschnitt 12.10.6.2
Eine Liste der statischen Crossconnects anzeigen

Um eine Liste der konfigurierten statischen Crossconnects anzusehen, geben Sie Folgendes ein:

```
show running-config mpls static-mpls crossconnects
```

Falls statische Crossconnects konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config mpls static-mpls crossconnect | tab
       OUT                          OUT
LABEL  INTERFACE    NEXT HOP        LABEL
----------------------------------------
20     switch.0001  192.168.10.2    32

 !
!
```

Falls keine statischen Crossconnects konfiguriert wurden, fügen Sie je nach Bedarf Crossconnects hinzu. Weitere Informationen über das Hinzufügen statischer Crossconnects finden Sie unter Abschnitt 12.10.6.3, „Einen statischen Crossconnect hinzufügen“.

Abschnitt 12.10.6.3
Einen statischen Crossconnect hinzufügen

Um einen statischen Crossconnect hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.

2. Fügen Sie einen statischen Crossconnect hinzu, indem Sie Folgendes eingeben:

```
mpls static-mpls crossconnect in-label in-label
```

Erläuterung:

- *in-label* ist das eingehende Label

3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
out-interface { out-interface }	**Zusammenfassung:** Eine Zeichenkette Die ausgehende Schnittstelle. Dieser Parameter ist obligatorisch.
next-hop { next-hop }	**Zusammenfassung:** Eine Zeichenkette mit 7 bis 15 Zeichen oder eine Zeichenkette mit 6 bis 40 Zeichen Der Router des nächsten Ziel-Hops (IPv4- oder IPv6-Format). Dieser Parameter ist obligatorisch.
out-label { out-label }	**Zusammenfassung:** { explicit-null, implicit-null } oder eine vorzeichenlose 32-Bit-Ganzzahl zwischen 16 und 1048575 Die ausgehenden Label: 'explicit-null', 'implicit-null' oder Ganzzahl16 -> 1048575. Dieser Parameter ist obligatorisch.

4. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.10.6.4
Einen statischen Crossconnect löschen

Um einen statischen Crossconnect zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie einen statischen Crossconnect durch Eingabe von:

```
no mpls static-mpls crossconnect in-label in-label
```

Erläuterung:

- *in-label* ist das eingehende Label

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.10.7
LDP verwalten

LDP (Label Distribution Protocol), das in RFC 5036 [http://tools.ietf.org/html/rfc5036] beschrieben ist, ist ein Protokoll, das den Austausch von MPLS-Labeldaten über einen MPLS-fähigen Router ermöglicht. Die Labels werden in beide Richtungen verteilt, so dass ein LSP (Label Switched Path) hergestellt und in einem MPLS-Netzwerk dynamisch verwaltet werden kann, im Gegensatz zur Konfiguration statischer Routen. LDP nutzt (mit Hilfe von OSPF oder IS-IS) bereits erstellte Routing-Informationen für die Verteilung von Labelinformationen an die MPLS-fähigen Router.

Mit LDP werden LSR (Label Switch Routers) für die Erkennung und Zuweisung von Labels zu ihren Nachbarn im MPLS-Netzwerk aktiviert. Die LSR erkennen dann ihre Peers und tauschen ihre Labelinformationen untereinander aus. Die Labelinformationen werden in den Tabellen Label Information Base (LIB) und Label Forwarding Information Base (LFIB) gespeichert.

INHALT

- Abschnitt 12.10.7.1, „Status des LDP Binding anzeigen“
- Abschnitt 12.10.7.2, „Status der LDP-Erkennungsschnittstellen anzeigen“
- Abschnitt 12.10.7.3, „Status der lokalen Knoten des LDP-Nachbarn anzeigen“
- Abschnitt 12.10.7.4, „Status der LDP-Nachbarverbindungsinformationen anzeigen“
- Abschnitt 12.10.7.5, „Status der LDP-Nachbarerkennungsinformationen anzeigen“
- Abschnitt 12.10.7.6, „Das LDP konfigurieren“
- Abschnitt 12.10.7.7, „Neighbor Discovery konfigurieren“
- Abschnitt 12.10.7.8, „Eine Liste der LDP-Schnittstellen anzeigen“
- Abschnitt 12.10.7.9, „Eine LDP-Schnittstelle aktivieren/deaktivieren“

Abschnitt 12.10.7.1

Status des LDP Binding anzeigen

Um den Status des LDP Binding im Gerät anzusehen, geben Sie Folgendes ein:

```
show mpls ldp status binding
```

Eine Tabelle oder Liste ähnlich dem folgenden Beispiel wird angezeigt:

```
ruggedcom# show mpls ldp status binding
                LOCAL     NEXT      REMOTE
PREFIX          LABEL     HOP       LABEL     IN USE
-------------------------------------------------------
1.1.1.1         17        2.2.2.2   imp-null  in-use
1.1.1.1         17        6.6.6.6   17
2.2.2.2         18        2.2.2.2   imp-null  in-use
2.2.2.2         18        6.6.6.6   18
3.3.3.3         imp-null
4.4.4.4         imp-null
5.5.5.5         19        2.2.2.2   19
5.5.5.5         19        6.6.6.6   imp-null  in-use
```

Diese Tabelle oder Liste liefert die folgenden Informationen:

Parameter	Beschreibung
prefix	**Zusammenfassung:** Eine Zeichenkette Das LDP-Transport-Präfix.
local-label	**Zusammenfassung:** Eine Zeichenkette Das eingehende (lokale) Label.
next-hop	**Zusammenfassung:** Eine Zeichenkette Der Router des nächsten Ziel-Hops.
remote-label	**Zusammenfassung:** Eine Zeichenkette Das entfernte LDP-Label.

Parameter	Beschreibung
in-use	**Zusammenfassung:** Eine Zeichenkette Die LDP-Gebrauchs-Flag.

Abschnitt 12.10.7.2
Status der LDP-Erkennungsschnittstellen anzeigen

Um den Status der LDP-Erkennungsschnittstellen im Gerät anzusehen, geben Sie Folgendes ein:

```
show mpls ldp status discovery
```

Falls LDP-Erkennungsschnittstellen konfiguriert wurden, wird eine Tabelle ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show mpls ldp status discovery
status discovery
 local id 4.4.4.4
 interfaces
INTERFACE    SRC IP ADDR   PEER ID  PEER IP       STATE
-----------------------------------------------------------
switch.0010  192.168.10.2  2.2.2.2  192.168.10.1  OPER
switch.0020  192.168.20.1  6.6.6.6  192.168.20.2  OPER
```

Diese Tabelle liefert die folgenden Informationen:

Parameter	Beschreibung
interface	**Zusammenfassung:** Eine Zeichenkette Die LDP-Erkennungsschnittstelle.
src-ip-addr	**Zusammenfassung:** Eine Zeichenkette IP-Quelladresse der LDP-Erkennung.
peer-id	**Zusammenfassung:** Eine Zeichenkette Die Peer-ID der LDP-Erkennung.
peer-ip	**Zusammenfassung:** Eine Zeichenkette Die Peer-IP-Adresse der LDP-Erkennung.
state	**Zusammenfassung:** Eine Zeichenkette Der Status der LDP-Erkennungsschnittstelle.

Weitere Informationen über das Konfigurieren von LDP-Erkennungsschnittstellen finden Sie unter Abschnitt 12.10.7.9, „Eine LDP-Schnittstelle aktivieren/deaktivieren“.

Abschnitt 12.10.7.3
Status der lokalen Knoten des LDP-Nachbarn anzeigen

Um den Status der lokalen Knoten für den LDP-Nachbarn im Gerät anzusehen, geben Sie Folgendes ein:

```
show mpls ldp status neighbor local-node-information
```

Eine Tabelle oder Liste ähnlich dem folgenden Beispiel wird angezeigt:

```
ruggedcom# show mpls ldp status neighbor local-node-information
                  KEEPALIVE
```

```
LDP ID   HOLDTIME  INTERVAL
-----------------------------
4.4.4.4   15s       180s
```

Diese Tabelle oder Liste liefert die folgenden Informationen:

Parameter	Beschreibung
ldp-id	**Zusammenfassung:** Eine Zeichenkette Die LDP-ID des lokalen Knotens des Nachbarn.
hello-holdtime	**Zusammenfassung:** Eine Zeichenkette Die LDP-Hello-Haltezeit des lokalen Knotens des Nachbarn.
session-holdtime	**Zusammenfassung:** Eine Zeichenkette Die LDP-Sitzungs-Haltezeit des lokalen Knotens des Nachbarn.

Abschnitt 12.10.7.4

Status der LDP-Nachbarverbindungsinformationen anzeigen

Um den Status der LDP-Nachbarverbindung im Gerät anzusehen, geben Sie Folgendes ein:

```
show mpls ldp status neighbor connection-information
```

Eine Tabelle ähnlich dem folgenden Beispiel wird angezeigt:

```
ruggedcom# show mpls ldp status neighbor connection-information
          TCP
PEER ID   CONNECTION    STATE  UPTIME
---------------------------------------
2.2.2.2   192.168.10.1  OPER   00:51:51
-         192.168.10.2
6.6.6.6   192.168.20.2  OPER   00:51:53
-         192.168.20.1
```

Parameter	Beschreibung
peer-id	**Zusammenfassung:** Eine Zeichenkette Die Peer-ID der LDP-Nachbar-Verbindung.
tcp-connection	**Zusammenfassung:** Eine Zeichenkette Die TCP-Verbindung der LDP-Nachbar-Verbindung.
state	**Zusammenfassung:** Eine Zeichenkette Der Zustand der LDP-Nachbar-Verbindung.
uptime	**Zusammenfassung:** Eine Zeichenkette Die Klarzeit der LDP-Nachbar-Verbindung.

Diese Tabelle liefert die folgenden Informationen:

Parameter	Beschreibung
peer-id	**Zusammenfassung:** Eine Zeichenkette Die Peer-ID der LDP-Nachbar-Verbindung.
tcp-connection	**Zusammenfassung:** Eine Zeichenkette Die TCP-Verbindung der LDP-Nachbar-Verbindung.
state	**Zusammenfassung:** Eine Zeichenkette

Parameter	Beschreibung
	Der Zustand der LDP-Nachbar-Verbindung.
uptime	**Zusammenfassung:** Eine Zeichenkette Die Klarzeit der LDP-Nachbar-Verbindung.

Abschnitt 12.10.7.5
Status der LDP-Nachbarerkennungsinformationen anzeigen

Um den Status der LDP-Nachbarerkennungsinformationen im Gerät anzusehen, geben Sie Folgendes ein:

```
show mpls ldp status neighbor discovery-information
```

Eine Tabelle oder Liste ähnlich dem folgenden Beispiel wird angezeigt:

```
ruggedcom# show mpls ldp status neighbor discovery-information
                                                          P
                                                P         KEEPALIVE
PEER ID  PEER IP       INTERFACE    LOCAL IP    HOLDTIME  INTERVAL
-------------------------------------------------------------------
2.2.2.2  192.168.10.1  switch.0010  192.168.10.2  15s       180s
6.6.6.6  192.168.20.2  switch.0020  192.168.20.1  15s       180s
```

Diese Tabelle oder Liste liefert die folgenden Informationen:

Parameter	Beschreibung
peer-id	**Zusammenfassung:** Eine Zeichenkette Die Peer-ID der LDP-Nachbar-Erkennung.
peer-ip	**Zusammenfassung:** Eine Zeichenkette Die Peer-ID der LDP-Nachbar-Erkennung.
interface	**Zusammenfassung:** Eine Zeichenkette Die lokale IP-Adresse der LDP-Nachbar-Erkennung.
local-ip	**Zusammenfassung:** Eine Zeichenkette Status der LDP-Nachbar-Erkennung.
peer-hello-holdtime	**Zusammenfassung:** Eine Zeichenkette Die Peer-Hello-Haltezeit der LDP-Nachbar-Erkennung.
agreed-hello-holdtime	**Zusammenfassung:** Eine Zeichenkette Die vereinbarte Hello-Haltezeit (kürzere Haltezeit lokal/Peer) der LDP-Nachbar-Erkennung.
peer-session-holdtime	**Zusammenfassung:** Eine Zeichenkette Die Peer-Sitzungs-Haltezeit der LDP-Nachbar-Erkennung.

Abschnitt 12.10.7.6
Das LDP konfigurieren

Um das LDP zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Aktivieren oder deaktivieren Sie das LDP durch Eingabe folgender Befehle:

Aktivieren

```
mpls ldp enable
```

Deaktivieren

```
no mpls ldp enable
```

3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
enabled	**Zusammenfassung:** { true, false } **Standard:** false Eine Boolesche Flag, die anzeigt, dass das Label Distribution Protocol (LDP) aktiviert ist. **HINWEIS** *Vor dem Aktivieren von LDP muss MPLS aktiviert sein.* **HINWEIS** *Statische MPLS-Bindings müssen entfernt werden, bevor das LDP aktiviert wird.*
holdtime { holdtime }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl **Standard:** 180 Die Haltezeit der Sitzung (in Sekunden), die als Keepalive-Timeout verwendet wird, um die Label Distribution Protocol (LDP)-Sitzung bei Abwesenheit von LDP-Nachrichten des Sitzungs-Peers aufrechtzuerhalten.

Abschnitt 12.10.7.7

Neighbor Discovery konfigurieren

Um die LDP Neighbor Discovery zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Um die LDP Neighbor Discovery zu konfigurieren, geben Sie den folgenden Befehl ein:

```
mpls ldp discovery
```

3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
interval { interval }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl **Standard:** 5 Die Zeit (in Sekunden) zwischen dem Senden aufeinanderfolgender "Hello"-Nachrichten.
holdtime { holdtime }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl **Standard:** 15 Die Zeit (in Sekunden), die ein gefundener LDP-Nachbar ohne Empfang einer LDP-"Hello"-Nachricht vom Nachbarn gespeichert wird.

Abschnitt 12.10.7.8

Eine Liste der LDP-Schnittstellen anzeigen

Um eine Liste der LDP-Schnittstellen anzusehen, geben Sie Folgendes ein:

```
show running-config mpls ldp interface-ldp
```

Falls Schnittstellen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config mpls ldp interface-ldp | tab
TRANSPORT             TRANSPORT IP
IFNAME       ENABLED  ADDRESS
-------------------------------------
fe-cm-1      false    -
switch.0001  false    -
switch.0010  true     192.168.10.1
switch.0020  false    -

 !
!
```

Weitere Informationen über die Aktivierung von LDP-Schnittstellen finden Sie unter Abschnitt 12.10.7.9, „Eine LDP-Schnittstelle aktivieren/deaktivieren“.

Abschnitt 12.10.7.9

Eine LDP-Schnittstelle aktivieren/deaktivieren

Um eine LDP-Schnittstelle zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Aktivieren/deaktivieren Sie die LDP-Schnittstelle, indem Sie Folgendes eingeben:

   Aktivieren

   ```
   mpls ldp interface-ldp name
   ```

   Deaktivieren

   ```
   no mpls ldp interface-ldp name
   ```

   Erläuterung:

   - *name* ist die Bezeichnung der Transport-Schnittstelle, die aktiviert oder deaktiviert werden soll.
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.11

Verwalten von VRF (Virtual Routing and Forwarding)

Durch VRF (Virtual Routing and Forwarding) können mehrere Routing-Instanzen gleichzeitig auf einem Netzwerk-Router vorhanden sein, ohne sich gegenseitig oder die globale Routing-Tabelle zu stören. Diese Funktion wird meist von Dienstanbietern verwendet, um verschiedene Verkehrsarten, die vom gleichen Router ausgehen, zu verteilen.

Jede Routing-Instanz ist komplett eigenständig und hat ihre eigenen Schnittstellen. Der Verkehr über diese Schnittstellen gilt als Teil nur dieses bestimmten VRF.

Der Verkehr, der durch den Tunnel läuft, kann ferner ein MPLS-Label erhalten, um die Sicherheit zu verbessern. Dies wird im Gegensatz zu VRF-Lite (das erstmals von Cisco eingeführt wurde) als Full-VRF bezeichnet.

Die RUGGEDCOM RX1400 können als CE, PE oder P (Provider Core) Router konfiguriert werden.

INHALT

- Abschnitt 12.11.1, „VRF-Konzepte“
- Abschnitt 12.11.2, „Statistiken zu VRF-Schnittstellen anzeigen“
- Abschnitt 12.11.3, „Konfigurieren von VRF“
- Abschnitt 12.11.4, „Eine VRF-Schnittstelle konfigurieren“
- Abschnitt 12.11.5, „VRF-Definitionen verwalten“
- Abschnitt 12.11.6, „Routenziele verwalten“
- Abschnitt 12.11.7, „VRF-Instanzen und OSPF verwalten“
- Abschnitt 12.11.8, „IP/VPN-Tunnel verwalten“
- Abschnitt 12.11.9, „VPNv4-Nachbarn verwalten“
- Abschnitt 12.11.10, „IPv4-Adressfamilien verwalten“
- Abschnitt 12.11.11, „Umverteilung für IPv4-Adressfamilien verwalten“
- Abschnitt 12.11.12, „Nachbarn für IPv4-Adressfamilien verwalten“
- Abschnitt 12.11.13, „Statische VRF-Routen verwalten“
- Abschnitt 12.11.14, „Gateways für statische VRF-Routen verwalten“
- Abschnitt 12.11.15, „Schnittstellen für statische VRF-Routen verwalten“

Abschnitt 12.11.1

VRF-Konzepte

Dieser Abschnitt beschreibt einige wesentliche Konzepte für die Implementierung von Virtual Routing and Forwarding (VRF) in RUGGEDCOM ROX II.

INHALT

- Abschnitt 12.11.1.1, „VRF und VRF-Lite“
- Abschnitt 12.11.1.2, „Vor- und Nachteile der Verwendung von VRF“

Abschnitt 12.11.1.1

VRF und VRF-Lite

Sowohl VRF als auch VRF-Lite nutzen das VRF-Konzept, um Schnittstellen zu isolieren, die Wiederverwendung von IP-Adressen zu ermöglichen und Routing-Tabellen zu verwalten. Beide stellen ferner ein Sicherheitsniveau für diese Schnittstellen zu den VRFs bereit. Bei VRF wird MPLS in Verbindung mit IP/VPNs benutzt, um ein höheres Sicherheitsniveau als VRF-Lite zu erhalten.

RUGGEDCOM ROX II unterstützt VRF und VRF-Lite gleichzeitig. VRF-Schnittstellen und VRF-Lite-Schnittstellen können miteinander kombiniert werden.

Abschnitt 12.11.1.2
Vor- und Nachteile der Verwendung von VRF

Die Verwendung von VRF hat die folgenden Vor- und Nachteile:

Vorteile

- Anlegen mehrerer getrennter Netzwerkleitungen für verschiedene Datenströme
- Individualisierte Sicherheit für jedes VRF
- Getrennte Verwaltung der VRF-Systeme für Prüfung und Abrechnung
- Anlegen getrennter Intranets in einer Arbeitsumgebung
- Anlegen von VRFs für verschiedene Abteilungen (z. B. Finanzen, Technik, Personal usw.)
- Verringerung der Größe von Routing-Tabellen
- Wiederverwendung von IP-Adressen oder Subnetzen
- MPLS IP-VPNs können deutlich teurere T1/E1-Standleitungen ersetzen und bieten den gleichen Sicherheitsstandard

Nachteile

- Höherer Speicherverbrauch. Jedes konfigurierte VRF erzeugt eine Replikation der BGP-Route und erfordert neue FIBs und IP-Routingtabellen
- Zusätzlicher Verarbeitungsaufwand und Speicherverbrauch durch Namespace-Management

Abschnitt 12.11.2
Statistiken zu VRF-Schnittstellen anzeigen

Um Statistiken zu Schnittstellen anzuzeigen, die einer VRF-Instanz zugeordnet sind, geben Sie Folgendes ein:

```
show interfaces vrf vrf ip
```

Erläuterung:

- *vrf* ist die gewählte VRF-Liste

Eine Tabelle oder Liste ähnlich dem folgenden Beispiel wird angezeigt:

```
ruggedcom# show interfaces vrf VRF1 ip | tab
        ADMIN                          RX       RX       RX      RX       TX       TX       TX      TX
      TX           IPV4
NAME    STATE    STATE    POINTOPOINT  BYTES    PACKETS  ERRORS  DROPPED  BYTES    PACKETS  ERRORS
 DROPPED  COLLISIONS  ADDRESS
-------------------------------------------------------------------------------------------------------------------
fe-1-1  not set  not set  false        8842726  117751   0       0        5366914  64721    0       0
      0

                  1.9.5.2/24
fe-1-2  not set  not set  false        4874496  70821    0       0        5849272  71022    0       0
      0

                  1.7.5.1/24
fe-1-3  not set  not set  false        7730176  120784   0       0        9423076  120810   0       0
      0
```

```
                1.1.1.1/32
```

Diese Tabelle oder Liste liefert die folgenden Informationen:

Parameter	Beschreibung
name	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 15 Zeichen Der Name der Schnittstelle.
admin-state	**Zusammenfassung:** { not set, up, down, testing, unknown, dormant, notPresent, lowerLayerDown } Der Verwaltungszustand des Ports. Dieser Parameter ist obligatorisch.
state	**Zusammenfassung:** { not set, up, down, testing, unknown, dormant, notPresent, lowerLayerDown } Zeigt, ob die Verbindung verfügbar ("up") oder nicht verfügbar ("down") ist. Dieser Parameter ist obligatorisch.
pointopoint	**Zusammenfassung:** { true, false } Die Punkt-zu-Punkt-Verbindung. Dieser Parameter ist obligatorisch.
bytes	**Zusammenfassung:** Eine vorzeichenlose 64-Bit-Ganzzahl Die Anzahl empfangener Bytes. Dieser Parameter ist obligatorisch.
packets	**Zusammenfassung:** Eine vorzeichenlose 64-Bit-Ganzzahl Die Anzahl der empfangenen Pakete. Dieser Parameter ist obligatorisch.
errors	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl der empfangenen Fehler-Pakete. Dieser Parameter ist obligatorisch.
dropped	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl der Pakete, die vom empfangenden Gerät verworfen wurden. Dieser Parameter ist obligatorisch.
bytes	**Zusammenfassung:** Eine vorzeichenlose 64-Bit-Ganzzahl Die Anzahl übertragener Bytes. Dieser Parameter ist obligatorisch.
packets	**Zusammenfassung:** Eine vorzeichenlose 64-Bit-Ganzzahl Die Anzahl der übertragenen Pakete. Dieser Parameter ist obligatorisch.
errors	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl der übertragenen Fehler-Pakete. Dieser Parameter ist obligatorisch.
dropped	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl der Pakete, die vom übertragenden Gerät verworfen wurden. Dieser Parameter ist obligatorisch.
collisions	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Anzahl der Collisions, die am Port erkannt wurden.

Parameter	Beschreibung
	Dieser Parameter ist obligatorisch.

Abschnitt 12.11.3

Konfigurieren von VRF

Um Virtual Routing and Forwarding (VRF) zu konfigurieren, gehen Sie wie folgt vor:

WICHTIG!
Vor der Konfiguration von VRF muss das BGP-Routing aktiviert werden.

Vollständige VRF-Konfiguration

1. Stellen Sie sicher, dass BGP aktiviert ist, und konfigurieren Sie die Autonomous System ID für das Border Gateway-Protokoll (BGP). Weitere Informationen finden Sie unter Abschnitt 12.8.1, „Konfigurieren von BGP“.
2. Konfigurieren Sie eine VRF-Definition und Ziele der Route für jeden Customer Edge-(CE)-Router. Weitere Informationen finden Sie unter Abschnitt 12.11.5.2, „Hinzufügen einer VRF-Definition“.
3. Konfigurieren Sie eine routingfähige Schnittstelle und IP-Adresse für jede VRF-Definition. Weitere Informationen finden Sie unter Abschnitt 12.11.4, „Eine VRF-Schnittstelle konfigurieren“.
4. Aktivieren Sie OSPF. Weitere Informationen finden Sie unter Abschnitt 12.9.2, „Konfigurieren des OSPF“.
5. Konfigurieren Sie eine oder mehrere VRF-Instanzen für OSPF. Weitere Informationen finden Sie unter Abschnitt 12.9.2, „Konfigurieren des OSPF“.
6. Fügen Sie einen oder mehrere BGP-Nachbarn hinzu. Weitere Informationen finden Sie unter Abschnitt 12.8.7.2, „Einen Nachbarn hinzufügen“.
7. Konfigurieren Sie einen oder mehrere IP/VPN-Tunnel für jede Schnittstelle. Weitere Informationen finden Sie unter Abschnitt 12.11.8.2, „Einen IP-/VPN-Tunnel hinzufügen“.
8. Fügen Sie der Familie von VPNv4-Adressen einen oder mehrere BGP-Nachbarn hinzu. Weitere Informationen finden Sie unter Abschnitt 12.11.9.2, „Einen Nachbarn hinzufügen“.
9. Verifizieren Sie die Netzwerkkonfiguration.

VRF-Lite-Konfiguration

1. Stellen Sie sicher, dass BGP aktiviert ist, und konfigurieren Sie die Autonomous System ID für das Border Gateway-Protokoll (BGP). Weitere Informationen finden Sie unter Abschnitt 12.8.1, „Konfigurieren von BGP“.
2. Konfigurieren Sie eine VRF-Definition und Ziele der Route für jeden Customer Edge-(CE)-Router. Weitere Informationen finden Sie unter Abschnitt 12.11.5.2, „Hinzufügen einer VRF-Definition“.
3. Konfigurieren Sie eine routingfähige Schnittstelle und IP-Adresse für jede VRF-Definition. Weitere Informationen finden Sie unter Abschnitt 12.11.4, „Eine VRF-Schnittstelle konfigurieren“.
4. Aktivieren Sie OSPF. Weitere Informationen finden Sie unter Abschnitt 12.9.2, „Konfigurieren des OSPF“.
5. Konfigurieren Sie eine oder mehrere VRF-Instanzen für OSPF. Weitere Informationen finden Sie unter Abschnitt 12.9.2, „Konfigurieren des OSPF“.
6. Konfigurieren Sie für jede VRF-Instanz eine Familie von IPv4-Adressen. Weitere Informationen finden Sie unter Abschnitt 12.11.10.2, „Eine Familie von IPv4-Adressen hinzufügen“.

7. Konfigurieren Sie eine oder mehrere statische VRF-Routen. Weitere Informationen finden Sie unter Abschnitt 12.11.13.2, „Hinzufügen einer statischen VRF-Route“.
8. Verifizieren Sie die Netzwerkkonfiguration.

Abschnitt 12.11.4
Eine VRF-Schnittstelle konfigurieren

Jede VRF-Definition muss mindestens einer routingfähigen Schnittstelle zugeordnet sein, der eine IP-Adresse zugewiesen wurde.

Um eine routingfähige Schnittstelle zur Weiterleitung von VRF-Verkehr für eine bestimmte VRF-Definition zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Stellen Sie die Kalkulation durch folgende Eingabe ein:

   ```
   ip interface vrf-forwarding vrf
   ```

   Erläuterung:

   - *interface* ist die Bezeichnung der routingfähigen Schnittstelle
   - *vrf* ist die gewünschte VRF-Instanz
3. Konfigurieren Sie für die Schnittstelle eine IPv4- oder IPv6-Schnittstelle. Weitere Informationen finden Sie in Abschnitt 7.1.3.2, „Eine IPv4-Adresse hinzufügen“ oder Abschnitt 7.1.4.2, „Eine IPv6-Adresse hinzufügen“.
4. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.11.5
VRF-Definitionen verwalten

VRF-Definitionen stellen einzelne CE-(Customer Edge)-Router in der VRF-Topologie dar. RUGGEDCOM ROX II unterstützt insgesamt bis zu acht Definitionen, wobei jede aus einem eindeutigen VRF-Namen, einer optionalen Beschreibung und einem Route Distinguisher (RD) besteht. Der Route Distinguisher ist ein 8-Oktett-Feld, das meist aus einer AS-Nummer oder IP-Adresse, gefolgt von einem Doppelpunkt (:) und der Standort-ID (z. B. 6500:20 oder 172.20.120.12:10) besteht. Mit dem Präfix für die IPv4-Adresse der zugehörigen Schnittstelle erkennt sie eindeutig jedes IP-Paket, wodurch der Provider Edge (PE) bestimmen kann, zu welchem VPN-Tunnel das Paket gehört.

Jeder VRF-Definition können auch ein oder mehrere Routenziele zugeordnet werden.

INHALT

- Abschnitt 12.11.5.1, „Eine Liste der VRF-Definitionen anzeigen“
- Abschnitt 12.11.5.2, „Hinzufügen einer VRF-Definition“
- Abschnitt 12.11.5.3, „Löschen einer VRF-Definition“

Abschnitt 12.11.5.1
Eine Liste der VRF-Definitionen anzeigen

Um eine Liste der VRF-Definitionen anzusehen, geben Sie Folgendes ein:

```
show running-config global vrf
```

Falls Definitionen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
show running-config global vrf | tab
global
 vrf
  definition
VRF   VRF                 EXPORT     IMPORT     BOTH
NAME  DESCRIPTION  RD     COMMUNITY  COMMUNITY  COMMUNITY
-------------------------------------------------------------
vrf1  Site A       100:1
                                                100:2
vrf2  Site B       100:2
                                                100:1

 !
!
```

Falls keine Definitionen konfiguriert wurden, fügen Sie je nach Bedarf Definitionen hinzu. Weitere Informationen finden Sie unter Abschnitt 12.11.5.2, „Hinzufügen einer VRF-Definition”.

Abschnitt 12.11.5.2
Hinzufügen einer VRF-Definition

Um eine VRF-Definition hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie die Definition hinzu, indem Sie Folgendes eingeben:

   ```
   global vrf definition name
   ```

   Erläuterung:

   - *name* ist die Bezeichnung der Definition. Die Bezeichnung muss eindeutig sein und darf nicht mehr als 32 Zeichen oder Leerzeichen enthalten. Das erste Zeichen darf kein Sonderzeichen sein. Für die übrige Bezeichnung sind nur folgende Sonderzeichen zulässig. Bindestrich (-), Unterstrich (_), Doppelpunkt (:) und Punkt (.).
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
vrf-description { vrf-description }	**Zusammenfassung:** Eine Zeichenkette mit 0 bis 256 Zeichen Eine Zeichenkette kann zur Beschreibung der VRF verwendet werden. Maximale Länge 256 Zeichen, einschließlich Leerzeichen.
rd { rd }	**Zusammenfassung:** Eine Zeichenkette mit 0 bis 32 Zeichen Das Unterscheidungsmerkmal der Route für die VRF: 8-Bit-Wert, typisches Format ist (as-number:id | ip-address:id) (z. B. 6500:20). Es wird dem IPv4-Präfix vorangestellt und erstellt so ein VPN-IPv4-Präfix. Beachten Sie, dass beim Ändern des Unterscheidungsmerkmals der Route die Routenziele beeinflusst werden: Es wird daher empfohlen nachzuprüfen, ob die konfigurierten Routenziele in Ihrem Netzwerk noch korrekt sind.

4. Fügen Sie ein oder mehrere Ziele der Route hinzu. Weitere Informationen finden Sie unter Abschnitt 12.11.6.2, „Ein Routenziel hinzufügen“.
5. Konfigurieren Sie eine routingfähige Schnittstelle für die VRF-Instanz. Weitere Informationen finden Sie unter Abschnitt 12.11.4, „Eine VRF-Schnittstelle konfigurieren“.
6. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.11.5.3
Löschen einer VRF-Definition

Um eine VRF-Definition zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Setzen Sie **vrf-forwarding** für die betreffende routingfähige Schnittstelle auf eine andere VRF-Instanz bzw. auf keine.
3. Löschen Sie die betreffende VRF-Instanz unter OSPF. Weitere Informationen finden Sie unter Abschnitt 12.11.7.3, „Eine VRF-Instanz löschen“.
4. Löschen Sie die betreffende Familie von IPv4-Adressen unter BGP. Weitere Informationen finden Sie unter Abschnitt 12.11.10.3, „Eine Familie von IPv4-Adressen löschen“.
5. Löschen Sie die Definition, indem Sie Folgendes eingeben:

   ```
   no routing vrf definition name
   ```

   Erläuterung:

   - *`name`* ist die Bezeichnung des Subnetzes
6. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.11.6
Routenziele verwalten

Routenziele legen die Routen für den Import/Export im MBGP-(Multi-Protocol BGP)-Netzwerk fest. Wie die normale globale Routing-Instanz legen die Routenziele die Import- und Export-Parameter für eine Route für BGP fest. Mit diesem Parameter kann der Benutzer angeben, welche Präfixe er zu anderen Nachbarn importieren und welche er exportieren will.

INHALT

- Abschnitt 12.11.6.1, „Eine Liste der Routenziele anzeigen“
- Abschnitt 12.11.6.2, „Ein Routenziel hinzufügen“
- Abschnitt 12.11.6.3, „Ein Routenziel löschen“

Abschnitt 12.11.6.1
Eine Liste der Routenziele anzeigen

Um eine Liste der VRF-Definitionen anzuzeigen, geben Sie Folgendes ein:

```
show running-config global vrf definition name routing-target
```

Falls Definitionen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config global vrf definition vrf1 route-target
global
 vrf
  definition vrf1
   route-target export 200:1
   !
   route-target import 200:2
   !
   route-target both 100:2
   !
  !
 !
!
```

Falls keine Definitionen konfiguriert wurden, fügen Sie je nach Bedarf Definitionen hinzu. Weitere Informationen finden Sie unter Abschnitt 12.11.5.2, „Hinzufügen einer VRF-Definition“.

Abschnitt 12.11.6.2
Ein Routenziel hinzufügen

Um ein Routenziel hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie die Definition hinzu, indem Sie Folgendes eingeben:

   ```
   global vrf definition name routing-target [ export | import | both ] community
   ```

   Erläuterung:

   - *name* ist die Bezeichnung der VRF-Definition
   - *community* ist das Unterscheidungsmerkmal der Route für die Ziel-VRF, um entweder die Routing-Tabelle in diese Ziel-VRF zu exportieren, sie von dort zu importieren oder beides.
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.11.6.3
Ein Routenziel löschen

Um ein Routenziel zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die Definition, indem Sie Folgendes eingeben:

   ```
   no global vrf definition name routing-target [ export | import | both ] community
   ```

   Erläuterung:

   - *name* ist die Bezeichnung der VRF-Definition
   - *community* ist das Unterscheidungsmerkmal der Route für die Ziel-VRF, um entweder die Routing-Tabelle in diese Ziel-VRF zu exportieren, sie von dort zu importieren oder beides.

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.11.7
VRF-Instanzen und OSPF verwalten

OSPF kann für eine oder mehrere VRF-Definitionen konfiguriert werden. Hierfür wird OSPF für eine VRF-Instanz aktiviert und dann werden die erforderlichen OSPF-Parameter konfiguriert.

OSPF kann an jeder physikalischen oder geschalteten Schnittstelle sowie an VRF-Lite-Schnittstellen (IPv4) und Full-VRF-Schnittstellen (IP/VPN mit MPLS) laufen.

INHALT

- Abschnitt 12.11.7.1, „Eine Liste der VRF-Instanzen anzeigen“
- Abschnitt 12.11.7.2, „Hinzufügen einer VRF-Instanz und Konfigurieren von OSPF“
- Abschnitt 12.11.7.3, „Eine VRF-Instanz löschen“

Abschnitt 12.11.7.1
Eine Liste der VRF-Instanzen anzeigen

Um eine Liste der für OSPF definierten VRF-Instanzen anzusehen, geben Sie Folgendes ein:

```
show running-config routing ospf vrf
```

Falls Definitionen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config routing ospf vrf
routing ospf
 vrf VRF1
  enabled
.
.
.
 vrf VRF2
  enabled
.
.
.
```

Falls keine Definitionen konfiguriert wurden, fügen Sie je nach Bedarf Definitionen hinzu. Weitere Informationen finden Sie unter Abschnitt 12.11.5.2, „Hinzufügen einer VRF-Definition“.

Abschnitt 12.11.7.2
Hinzufügen einer VRF-Instanz und Konfigurieren von OSPF

Um eine VRF-Instanz hinzuzufügen und OSPF zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***routing » dynamic » ospf » vrf*** und konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
{ vrf-name }	**Zusammenfassung:** Eine Zeichenkette Die Bezeichnung der VRF.
enabled	Aktiviert das dynamische OSPF-Routing-Protokoll.
abr-type { abr-type }	**Zusammenfassung:** { cisco, ibm, shortcut, standard } **Standard:** cisco Der Typ OSPF ABR.
auto-cost-reference-bandwidth { auto-cost-reference-bandwidth }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 1 und 4294967 **Standard:** 100 Berechnet die OSPF-Schnittstellenkosten entsprechend der Bandbreite [1-4294967 Mbit/s]
compatible-rfc1583	Sorgt für Kompatibilität mit dem obsoleten RFC1583 OSPF (aktuell ist RFC2178)
default-information-originate	Kündigt die voreingestellte Route an.
default-metric { default-metric }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 0 und 16777214 Die Standard-Metrik der "Redistribute"-Routen.
distance { distance }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 1 und 255 Die administrative Distanz.
opaque-lsa	Aktiviert die Opaque-LSA-Funktion (RFC2370).
passive-default	**Zusammenfassung:** { true, false } **Standard:** true Passiver Standardwert für eine neue Schnittstelle.
refresh-timer { refresh-timer }	**Zusammenfassung:** Eine vorzeichenlose 16-Bit-Ganzzahl zwischen 10 und 1800 **Standard:** 10 Der Refresh-Timer.
router-id { router-id }	**Zusammenfassung:** Eine Zeichenkette mit 7 bis 15 Zeichen Die Router-ID für OSPF.
always	**Zusammenfassung:** { true, false } **Standard:** false Gibt immer die Standard-Route an, auch wenn in der Routingtabelle keine Standard-Route vorhanden ist.
metric { metric }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 0 und 16777214 Der metrische Wert für die Standard-Route.
metric-type { metric-type }	**Zusammenfassung:** Eine vorzeichenbehaftete 8-Bit-Ganzzahl zwischen 1 und 2 **Standard:** 2 Der metrische Typ für die Standard-Route.
route-map { route-map }	**Zusammenfassung:** Eine Zeichenkette Die Bezeichnung der Route-Map.
external { external }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 1 und 255 Die administrative Distanz für externe Routen.
inter-area { inter-area }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 1 und 255 Die administrative Distanz für Inter-Area-Routen.
intra-area { intra-area }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 1 und 255

Parameter	Beschreibung
	Die administrative Distanz für Intra-Area-Routen.

3. Konfigurieren Sie Präfixlistenfilter für die VRF-Instanz. Weitere Informationen finden Sie unter Abschnitt 12.9.4.3, „Hinzufügen einer Präfixliste“.
4. Konfigurieren Sie Bereiche für die VRF-Instanz. Weitere Informationen finden Sie unter Abschnitt 12.9.5.2, „Hinzufügen eines Bereichs“.
5. Konfigurieren Sie Route-Map-Filter für die VRF-Instanz. Weitere Informationen finden Sie unter Abschnitt 12.9.6.3, „Hinzufügen eines Route-Map-Filters“.
6. Konfigurieren Sie Umverteilungsmetriken für die VRF-Instanz. Weitere Informationen finden Sie unter Abschnitt 12.9.8.2, „Hinzufügen einer Umverteilungsmetrik“.
7. Konfigurieren Sie Schnittstellen für die VRF-Instanz. Weitere Informationen finden Sie unter Abschnitt 12.9.9.2, „Eine Routing-Schnittstelle konfigurieren“.
8. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.11.7.3
Eine VRF-Instanz löschen

Um eine VRF-Instanz unter OSPF zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den Definitionsschlüssel durch Eingabe von:

```
no routing ospf vrf name
```

   Erläuterung:

   - *`name`* ist die Bezeichnung der VRF-Instanz
3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.11.8
IP/VPN-Tunnel verwalten

IP/VPN-Tunnel nutzen das VPNv4-Protokoll für den Austausch von Kunden-Präfixen (d. h. Routenverteilungen und Routenziele) und Labels zwischen Provider Edge (PE)-Routern. IP/VPNs ermöglichen die Trennung der Schnittstellen, die jedes Ende des VPN verbinden.

HINWEIS
VRF pflegt eine Tabelle mit allen Schnittstellen, die zu jedem IP/VPN-Tunnel gehören.

INHALT

- Abschnitt 12.11.8.1, „Eine Liste der IP/VPN-Tunnel anzeigen“
- Abschnitt 12.11.8.2, „Einen IP-/VPN-Tunnel hinzufügen“

- Abschnitt 12.11.8.3, „Einen IP/VPN-Tunnel löschen“

Abschnitt 12.11.8.1
Eine Liste der IP/VPN-Tunnel anzeigen

Um eine Liste der für VRF konfigurierten IP/VPN-Tunnel anzuzeigen, geben Sie Folgendes ein:

```
show running-config routing bgp address-family vpnv4
```

Eine Tabelle oder Liste ähnlich dem folgenden Beispiel wird angezeigt:

```
ruggedcom# show running-config routing bgp address-family vpnv4 | tab
routing bgp
 address-family vpnv4
  neighbor
         SEND
IP       COMMUNITY
--------------------
1.2.6.2  both

 !
!
```

Abschnitt 12.11.8.2
Einen IP-/VPN-Tunnel hinzufügen

Um für VRF einen neuen IP-/VPN-Tunnel hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den Nachbarn hinzu, indem Sie Folgendes eingeben:

   ```
   routing bgp address-family vpnv4 neighbor address send-community [ both | extended | none |
   standard ]
   ```

   Erläuterung:

   - *address* ist die IP-Adresse des Nachbarn
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.11.8.3
Einen IP/VPN-Tunnel löschen

Um einen IP/VPN-Tunnel zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die Adresse, indem Sie Folgendes eingeben:

   ```
   no routing bgp address-family vpnv4 neighbor address
   ```

   Erläuterung:

   - *address* ist die IP-Adresse des Nachbarn

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.11.9
VPNv4-Nachbarn verwalten

VPNv4-Nachbarn sind andere Router, mit denen Routen ausgetauscht werden. Damit VRF-Lite funktionieren kann, müssen ein oder mehrere Nachbarn angegeben werden.

INHALT

- Abschnitt 12.11.9.1, „Eine Liste der Nachbarn anzeigen“
- Abschnitt 12.11.9.2, „Einen Nachbarn hinzufügen“
- Abschnitt 12.11.9.3, „Einen Nachbarn löschen“

Abschnitt 12.11.9.1
Eine Liste der Nachbarn anzeigen

Um eine Liste der konfigurierten VPNv4-Nachbarn anzusehen, geben Sie Folgendes ein:

```
show running-config routing bgp address-family vpnv4 neighbor
```

Falls Nachbarn konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config routing bgp address-family vpnv4 neighbor | tab
          SEND
IP        COMMUNITY
--------------------
1.2.6.2   both

 !
!
```

Falls keine Nachbarn konfiguriert wurden, fügen Sie je nach Bedarf Nachbarn hinzu. Weitere Informationen finden Sie unter Abschnitt 12.11.12.2, „Einen Nachbarn hinzufügen“.

Abschnitt 12.11.9.2
Einen Nachbarn hinzufügen

Um einen neuen VPNv4-Nachbarn hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den Nachbarn hinzu, indem Sie Folgendes eingeben:

   ```
   routing bgp address-family vpnv4 neighbor address send-community [ both | extended | none |
   standard ]
   ```

   Erläuterung:

   - *`address`* ist die IP-Adresse des Nachbarn
3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.11.9.3
Einen Nachbarn löschen

Um einen VPNv4-Nachbarn zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie das Netzwerk durch Eingabe von:

   ```
   no routing bgp address-family vpnv4 neighbor address
   ```

   Erläuterung:

   - *address* ist die IP-Adresse des Nachbarn
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.11.10
IPv4-Adressfamilien verwalten

IPv4-Adressfamilien werden bei der Implementierung von VRF-Lite konfiguriert. Adressfamilien in BGP geben die Nachbarn an, mit denen der Router die VRF-Routinginformationen teilt und welche Methode für die Routingverteilung zulässig ist. Für jede VRF-Instanz können eine oder mehrere Adressfamilien konfiguriert werden.

Die Routenverteilung kann auf direkt angebundene Routen, statische Routen oder von OSPF eingelernte Routen beschränkt werden.

INHALT

- Abschnitt 12.11.10.1, „Eine Liste der IPv4-Adressfamilien anzeigen“
- Abschnitt 12.11.10.2, „Eine Familie von IPv4-Adressen hinzufügen“
- Abschnitt 12.11.10.3, „Eine Familie von IPv4-Adressen löschen“

Abschnitt 12.11.10.1
Eine Liste der IPv4-Adressfamilien anzeigen

Um eine Liste der für VRF konfigurierten IPv4-Adressfamilien anzuzeigen, geben Sie Folgendes ein:

```
show running-config routing bgp address-family ipv4 vrf
```

Falls IPv4-Adressfamilien konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config routing bgp address-family ipv4 vrf
routing bgp
 address-family ipv4
  vrf VRF1
   redistribute connected
    no metric
    no route-map
   !
   redistribute ospf
    no metric
    no route-map
   !
```

```
   redistribute static
    no metric
    no route-map
   !
  !
 !
!
```

Falls keine IPv4-Adressfamilien konfiguriert wurden, fügen Sie nach Bedarf Adressfamilien hinzu. Weitere Informationen finden Sie unter Abschnitt 12.11.10.2, „Eine Familie von IPv4-Adressen hinzufügen“.

Abschnitt 12.11.10.2
Eine Familie von IPv4-Adressen hinzufügen

Um eine Familie von IPv4-Adressen hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie die Familie von IPv4-Adressen hinzu, indem Sie Folgendes eingeben:

   ```
   routing bgp address-family ipv4 vrf vrf
   ```

   Erläuterung:

   - *vrf* ist die Bezeichnung der zugehörigen VRF-Definition
3. Fügen Sie einen oder mehrere Nachbarn hinzu. Weitere Informationen finden Sie unter Abschnitt 12.11.12.2, „Einen Nachbarn hinzufügen“.
4. Fügen Sie eine oder mehrere Umverteilungen hinzu. Für weitere Informationen siehe Abschnitt 12.11.11.2, „Eine Umverteilung hinzufügen“.
5. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.11.10.3
Eine Familie von IPv4-Adressen löschen

Um eine Familie von IPv4-Adressen zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die Familie von IPv4-Adressen, indem Sie Folgendes eingeben:

   ```
   no routing bgp address-family ipv4 vrf vrf
   ```

   Erläuterung:

   - *vrf* ist die Bezeichnung der zugehörigen VRF-Definition
3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.11.11

Umverteilung für IPv4-Adressfamilien verwalten

Die Umverteilung ist im Allgemeinen die Mitteilung von Routen durch ein Protokoll, die über ein anderes dynamisches Routing-Protokoll, eine statische Route oder einen direkt angebundenen Router eingelernt wurden. Damit soll die Interoperabilität zwischen Netzwerken, auf denen verschiedene Routing-Protokolle laufen, verbessert werden. Bei VRF wird das dynamische OSPF-Routing-Protokoll unterstützt.

Für jede VRF-Instanz können eine oder mehrere Umverteilungen festgelegt werden. Mit einer Umverteilung wird die Quelle der Routing-Informationen, eine Metrik und (optional) eine vordefinierte Routing-Karte festgelegt.

Die Metrik wird für Entscheidungen über die Route innerhalb des autonomen Systems (AS) verwendet. Es muss sorgfältig darauf geachtet werden, dass die Metrik vom OSPF-Routing-Protokoll verstanden wird.

INHALT

- Abschnitt 12.11.11.1, „Eine Liste der Umverteilungen anzeigen“
- Abschnitt 12.11.11.2, „Eine Umverteilung hinzufügen“
- Abschnitt 12.11.11.3, „Eine Umverteilung löschen“

Abschnitt 12.11.11.1

Eine Liste der Umverteilungen anzeigen

Um eine Liste von Umverteilungen für eine Familie von IPv4-Adressen anzusehen, geben Sie Folgendes ein:

```
show running-config routing bgp address-family ipv4 vrf vrf redistribute
```

Erläuterung:

- *vrf* ist die gewählte VRF-Instanz

Falls Umverteilungen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config routing bgp address-family ipv4 vrf VRF1 redistribute | tab
                   ROUTE
SOURCE     METRIC  MAP
-------------------------
connected  -       -
ospf       -       -
static     -       -

  !
 !
!
```

Falls keine Umverteilungen konfiguriert sind, fügen Sie nach Bedarf Umverteilungen hinzu. Weitere Informationen finden Sie unter Abschnitt 12.11.11.2, „Eine Umverteilung hinzufügen“.

Abschnitt 12.11.11.2

Eine Umverteilung hinzufügen

Um für eine Familie von IPv4-Adressen eine Umverteilung hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie die Umverteilung hinzu, indem Sie Folgendes eingeben:

```
routing bgp address-family ipv4 vrf vrf redistribute [ connected | ospf | static ]
```

Erläuterung:

- *vrf* ist die gewählte VRF-Instanz

3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
metric { metric }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 0 und 4294967295 Die Metrik für umverteilte Routen.
route-map { route-map }	**Zusammenfassung:** Eine Zeichenkette Die Bezeichnung der Route-Map.

4. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.11.11.3
Eine Umverteilung löschen

Um die für eine Familie von IPv4-Adressen definierte Umverteilung zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die Umverteilung, indem Sie Folgendes eingeben:

```
no routing bgp address-family ipv4 vrf vrf redistribute [ connected | ospf | static ]
```

Erläuterung:

- *vrf* ist die gewählte VRF-Instanz

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.11.12
Nachbarn für IPv4-Adressfamilien verwalten

Nachbarn sind andere Router, mit denen Routen ausgetauscht werden. Damit VRF funktionieren kann, müssen ein oder mehrere Nachbarn angegeben werden.

INHALT

- Abschnitt 12.11.12.1, „Eine Liste der Nachbarn anzeigen“
- Abschnitt 12.11.12.2, „Einen Nachbarn hinzufügen“
- Abschnitt 12.11.12.3, „Konfigurieren der Verteilung von Präfixlisten“
- Abschnitt 12.11.12.4, „Nachverfolgen von Befehlen“
- Abschnitt 12.11.12.5, „Einen Nachbarn löschen“

Abschnitt 12.11.12.1

Eine Liste der Nachbarn anzeigen

Um eine Liste von Nachbarn anzuzeigen, die für eine Familie von IPv4-Adressen konfiguriert sind, geben Sie Folgendes ein:

```
show running-config routing bgp address-family ipv4 vrf vrf neighbor
```

Erläuterung:

- *vrf* ist die gewählte VRF-Instanz

Falls Nachbarn konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
show running-config routing bgp address-family ipv4 vrf VRF1 neighbor
routing bgp
 address-family ipv4
  vrf VRF1
   neighbor 192.168.12.30
    remote-as 1
    no ebgp-multihop
    no maximum-prefix
    no next-hop-self
    no password
    no disable-connected-check
    no soft-reconfiguration
    no weight
    no route-map in
    no route-map out
   !
  !
 !
!
```

Falls keine Nachbarn konfiguriert wurden, fügen Sie je nach Bedarf Nachbarn hinzu. Weitere Informationen finden Sie unter Abschnitt 12.11.12.2, „Einen Nachbarn hinzufügen“.

Abschnitt 12.11.12.2

Einen Nachbarn hinzufügen

Um einen neuen Nachbarn zu einer Familie von IPv4-Adressen hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den Nachbarn hinzu, indem Sie Folgendes eingeben:

   ```
   routing bgp address-family ipv4 vrf vrf neighbor address
   ```

   Erläuterung:

   - *vrf* ist die gewählte VRF-Instanz
   - *address* ist die IP-Adresse des Nachbarn
3. Konfigurieren Sie die Neighbor-Einstellungen mithilfe der folgenden Parameter:

Parameter	Beschreibung
send-community { send-community }	**Zusammenfassung:** { standard, extended, both, none } **Standard:** both Identifiziert die Senden-Community. Die Voreinstellung ist "both".
remote-as { remote-as }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 1 und 65535

Parameter	Beschreibung
	Ein BGP-Nachbar. Dieser Parameter ist obligatorisch.
ebgp-multihop { ebgp-multihop }	**Zusammenfassung:** Eine vorzeichenlose 8-Bit-Ganzzahl zwischen 1 und 255 Die maximale Hop-Zählung. Dadurch sind EBGP-Nachbarn an nicht direkt verbundenen Netzwerken zulässig.
maximum-prefix { maximum-prefix }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 1 und 4294967295 Die maximale Präfixnummer, die von diesem Peer angenommen wird.
next-hop-self	Deaktiviert die Berechnung des nächsten Hops für diesen Nachbarn.
password { password }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 1024 Zeichen Passwort.
update-source { update-source }	**Zusammenfassung:** Eine Zeichenkette mit 7 bis 15 Zeichen IP-Quelladresse von Routing-Updates.
disable-connected-check	Deaktiviert die Verbindungsüberprüfung beim Einrichten einer eBGP-Peering-Sitzung mit einem Single-Hop-Peer, der eine Loopback-Schnittstelle verwendet.
soft-reconfiguration	Soft-Rekonfiguration je Nachbar.
weight { weight }	**Zusammenfassung:** Eine vorzeichenlose 16-Bit-Ganzzahl Das Standardgewicht für Routen von diesem Nachbarn.

4. Konfigurieren Sie die Route Map-Einstellungen mithilfe der folgenden Parameter:

Parameter	Beschreibung
in { in }	**Zusammenfassung:** Eine Zeichenkette Route-Map auf eingehende Routen anwenden.
out { out }	**Zusammenfassung:** Eine Zeichenkette Route-Map auf ausgehende Routen anwenden.

5. Konfigurieren Sie die Präfixlisten-Verteilung. Weitere Informationen finden Sie unter Abschnitt 12.11.12.3, „Konfigurieren der Verteilung von Präfixlisten“.
6. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.11.12.3
Konfigurieren der Verteilung von Präfixlisten

Um die Verteilung von Präfixlisten für einen Nachbarn in einer Familie von IPv4-Adressen zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Übernehmen Sie die gewünschte Präfixliste in die gewählte Routenrichtung, indem Sie Folgendes eingeben:

```
routing bgp address-family ipv4 vrf vrf neighbor address distribute-prefix-list [ in | out ]
prefix-list prefix
```

Erläuterung:

- *`vrf`* ist die gewählte VRF-Instanz

- *address* ist die Adresse des gewählten Nachbarn
- *prefix* ist die gewählte BGP-Präfixliste

3. Konfigurieren Sie bei Bedarf einen Event Tracker, um die Netzwerkbefehle zu beobachten. Weitere Informationen finden Sie unter Abschnitt 12.11.12.4, „Nachverfolgen von Befehlen“.
4. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.11.12.4
Nachverfolgen von Befehlen

Netzwerkbefehle lassen sich mithilfe von Event Trackern, die unter ***global » tracking*** konfiguriert werden, nachverfolgen. Weitere Informationen über Event Tracker finden Sie in Abschnitt 12.5, „Event-Tracker verwalten“.

Ein Netzwerkbefehl wird in Abhängigkeit vom Status des Event Trackers aktiviert. Der Parameter `apply-when` bestimmt, wann der Befehl aktiviert wird. Beispiel: Wenn der Parameter `apply-when` auf **down**gesetzt ist, wird der Netzwerkbefehl aktiv (und kündigt dadurch das Netzwerk den RIP-Peers eines Routers an), wenn das nachverfolgte Ziel nicht verfügbar ist.

Um einen Befehl für eine Familie von IPv4-Adressen nachzuverfolgen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***routing » dynamic » bgp » address-family » ipv4 » {vrf} » neighbor » {address} » distribute-prefix-list » In|out***, wobei *{vrf}* die gewählte VRF-Instanz und *{address}* die IP-Adresse des Nachbarn ist.
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
event { event }	**Zusammenfassung:** Eine Zeichenkette Markiert das Tracken eines Ereignisses, wobei die "distribute-prefix-list" nur anzuwenden ist, wenn das getrackte Ereignis verfügbar ("UP") wird. Dieser Parameter ist obligatorisch.
apply-when { apply-when }	**Zusammenfassung:** { up, down } **Standard:** up Wendet die "distribute-prefix-list" an, wenn das getrackte Ereignis verfügbar ("UP") oder nicht verfügbar ("DOWN") wird.

4. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.11.12.5
Einen Nachbarn löschen

Um ein VPNv4-Nachbarn zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie das Netzwerk, indem Sie Folgendes eingeben:

```
no routing address-family ipv4 vrf vrf neighbor address
```

Erläuterung:

- *vrf* ist die gewählte VRF-Instanz
- *address* ist die IP-Adresse des Nachbarn

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.11.13
Statische VRF-Routen verwalten

Routing-Informationen können zwischen Routern entweder mit Hilfe dynamischer Routing-Daten ausgetauscht oder manuell konfiguriert werden. Statische Routen sind explizite Pfade zwischen Routern, die manuell konfiguriert werden. Statische Routen werden normalerweise für stabile, oft kleinere Netzwerke verwendet, deren Konfiguration sich kaum ändert. Sie können als Ergänzung zu dynamischen Routen verwendet werden.

INHALT

- Abschnitt 12.11.13.1, „Eine Liste der statischen VRF-Routen anzeigen“
- Abschnitt 12.11.13.2, „Hinzufügen einer statischen VRF-Route“
- Abschnitt 12.11.13.3, „Eine Black-Hole-Verbindung für eine statische VRF-Route konfigurieren“
- Abschnitt 12.11.13.4, „Eine statische VRF-Route löschen“

Abschnitt 12.11.13.1
Eine Liste der statischen VRF-Routen anzeigen

Um eine Liste routingfähiger Ethernet-Ports anzusehen, geben Sie Folgendes ein:

```
show running-config routing vrf vrf ipv4
```

Erläuterung:

- *vrf* ist die gewählte VRF-Instanz

Falls Routen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config routing vrf VRF1 ipv4 | tab
                          HW
NETWORK          DISTANCE  ACCELERATE  GW       DISTANCE  INTERFACE  DISTANCE
-------------------------------------------------------------------------------
192.168.10.0/24  -         -
                                       1.9.5.1  -

!
```

Falls keine statischen Routen konfiguriert wurden, fügen Sie je nach Bedarf Routen hinzu. Weitere Informationen finden Sie unter Abschnitt 12.11.13.2, „Hinzufügen einer statischen VRF-Route“.

Abschnitt 12.11.13.2
Hinzufügen einer statischen VRF-Route

Um eine statische IPv4-Route für eine VRF-Instanz hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.

2. Fügen Sie eine statische VRF-Route hinzu, indem Sie Folgendes eingeben:

```
routing vrf vrf ipv4 route subnet
```

Erläuterung:

- *vrf* ist die gewählte VRF-Instanz
- *subnet* ist das Subnetz (Netzwerk/Präfix) der statischen Route

3. Wenn auf dem Gerät ein Layer-3-Switch installiert ist, konfigurieren Sie je nach Bedarf die folgenden Parameter:

HINWEIS
Es werden ausschließlich TCP- und UDP-Verkehrsströme von der IP/Layer-3-Switching-Fabric beschleunigt. Nicht-IP-Pakettypen wie beispielsweise ICMP und IGMP werden nicht beschleunigt.

Parameter	Beschreibung
hw-accelerate	Wenn die statische Unicast-Route hardwarebeschleunigt werden kann, ist diese Option verfügbar. Damit eine statische Unicast-Route hardwarebeschleunigt werden kann, müssen die eingehenden und ausgehenden Schnittstellen umgeschaltet werden.

4. Konfigurieren Sie je nach Bedarf eine Black-Hole-Verbindung für die statische Route. Weitere Informationen finden Sie unter Abschnitt 12.11.13.3, „Eine Black-Hole-Verbindung für eine statische VRF-Route konfigurieren“.
5. Fügen Sie je nach Bedarf Gateways für die statische Route hinzu. Weitere Informationen finden Sie unter Abschnitt 12.11.14.2, „Hinzufügen eines Gateway für eine statische VRF-Route“.
6. Fügen Sie je nach Bedarf Schnittstellen für die statische Route hinzu. Weitere Informationen finden Sie unter Abschnitt 12.11.15.2, „Hinzufügen eines Gateway für eine statische VRF-Route“.
7. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.11.13.3

Eine Black-Hole-Verbindung für eine statische VRF-Route konfigurieren

Um eine Black-Hole-Verbindung für eine statische VRF-Route zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Konfigurieren Sie die Black-Hole-Verbindung, indem Sie Folgendes eingeben:

```
routing vrf vrf ipv4 route subnet blackhole distance distance
```

Erläuterung:

- *vrf* ist die gewählte VRF-Instanz.
- *subnet* ist das Subnetz (Netzwerk/Präfix) der statischen Route.
- *distance* ist die administrative Distanz. Der Standardwert ist 1.

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.11.13.4
Eine statische VRF-Route löschen

Um eine statische IPv4-Route für eine VRF-Instanz zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die statische-Route, indem Sie Folgendes eingeben:

   ```
   no routing vrf vrf ipv4 route subnet
   ```

   Erläuterung:

   - *vrf* ist die gewählte VRF-Instanz
   - *subnet* ist das Subnetz (Netzwerk/Präfix) der statischen Route
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.11.14
Gateways für statische VRF-Routen verwalten

Dieser Abschnitt beschreibt, wie Sie Gateways für statische VRF-Routen konfigurieren und verwalten können.

INHALT

- Abschnitt 12.11.14.1, „Eine Liste der Gateways für statische VRF-Routen anzeigen“
- Abschnitt 12.11.14.2, „Hinzufügen eines Gateway für eine statische VRF-Route“
- Abschnitt 12.11.14.3, „Ein Gateway für eine statische VRF-Route löschen“

Abschnitt 12.11.14.1
Eine Liste der Gateways für statische VRF-Routen anzeigen

Um eine Liste der Gateway-Adressen, die einer statischen IPv4-Route zugewiesen sind, anzuzeigen, geben Sie Folgendes ein:

```
show running-config routing vrf vrf ipv4 route subnet via
```

Erläuterung:

- *vrf* ist die gewählte VRF-Instanz.
- *subnet* ist das Subnetz (Netzwerk/Präfix) der statischen Route

Falls Gateway-Adressen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config routing vrf VRF1 ipv4 route via | tab
NETWORK          GW       DISTANCE
-------------------------------------
192.168.10.0/24
                 1.9.5.1  -

!
```

Falls keine Gateway-Adressen konfiguriert wurden, fügen Sie je nach Bedarf Adressen hinzu. Weitere Informationen finden Sie unter Abschnitt 12.11.14.2, „Hinzufügen eines Gateway für eine statische VRF-Route“.

Abschnitt 12.11.14.2
Hinzufügen eines Gateway für eine statische VRF-Route

Um ein Gateway für eine statische VRF-Route hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie die Gateway-Adresse hinzu, indem Sie Folgendes eingeben:

   ```
   routing vrf vrf ipv4 route subnet via gateway
   ```

   Erläuterung:

   - *vrf* ist die gewählte VRF-Instanz.
   - *subnet* ist das Subnetz (Netzwerk/Präfix) der statischen Route
   - *gateway* ist die Gateway-Adresse für die statische Route
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
distance { distance }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 1 und 255 Der Abstand für die statische Route.

4. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.11.14.3
Ein Gateway für eine statische VRF-Route löschen

Um eine Gateway-Adresse, die einer statischen VRF-Route zugewiesen ist, zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die Gateway-Adresse, indem Sie Folgendes eingeben:

   ```
   no routing vrf vrf ipv4 route subnet via gateway
   ```

   Erläuterung:

   - *vrf* ist die gewählte VRF-Instanz.
   - *subnet* ist das Subnetz (Netzwerk/Präfix) der statischen Route
   - *gateway* ist die Gateway-Adresse für die statische Route
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.11.15

Schnittstellen für statische VRF-Routen verwalten

Dieser Abschnitt beschreibt, wie Sie Schnittstellen für statische VRF-Routen verwalten können.

INHALT

- Abschnitt 12.11.15.1, „Eine Liste der Schnittstellen für statische VRF-Routen anzeigen“
- Abschnitt 12.11.15.2, „Hinzufügen eines Gateway für eine statische VRF-Route“
- Abschnitt 12.11.15.3, „Ein Gateway für eine statische VRF-Route löschen“

Abschnitt 12.11.15.1

Eine Liste der Schnittstellen für statische VRF-Routen anzeigen

Um eine Liste der Schnittstellen, die einer statischen IPv4-Route zugewiesen sind, anzuzeigen, geben Sie Folgendes ein:

```
show running-config routing vrf vrf ipv4 route dev
```

Erläuterung:

- *vrf* ist die gewählte VRF-Instanz.

Falls Gateway-Adressen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config routing vrf VRF1 ipv4 route dev | tab
NETWORK          INTERFACE  DISTANCE
--------------------------------------
192.168.10.0/24
                 fe-cm-1    -

!
```

Falls keine Gateway-Adressen konfiguriert wurden, fügen Sie je nach Bedarf Adressen hinzu. Weitere Informationen finden Sie unter Abschnitt 12.11.15.2, „Hinzufügen eines Gateway für eine statische VRF-Route“.

Abschnitt 12.11.15.2

Hinzufügen eines Gateway für eine statische VRF-Route

Um eine Schnittstelle für eine statische VRF-Route hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie die Gateway-Adresse hinzu, indem Sie Folgendes eingeben:

   ```
   routing vrf vrf ipv4 route subnet dev interface
   ```

   Erläuterung:

   - *vrf* ist die gewählte VRF-Instanz.
   - *subnet* ist das Subnetz (Netzwerk/Präfix) der statischen Route
   - *interface* ist die Bezeichnung der Schnittstelle für die statische Route
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
distance { distance }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 1 und 255 Der Abstand für die statische Route.

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.11.15.3
Ein Gateway für eine statische VRF-Route löschen

Um eine Schnittstelle, die einer statischen VRF-Route zugewiesen ist, zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die Gateway-Adresse, indem Sie Folgendes eingeben:

```
no routing vrf vrf ipv4 route subnet dev gateway
```

Erläuterung:

- *`vrf`* ist die gewählte VRF-Instanz.
- *`subnet`* ist das Subnetz (Netzwerk/Präfix) der statischen Route
- *`interface`* ist die Bezeichnung der Schnittstelle für die statische Route

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.12
Statische Routen verwalten

Statische Routen können manuell in der Routing-Tabelle hinzugefügt werden, wenn keine anderen Router Benachrichtigungen über Änderungen der Netzwerktopologie senden.

INHALT

- Abschnitt 12.12.1, „Eine Liste der statischen Routen anzeigen“
- Abschnitt 12.12.2, „Hinzufügen einer statischen IPv4-Route“
- Abschnitt 12.12.3, „Eine statische IPv6-Route hinzufügen“
- Abschnitt 12.12.4, „Eine statische Route löschen“
- Abschnitt 12.12.5, „Eine Black-Hole-Verbindung für eine statische IPv4-Route konfigurieren“
- Abschnitt 12.12.6, „Gateways für statische Routen verwalten“
- Abschnitt 12.12.7, „Schnittstellen für statische Routen verwalten“

Abschnitt 12.12.1
Eine Liste der statischen Routen anzeigen

Um eine Liste routingfähiger Ethernet-Ports anzusehen, geben Sie Folgendes ein:

```
show running-config routing protocol
```

Erläuterung:

- *protocol* ist entweder *IPv4* oder *IPv6*

Falls Routen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config routing ipv4 | tab
                         HW
NETWORK          DISTANCE  ACCELERATE  GW             DISTANCE  INTERFACE    DISTANCE
-------------------------------------------------------------------------------------
0.0.0.0/0        -         -
                                       172.30.128.1   -
                                                                switch.0001  -
10.200.16.0/20   -         -
```

Falls keine statischen Routen konfiguriert wurden, fügen Sie je nach Bedarf Routen hinzu. Weitere Informationen finden Sie unter Abschnitt 12.12.2, „Hinzufügen einer statischen IPv4-Route“ oder Abschnitt 12.12.3, „Eine statische IPv6-Route hinzufügen“.

Abschnitt 12.12.2
Hinzufügen einer statischen IPv4-Route

Um eine statische IPv4-Route hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.

   WICHTIG!
   Wenn die Route als Black-Hole-Route zu konfigurieren ist, stellen Sie sicher, dass das Subnetz mit dem Subnetz einer anderen statischen Route übereinstimmt. Die Black-Hole-Route agiert dann als Backup-Route, falls die andere statische Route ausfällt.

2. Fügen Sie die statische IPv4-Route hinzu, indem Sie Folgendes eingeben:

   ```
   routing ipv4 route subnet
   ```

   Erläuterung:

   - *subnet* ist das Subnetz (Netzwerk/Präfix) der statischen Route

3. Wenn auf dem Gerät ein Layer-3-Switch installiert ist, konfigurieren Sie je nach Bedarf die folgenden Parameter:

   HINWEIS
   Es werden ausschließlich TCP- und UDP-Verkehrsströme von der IP/Layer-3-Switching-Fabric beschleunigt. Nicht-IP-Pakettypen wie beispielsweise ICMP und IGMP werden nicht beschleunigt.

Parameter	Beschreibung
hw-accelerate	Wenn die statische Unicast-Route hardwarebeschleunigt werden kann, ist diese Option verfügbar. Damit eine statische Unicast-Route hardwarebeschleunigt werden kann, müssen die eingehenden und ausgehenden Schnittstellen umgeschaltet werden.

4. [Optional] Konfigurieren Sie die Route als Black-Hole-Route. Weitere Informationen finden Sie unter Abschnitt 12.12.5, „Eine Black-Hole-Verbindung für eine statische IPv4-Route konfigurieren“.
5. [Optional] Wenn die statische Route keine Black-Hole-Route ist, konfigurieren Sie entweder die Schnittstelle zum Next-Hop-Router (bei Vorhandensein einer direkten Verbindung) oder die IP-Adresse (Gateway) des Next-Hop-Routers. Je statische Route kann nur eine konfiguriert werden. Für weitere Informationen siehe Abschnitt 12.12.6.3, „Ein Gateway für eine statische IPv4-Route hinzufügen“ oder Abschnitt 12.12.7.3, „Eine Schnittstelle für eine statische IPv4-Route hinzufügen“.
6. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.12.3
Eine statische IPv6-Route hinzufügen

Um eine statische IPv6-Route hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie die statische Ipv6-Route hinzu, indem Sie Folgendes eingeben:

   ```
   routing ipv6 route subnet
   ```

   Erläuterung:

   - *`subnet`* ist das Subnetz (Netzwerk/Präfix) der statischen Route
3. Konfigurieren Sie die IP-Adresse des nächsten Hops (Gateway) oder Schnittstelle. Je statischer Route kann nur eine konfiguriert werden. Weitere Informationen finden Sie in Abschnitt 12.12.6.1, „Gateways für statische IPv6-Routen konfigurieren“ oder Abschnitt 12.12.7.1, „Schnittstellen für statische Ipv6-Routen konfigurieren“.
4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.12.4
Eine statische Route löschen

Um eine statische Route zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die statische-Route, indem Sie Folgendes eingeben:

   ```
   no routing protocol route subnet
   ```

   Erläuterung:

   - *`protocol`* ist entweder *IPv4* oder *IPv6*
   - *`subnet`* ist das Subnetz (Netzwerk/Präfix) der statischen Route
3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.12.5

Eine Black-Hole-Verbindung für eine statische IPv4-Route konfigurieren

Um eine Black-Hole-Verbindung für eine statische IPv4-Route zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***routing » ipv4 » {subnet} » blackhole***, wobei *subnet* das Subnetz (Netzwerk/Präfix) der statischen Route ist.
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
distance { distance }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 1 und 255 **Standard:** 1 Der Abstand für das Blackhole dieser statischen Route. Voreinstellung ist 1.

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.12.6

Gateways für statische Routen verwalten

Wenn das Gerät nicht direkt mit dem Next-Hop-Router verbunden ist, können Sie eine statische Route für die Weiterleitung des Verkehrs zur IP-Adresse des Next-Hop-Routers konfigurieren. Dies wird als *Gateway* bezeichnet.

Bei statischen IPv6-Routen kann pro Route nur ein Gateway ausgewählt werden.

INHALT

- Abschnitt 12.12.6.1, „Gateways für statische IPv6-Routen konfigurieren“
- Abschnitt 12.12.6.2, „Eine Liste der Gateways für statische IPv4-Routen anzeigen“
- Abschnitt 12.12.6.3, „Ein Gateway für eine statische IPv4-Route hinzufügen“
- Abschnitt 12.12.6.4, „Ein Gateway für eine statische IPv4-Route löschen“

Abschnitt 12.12.6.1

Gateways für statische IPv6-Routen konfigurieren

Um eine Gateway-Adresse für eine statische Ipv6-Route zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu***routing » ipv6 » route » {subnet} » via***, wobei *subnet* das Subnetz (Netzwerk/Präfix) der statischen Route ist.
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
gw { gw }	**Zusammenfassung:** Eine Zeichenkette mit 6 bis 40 Zeichen Das Gateway für die statische Route.

Parameter	Beschreibung
	Dieser Parameter ist obligatorisch.
distance { distance }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 1 und 255 Der Abstand für die statische Route.

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.12.6.2
Eine Liste der Gateways für statische IPv4-Routen anzeigen

Um eine Liste der Gateway-Adressen, die einer statischen IPv4-Route zugewiesen sind, anzuzeigen, geben Sie Folgendes ein:

```
show running-config routing ipv4 route subnet via
```

Erläuterung:

- *`subnet`* ist das Subnetz (Netzwerk/Präfix) der statischen Route

Falls Gateway-Adressen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config routing ipv4 route 0.0.0.0/0 via
routing ipv4 route 0.0.0.0/0
 via 172.30.128.1
  no distance
 !
!
```

Falls keine Gateway-Adressen konfiguriert wurden, fügen Sie je nach Bedarf Adressen hinzu. Weitere Informationen finden Sie unter Abschnitt 12.12.6.3, „Ein Gateway für eine statische IPv4-Route hinzufügen“.

Abschnitt 12.12.6.3
Ein Gateway für eine statische IPv4-Route hinzufügen

Um ein Gateway für eine statische IPv4-Route hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie die Gateway-Adresse hinzu, indem Sie Folgendes eingeben:

   ```
   routing ipv4 route subnet via gateway
   ```

   Erläuterung:

   - *`subnet`* ist das Subnetz (Netzwerk/Präfix) der statischen Route
   - *`gateway`* ist die Gateway-Adresse für die statische Route
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
distance { distance }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 1 und 255 Der Abstand für die statische Route.

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.12.6.4
Ein Gateway für eine statische IPv4-Route löschen

Um ein Gateway für eine statische IPv4-Route zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die Gateway-Adresse, indem Sie Folgendes eingeben:

   ```
   no routing ipv4 route subnet via gateway
   ```

   Erläuterung:

   - *`subnet`* ist das Subnetz (Netzwerk/Präfix) der statischen Route
   - *`gateway`* ist die Gateway-Adresse für die statische Route
3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.12.7
Schnittstellen für statische Routen verwalten

Statische Routen können für die Weiterleitung von Paketen an eine ausgehende Schnittstelle konfiguriert werden. Wenn das Gerät direkt mit einem benachbarten Router verbunden ist, sendet es ARP-(Address Resolution Protocol)-Anforderungen zur Feststellung der Next-Hop-IP-Adresse.

Bei statischen IPv6-Routen kann pro Route nur eine Schnittstelle ausgewählt werden.

INHALT

- Abschnitt 12.12.7.1, „Schnittstellen für statische Ipv6-Routen konfigurieren“
- Abschnitt 12.12.7.2, „Eine Liste der Schnittstellen für statische IPv4-Routen anzeigen“
- Abschnitt 12.12.7.3, „Eine Schnittstelle für eine statische IPv4-Route hinzufügen“
- Abschnitt 12.12.7.4, „Eine Schnittstelle für eine statische IPv4-Route löschen“

Abschnitt 12.12.7.1
Schnittstellen für statische Ipv6-Routen konfigurieren

Um eine Schnittstelle für eine statische Ipv6-Route zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu***routing » ipv6 » route » {subnet} » dev***, wobei *subnet* das Subnetz (Netzwerk/Präfix) der statischen Route ist.
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
interface { interface }	**Zusammenfassung:** Eine Zeichenkette

Parameter	Beschreibung
	Die Schnittstelle für die statische Route. Dieser Parameter ist obligatorisch.
distance { distance }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 1 und 255 Der Abstand für die statische Route.

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.12.7.2
Eine Liste der Schnittstellen für statische IPv4-Routen anzeigen

Um eine Liste der Schnittstellen, die einer statischen IPv4-Route zugewiesen sind, anzuzeigen, geben Sie Folgendes ein:

```
show running-config routing ipv4 route subnet dev
```

Erläuterung:

- *`subnet`* ist das Subnetz (Netzwerk/Präfix) der statischen Route

Falls Schnittstellen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config routing ipv4 route 0.0.0.0/0 dev
routing ipv4 route 0.0.0.0/0
 dev switch.0001
  no distance
 !
!
```

Falls keine Schnittstellen konfiguriert wurden, fügen Sie je nach Bedarf Schnittstellen hinzu. Weitere Informationen finden Sie unter Abschnitt 12.12.7.3, „Eine Schnittstelle für eine statische IPv4-Route hinzufügen“.

Abschnitt 12.12.7.3
Eine Schnittstelle für eine statische IPv4-Route hinzufügen

Um eine Schnittstelle für eine statische IPv4-Route hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie die Gateway-Adresse hinzu, indem Sie Folgendes eingeben:

   ```
   routing ipv4 route subnet dev interface
   ```

   Erläuterung:

   - *`subnet`* ist das Subnetz (Netzwerk/Präfix) der statischen Route
   - *`interface`* ist die Bezeichnung der Schnittstelle für die statische Route
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
distance { distance }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 1 und 255 Der Abstand für die statische Route.

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.12.7.4
Eine Schnittstelle für eine statische IPv4-Route löschen

Um eine Schnittstelle für eine statische IPv4-Route zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die Gateway-Adresse, indem Sie Folgendes eingeben:

   ```
   no routing ipv4 route subnet dev interface
   ```

   Erläuterung:

   - *`subnet`* ist das Subnetz (Netzwerk/Präfix) der statischen Route
   - *`interface`* ist die Bezeichnung der Schnittstelle für die statische Route
3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.13
Statisches Multicast-Routing verwalten

Mit dem statischen Multicast-Routing können Netzwerkdesigner den Multicast-Verkehrsfluss steuern, indem manuell statische Routen in der Routing-Tabelle hinzugefügt werden.

INHALT

- Abschnitt 12.13.1, „Statisches Multicast-Routing aktivieren/deaktivieren“
- Abschnitt 12.13.2, „Statische Multicast-Gruppen verwalten“
- Abschnitt 12.13.3, „Out-Schnittstellen verwalten“

Abschnitt 12.13.1
Statisches Multicast-Routing aktivieren/deaktivieren

Um das statische Multicast-Routing zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Aktivieren Sie das statische Multicast-Routing durch Eingabe von:

   ```
   routing multicast static enable
   ```

   Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
enabled	Aktiviert den statischen Multicast-Routing-Dienst

Parameter	Beschreibung
	HINWEIS *Dynamisches und statisches Multicast-Routing kann nicht gemeinsam aktiviert werden.*

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.13.2
Statische Multicast-Gruppen verwalten

Legen Sie eine statische Multicast-Gruppe für jede Multicast-Route fest. Es können mehrere Routen konfiguriert werden, solange die Quell- und Multicast-IP-Adressen in der Route einmalig sind.

WICHTIG!
Die Quell-IP-Adresse für statische Routen ist immer eine Unicast-Adresse (z. B. 192.168.0.10), während die Ziel-IP-Adresse immer eine Multicast-Adresse ist (z. B. 225.2.100.1).

INHALT

- Abschnitt 12.13.2.1, „Eine Liste statischer Multicast-Gruppen anzeigen“
- Abschnitt 12.13.2.2, „Hinzufügen einer statischen Multicast-Gruppe“
- Abschnitt 12.13.2.3, „Eine statische Multicast-Gruppe löschen“

Abschnitt 12.13.2.1
Eine Liste statischer Multicast-Gruppen anzeigen

Um eine Liste der statischen Multicast-Gruppen anzusehen, geben Sie Folgendes ein:

```
show running-config routing multicast static
```

Falls statische Multicast-Gruppen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config routing multicast static | tab
routing multicast static enabled
routing multicast static mcast-groups
                          MULTICAST    IN           HW
DESCRIPTION  SOURCE IP    IP           INTERFACE    ACCELERATE  IFNAME
-------------------------------------------------------------------------
test.001     169.150.24.12  238.1.12.12  switch.0001  -          fe-cm-1
```

Falls keine statischen Multicast-Gruppen konfiguriert wurden, fügen Sie je nach Bedarf Gruppen hinzu. Weitere Informationen über das Hinzufügen statischer Multicast-Gruppen finden Sie unter Abschnitt 12.13.2.2, „Hinzufügen einer statischen Multicast-Gruppe“.

Abschnitt 12.13.2.2

Hinzufügen einer statischen Multicast-Gruppe

Um eine statische Multicast-Gruppe hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie die Multicast-Gruppe hinzu, indem Sie Folgendes eingeben:

```
routing multicast static mcast-groups description
```

Erläuterung:

- *description* ist die Bezeichnung der Multicast-Gruppe. Maximal 32 Zeichen sind zulässig, mit Ausnahme von Leerzeichen.

3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
source-ip { source-ip }	**Zusammenfassung:** Eine Zeichenkette mit 7 bis 15 Zeichen oder eine Zeichenkette mit 6 bis 40 Zeichen Die erwartete IP-Quelladresse des Multicast-Pakets, im Format xxx.xxx.xxx.xxx. Diese Adresse wird einzeln mit der Multicast-Adresse gepaart. Mit dieser IP-Adresse können Sie keinen anderen Multicast-Routing-Eintrag mit einer unterschiedlichen Multicast-IP-Adresse erstellen. Dieser Parameter ist obligatorisch.
multicast-ip { multicast-ip }	**Zusammenfassung:** Eine Zeichenkette mit 7 bis 15 Zeichen oder eine Zeichenkette mit 7 bis 39 Zeichen Die weiterzuleitende Multicast-IP-Adresse, im Format xxx.xxx.xxx.xxx Die Adresse muss im Bereich zwischen 224.0.0.0 und 239.255.255.255 liegen. Diese Adresse wird einzeln mit der IP-Quelladresse gepaart. Mit dieser IP-Adresse können Sie keinen anderen Multicast-Routing-Eintrag mit einer unterschiedlichen IP-Quelladresse erstellen. Dieser Parameter ist obligatorisch.
in-interface { in-interface }	**Zusammenfassung:** Eine Zeichenkette Die Schnittstelle, an der das Multicast-Paket ankommt. Dieser Parameter ist obligatorisch.
hw-accelerate	Wenn die statische Multicast-Route hardwarebeschleunigt werden kann, ist die Option verfügbar. Damit eine Multicast-Route hardwarebeschleunigt werden kann, müssen die eingehenden und ausgehenden Schnittstellen umgeschaltet werden.

4. Konfigurieren Sie OUT-Interfaces. Siehe Abschnitt 12.13.3.2, „Ein OUT-Interface hinzufügen“.
5. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.13.2.3

Eine statische Multicast-Gruppe löschen

Um eine statische Multicast-Gruppe zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die Multicast-Gruppe, indem Sie Folgendes eingeben:

```
no routing multicast static mcast-groups description
```

Erläuterung:

- *description* ist die Bezeichnung der Multicast-Gruppe, die gelöscht werden soll

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.13.3

Out-Schnittstellen verwalten

Eine Out-Schnittstelle ist die Schnittstelle, an die Multicast-Pakete weitergeleitet werden. Für jede statische Multicast-Gruppe können mehrere Out-Schnittstellen festgelegt werden.

INHALT

- Abschnitt 12.13.3.1, „Eine Liste der Out-Schnittstellen anzeigen“
- Abschnitt 12.13.3.2, „Ein OUT-Interface hinzufügen“
- Abschnitt 12.13.3.3, „Ein Out-Interface löschen“

Abschnitt 12.13.3.1

Eine Liste der Out-Schnittstellen anzeigen

Um eine Liste der Out-Schnittstellen anzusehen, geben Sie Folgendes ein:

```
show runing-config routing multicast static mcast-group out-interface
```

Falls Out-Schnittstellen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config routing multicast static mcast-groups out-interface
routing multicast static mcast-groups test
 out-interface fe-cm-1
 !
!
```

Falls keine Out-Schnittstellen konfiguriert wurden, fügen Sie je nach Bedarf Schnittstellen hinzu. Weitere Informationen über das Hinzufügen von Out-Schnittstellen finden Sie unter Abschnitt 12.13.3.2, „Ein OUT-Interface hinzufügen“.

Abschnitt 12.13.3.2

Ein OUT-Interface hinzufügen

Um ein OUT-Interface hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie das OUT-Interface hinzu, indem Sie Folgendes eingeben:

   ```
   routing multicast static mcast-groups group out-interface ifname
   ```

   Erläuterung:

   - *group* ist die Bezeichnung der Multicast-Gruppe

- *ifname* ist eine Zeichenkette mit bis zu 15 Zeichen zur Benennung des OUT-Interface

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.13.3.3
Ein Out-Interface löschen

Um ein Out-Interface zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie das Out-Interface, indem Sie Folgendes eingeben:

```
no routing multicast static mcast-groups group out-interface ifname
```

Erläuterung:

- *group* ist die Bezeichnung der Gruppe mit dem Out-Interface, das gelöscht werden soll
- *ifname* ist die Bezeichnung des Out-Interface, das gelöscht werden soll

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.14
Verwalten des dynamischen Multicast-Routing

Die PIM-SM-Funktion wird für das dynamische Multicast-Routing verwendet. PIM-SM steht für "Protocol Independent Multicast - Sparse Mode". Hierbei handelt es sich um ein Multicast-Routing-Protokoll, das Multicast-Routen dynamisch bereinigen und beibehalten kann. PIM stützt sich auf die Unicast-Routing-Tabelle des Routers hinsichtlich seiner Fähigkeiten und stützt sich nicht auf ein bestimmtes Verfahren zum Lernen von Routen und ist daher "Protokoll-unabhängig".

Folgende Begriffe werden in PIM-SM verwendet:

- **Rendezvous-Punkt**
  Der Rendezvous-Punkt (RP) ist ein Ziel im Netzwerk (einer der Router), wo der gesamte Multicast-Verkehr zuerst registriert wird. Immer wenn ein PIM-Router einen Multicast-Datenstrom empfängt, werden Quelle und Multicast-Adresse zusammen mit dem Rendezvous-Punkt erfasst.
- **Boot-Strap-Router**
  Bei einem PIM-SM Boot-Strap-Router (BSR) handelt es sich um einen Router, der den Standort des Rendezvous-Punkts an alle anderen PIM-Router im Netzwerk weitergibt.
- **Designated-Router**
  Ein Designated-Router (DR) ist ein Router, der einem Multicast-Host oder -Gerät direkt zugeordnet ist. Der Router mit der höchsten IP-Adresse wird normalerweise der Designated-Router.
- **Shared Tree**
  Der Shared Tree (bzw. RP-Tree) ist ein Baum für die Verkehrsverteilung, der am Rendezvous-Punkt beginnt. Der Rendezvous-Punkt leitet den entsprechenden Multicast-Gruppen-Verkehr über diesen Baum weiter, wenn es Subscriber für einen vorhandenen Multicast-Fluss gibt. Beachten Sie, dass der gemeinsame Baum gruppenabhängig ist. Das bedeutet, dass der gemeinsame Baum für eine Gruppe von dem gemeinsamen Baum für eine andere Gruppe im selben Netzwerk abweichen kann, was von der Verteilung der Multicast-Traffic-Subscriber abhängt.

- **Shortest Path Tree**
  Bei dem Shortest Path Tree (SPT) handelt es sich um einen Baum zur Verteilung von Datenverkehr, der an der Quelle des Multicast-Verkehrs oder am Router, der der Quelle am nächsten ist, beginnt. Der Shortest Path Tree wird immer dann aktiviert, wenn ein kürzerer Pfad zwischen der Quelle und dem Empfänger existiert. Der Shortest Path Tree kann nur vom Rendezvous-Punkt oder vom mit dem Subscriber direkt verbundenen Router ausgelöst werden.
- **Internet Group Management-Protokoll**
  Das Internet Group Management-Protokoll (IGMP) wird von Hosts und Routern verwendet, um Multicast-Gruppen beizutreten und diese zu verlassen. Router senden regelmäßig IGMP-Anfragen, in denen sie fragen, ob Hosts an IP-Multicast-Verkehr interessiert sind. Wenn ein zugeordneter Host am Empfangen von Verkehr für eine bestimmte Gruppe interessiert ist, sendet er eine IGMP-Report-Nachricht, in der er sein Interesse ausdrückt. Der Router a) propagiert diese Beitrittsnachricht an einen anderen Router und b) sendet den relevanten Verkehr an das Segment, dem der Host zugeordnet ist.

INHALT

- Abschnitt 12.14.1, „PIM-SM-Grundlagen“
- Abschnitt 12.14.2, „Anzeigen des Status von PIM-SM“
- Abschnitt 12.14.3, „Status des dynamischen Multicast-Routings anzeigen“
- Abschnitt 12.14.4, „PIM-SM konfigurieren“
- Abschnitt 12.14.5, „Das Gerät als BSR-Kandidat einstellen“
- Abschnitt 12.14.6, „Das Gerät als RP-Kandidat einstellen“
- Abschnitt 12.14.7, „PIM-SM-Schnittstellen verwalten“
- Abschnitt 12.14.8, „Statische RP-Adressen verwalten“
- Abschnitt 12.14.9, „Multicast-Gruppen-Präfixe verwalten“

Abschnitt 12.14.1

PIM-SM-Grundlagen

Wenn ein PIM-Router eine Subskription von einem Host, z. B. Host A, für bestimmten Multicast-Verkehr empfängt, dann sendet der direkt verbundene Designated-Router (DR) eine PIM-Join-Nachricht für diese Multicast-Gruppe in Richtung Rendezvous-Punkt (RP). Die Nachricht wird Hop für Hop gesendet und Router, die die Nachricht erhalten, würden die Gruppe registrieren und die Nachricht weiter an den RP senden. Dadurch wird ein gemeinsamer Baum (RP-Baum) erstellt. Der Baum ist erst vollständig, wenn alle Quellen erscheinen.

Wenn ein Host oder ein Gerät Multicast-Verkehr an die von A abonnierte Multicast-Gruppe sendet, nimmt der direkt verbundene Designated-Router den Verkehr, kapselt ihn mit PIM-Register-Headern und sendet ihn als Unicast an den RP. Wenn der RP diesen Verkehr empfängt, entkapselt er die Pakete und sendet die Daten über den RP-Baum in Richtung Subscriber. Die Router, die diese Pakete empfangen, leiten diese einfach über den RP-Baum weiter, bis der Subscriber erreicht wird. Beachten Sie, dass es weitere Subscriber im Netzwerk geben kann und dass der Pfad zu diesen Subscribern vom RP auch Teil des RP-Baums ist.

Nachdem der gemeinsame Baum erstellt wurde, fließt der Verkehr von der Quelle zum RP zum Empfänger. In diesem Prozess gibt es zwei Ineffizienzen. Erstens: Der Verkehr wird an der Quelle gekapselt und am RP entkapselt, was bei hohem Verkehrsaufkommen eine Leistungseinbuße sein kann. Zweitens: Der Verkehr nimmt möglicherweise einen längeren Pfad, als es für das Erreichen seiner Empfänger notwendig ist.

Nachdem der gemeinsame Baum erstellt wurde, kann der RP eine Join-Nachricht an die Quelle senden, in der er angibt, dass er nur Verkehr für eine Gruppe (z. B. Gruppe B) von der Quelle (z. B. Quelle S) haben möchte. Der DR für die Quelle beginnt anschließend mit dem Senden des Verkehrs in Multicast-Form (statt Unicast).

Ohne Kapselung gibt es einen geringen Leistungsmehraufwand mit Ausnahme von dem, was für den Verkehr beim Routing im Allgemeinen normal ist. Der RP sendet weiterhin Verkehr über den RP-Baum, nachdem er ihn empfangen hat. Das bedeutet auch, dass der Verkehr den RP-Baum erreichen kann, bevor er den RP erreicht (wenn die Quelle vom RP-Baum abzweigt). Das hat den zusätzlichen Vorteil, dass der Verkehr effizienter in Richtung Empfänger fließt, die sich auf derselben Seite des RP-Baums wie die Quelle befinden.

Wenn der DR des Empfängers entscheidet, dass der vom RP-Baum kommende Verkehr einen suboptimalen Pfad genommen hat, als wenn er von der Quelle empfangen worden wäre, gibt er eine quellenspezifische Join-Nachricht in Richtung Quelle aus. Das hätte zur Folge, dass alle Zwischenrouter die Join-Nachricht registrieren und der Verkehr anschließend entlang dieses Baums fließen würde. Hierbei handelt es sich um den Shortest Path Tree (SP-Baum). An diesem Punkt würde der Empfänger den Verkehr sowohl vom RP- als auch vom SP-Baum empfangen. Nachdem der Fluss vom SP-Baum gestartet ist, verwirft der DR die Pakete vom RP-Baum und sendet eine Prune-Nachricht für diesen Verkehr in Richtung des RP. Dadurch kann der Verkehr vom RP nicht ankommen. Dieses Szenario tritt höchstwahrscheinlich nur dann auf, wenn der Verkehr eine Umleitung nehmen muss, wenn er vom RP ankommt. Andernfalls wird der RP-Baum verwendet.

Abschnitt 12.14.2

Anzeigen des Status von PIM-SM

Um den Status von PIM-SM anzuzeigen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Geben Sie in der Eingabeaufforderung Folgendes ein **`show routing status pim-sm`** und drücken Sie auf **Enter**. Die Informationen zum PIM-SM-Routing-Status werden angezeigt:

HINWEIS
*Ein Standard-Routing-Protokoll mit der lokalen Adresse **169.254.0.1** wird immer angezeigt, wenn der Befehl **`show routing status pim-sm`** ausgeführt wird. Dieses interne Routing-Protokoll ist ein Platzhalter für den quellenspezifischen Multicast-Adressbereich.*

```
ruggedcom# show routing status pim-sm
routing status pim-sm
bsr 1.1.1.1
vinterface
       LOCAL
INDEX  ADDRESS       SUBNET           FLAGS      ID
-----------------------------------------------------------------
0      192.168.0.12  192.168.0.0/24   DISABLED
1      169.254.72.4  169.254.72.0/28  DISABLED
2      1.1.1.1       1.1.1.1/32       DR NO-NBR
3      169.254.0.1   169.254.0.0/24   DISABLED
4      192.168.11.1  192.168.11.0/24  DR NO-NBR
5      192.168.12.1  192.168.12.0/24  PIM
                                                 192.168.12.2
6      192.168.14.1  192.168.14.0/24  PIM
                                                 192.168.14.4

rp
ID       PREFIX         PRIORITY  HOLDTIME
-------------------------------------------
3.3.3.3
         225.0.0.1/32   1         105
         225.0.0.2/32   1         105
```

Parameter	Beschreibung
local-address	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 16 Zeichen

Parameter	Beschreibung
	Lokale Adresse.
subnet	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 20 Zeichen Subnetz.
flags	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 128 Zeichen Gibt Informationen zur virtuellen Schnittstelle an. • DISABLED: Die virtuelle Schnittstelle ist für PIM-SM verwaltungstechnisch deaktiviert. • DOWN: Diese virtuelle Schnittstelle ist nicht verfügbar. • DR: Designated-Router. • NO-NBR: Kein Nachbar an dieser virtuellen Schnittstelle. • PIM: PIM-Nachbar. • DVMRP: DVMRP-Nachbar.

Abschnitt 12.14.3
Status des dynamischen Multicast-Routings anzeigen

Um den Status des dynamischen Multicast-Routings anzusehen, geben Sie Folgendes ein:

```
show routing status multicast
```

Falls Multicast-Routen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show routing status multicast
                            IN           OUT
SOURCE          GROUP       INTERFACE    INTERFACE
-------------------------------------------------------
192.168.11.101  225.0.0.1   switch.0011  switch.0012 switch.0014
```

Abschnitt 12.14.4
PIM-SM konfigurieren

PIM-SM kann dazu verwendet werden, eine Multicast-Routing-Tabelle zu erstellen und dynamisch zu verwalten.

Um PIM-SM zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***routing » multicast » dynamic » pim-sm***.
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
enabled	PIM-SM-Dienst aktivieren.
default-preference { default-preference }	**Zusammenfassung:** Eine vorzeichenlose 16-Bit-Ganzzahl von 1 oder höher **Standard:** 1024 Wert der Standardeinstellungen. Einstellungen werden von "assert elections" verwendet, um vorgeschaltete Router zu bestimmen.
default-metric { default-metric }	**Zusammenfassung:** Eine vorzeichenlose 16-Bit-Ganzzahl von 1 oder höher **Standard:** 1024

Parameter	Beschreibung
	Metrischer Standardwert. Metrik sind die Kosten für das Senden von Daten durch die Schnittstelle.
broken-cisco-checksum	Wenn Ihr RP ein Cisco ist und viele PIM_REGISTER-Prüfsummenfehler von diesem Router zeigt, ist es nützlich, die Option zu wählen.

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.14.5
Das Gerät als BSR-Kandidat einstellen

Um das Gerät als BSR-Kandidat einzustellen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Stellen Sie das Gerät als BSR-Kandidat ein, indem Sie Folgendes eingeben:

```
routing multicast dynamic pim-sm bsr-candidate local-address address priority number
```

   Erläuterung:

   - *`address`* ist die lokale Adresse, die in den Cand-BSR-Nachrichten zu verwenden ist. Falls sie nicht festgelegt ist, wird die größte lokale IP-Adresse verwendet (passive Schnittstellen ausgenommen).
   - *`priority`* legt die Priorität für das BSR fest. Höhere Werte haben höhere Priorität.
3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.14.6
Das Gerät als RP-Kandidat einstellen

Um das Gerät als RP-Kandidat einzustellen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Stellen Sie das Gerät als RP-Kandidat ein, indem Sie Folgendes eingeben:

```
routing multicast dynamic pim-sm rp-candidate local-address address timer timer priority number
```

   Erläuterung:

   - *`address`* ist die lokale Adresse, die in den Cand-RP-Nachrichten zu verwenden ist. Falls sie nicht festgelegt ist, wird die größte lokale IP-Adresse verwendet (passive Schnittstellen ausgenommen).
   - *`timer`* ist die Anzahl an Sekunden, die zwischen der Ankündigung und der Cand-RP-Nachricht zu warten ist.
   - *`priority`* legt die Priorität für dieses CRP fest. Niedrigere Werte haben höhere Priorität.
3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.14.7

PIM-SM-Schnittstellen verwalten

PIM-SM erfordert mindestens eine Schnittstelle, an der Mitteilungen empfangen oder gesendet werden. Die Schnittstelle darf nicht passiv sein und muss eine IP-Adresse besitzen.

INHALT

- Abschnitt 12.14.7.1, „Eine Liste der PIM-SM-Schnittstellen anzeigen“
- Abschnitt 12.14.7.2, „Aktivieren/Deaktivieren einer PIM-SM-Schnittstelle“

Abschnitt 12.14.7.1

Eine Liste der PIM-SM-Schnittstellen anzeigen

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***routing » multicast » dynamic » pim-sm*** und drücken Sie auf **Enter**.
3. Wenn die Eingabeaufforderung erscheint, geben Sie Folgendes ein: **`show full-configuration`** und drücken auf **Enter**. Die PIM-SM-Schnittstellendaten werden angezeigt:

```
ruggedcom(config-pim-sm)# show full-configuration | tab
routing multicast dynamic pim-sm
 enabled
 bsr-candidate local-address 1.1.1.1
 bsr-candidate priority 1
 rp-candidate local-address 1.1.1.1
 rp-candidate priority 1
 no broken-cisco-checksum
 interface
IFNAME       PASSIVE
----------------------
dummy0       false
fe-1-1       false
fe-1-16      false
fe-cm-1      true
ge-sm-1      false
switch.0001  true

 group-prefix
PREFIX
--------------
225.0.0.1/32
225.0.0.2/32

!
```

Falls keine PIM-SM-Schnittstellen konfiguriert wurden, fügen Sie je nach Bedarf Schnittstellen hinzu. Weitere Informationen über die Aktivierung von PIM-SM-Schnittstellen finden Sie unter Abschnitt 12.14.7.2, „Aktivieren/Deaktivieren einer PIM-SM-Schnittstelle“.

Abschnitt 12.14.7.2

Aktivieren/Deaktivieren einer PIM-SM-Schnittstelle

Um eine PIM-SM-Schnittstelle zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

HINWEIS
Durch das Aktivieren von PIM-SM an einer Schnittstelle wird auch IGMPv2 an der Schnittstelle aktiviert, wobei die Schnittstelle mit der niedrigsten IP-Adresse der IGMP-Abfragende wird und alle 125 Sekunden periodische Abfragenachrichten sendet.

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Die Schnittstelle ist standardmäßig passiv. Aktivieren Sie diese, indem Sie Folgendes eingeben:

   ```
   no interface ifname passive
   ```

   Erläuterung:

   - *ifname* ist die Bezeichnung der Schnittstelle
   - *passive* legt fest, ob die Schnittstelle passiv (Standard) oder aktiv (nicht passiv) ist.

   HINWEIS
   Es können maximal 30 nicht-passive Schnittstellen für PIM-SM aktiv sein.
3. Wenn, nur bei VLAN-Schnittstellen, das IGMP Snooping an der Schnittstelle aktiviert ist, stellen Sie sicher, dass das IGMP-Abfrageintervall auf 125 Sekunden gesetzt ist. Weitere Informationen finden Sie unter Abschnitt 8.4.3.1, „IGMP Snooping konfigurieren“.

   Dasselbe ist für jeden Layer-2-Switch im Netzwerk erforderlich.
4. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.14.8
Statische RP-Adressen verwalten

Eine gängige Methode für die Lokalisierung von Rendezvous Points (RPs) besteht darin, sie direkt nach ihren IP-Adressen und nicht dynamisch anzusprechen. Statische IP-Adressen können verwendet werden, wenn nur wenige RPs im Netzwerk vorhanden sind und/oder die RP-Zuordnung sich nicht oft ändert. Es ist jedoch wichtig, dass alle statischen RP-Adressen in allen PIM-SM-fähigen Geräten in der Multicast-Domain gespiegelt werden.

INHALT

- Abschnitt 12.14.8.1, „Eine Liste der statischen RP-Adressen anzeigen “
- Abschnitt 12.14.8.2, „Eine statische RP-Adresse hinzufügen“
- Abschnitt 12.14.8.3, „Eine statische RP-Adresse löschen“

Abschnitt 12.14.8.1
Eine Liste der statischen RP-Adressen anzeigen

Um eine Liste der statischen RP-Adressen anzusehen, geben Sie Folgendes ein:

```
show running-config routing multicast dynamic pim-sm rp-address
```

Falls Adressen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config routing multicast dynamic pim-sm rp-address | tab
```

```
ADDRESS         GROUP        PRIORITY
-----------------------------------------
172.30.145.254  225.0.2.6/8  -
192.168.0.10    225.0.0.1/8  -

!
```

Falls keine Adressen konfiguriert wurden, fügen Sie je nach Bedarf Adressen hinzu. Weitere Informationen finden Sie unter Abschnitt 12.14.8.2, „Eine statische RP-Adresse hinzufügen“.

Abschnitt 12.14.8.2
Eine statische RP-Adresse hinzufügen

Um eine statische RP-Adresse hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie die RP-Adresse hinzu, indem Sie Folgendes eingeben:

   ```
   routing multicast dynamic pim-sm rp-address static-address group-address priority priority
   ```

   Erläuterung:

   - *static-address* ist die IP-Adresse des RP
   - *group-address* ist die Multicast-Adresse der vom RP gesteuerten Gruppe
   - *priority* ist die Priorität des RP im Auswahlverfahren
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.14.8.3
Eine statische RP-Adresse löschen

Um eine statische RP-Adresse zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die ausgewählte RP-Adresse durch Eingabe von:

   ```
   no routing multicast dynamic pim-sm rp-address static-address
   ```

   Erläuterung *static-address* ist die statische RP-(Rendezvous Point)-Adresse
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.14.9

Multicast-Gruppen-Präfixe verwalten

Wenn das Gerät an einem RP (Rendezvous Point) gemeldet ist, kann es bis zu 20 Gruppen von Multicast-Geräten bedienen. Das Gerät wird einer Multicast-Gruppe durch Festlegen des Präfixes für die Multicast-IP-Adresse der Gruppe (z. B. 225.1.2.0/24) zugeordnet.

INHALT

- Abschnitt 12.14.9.1, „Eine Liste der Multicast-Gruppen-Präfixe anzeigen“
- Abschnitt 12.14.9.2, „Ein Präfix für eine Multicast-Gruppe hinzufügen“
- Abschnitt 12.14.9.3, „Ein Präfix für eine Multicast-Gruppe löschen“

Abschnitt 12.14.9.1

Eine Liste der Multicast-Gruppen-Präfixe anzeigen

Um eine Liste der Multicast-Gruppen-Präfixe anzusehen, geben Sie Folgendes ein:

```
show running-config routing multicast dynamic pim-sm group-prefix
```

Falls Präfixe konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config routing multicast dynamic pim-sm group-prefix
routing multicast dynamic pim-sm
 group-prefix 225.1.2.0/24
 !
!
```

Falls keine Präfixe konfiguriert wurden, fügen Sie je nach Bedarf Präfixe hinzu. Weitere Informationen finden Sie unter Abschnitt 12.14.9.2, „Ein Präfix für eine Multicast-Gruppe hinzufügen“.

Abschnitt 12.14.9.2

Ein Präfix für eine Multicast-Gruppe hinzufügen

Um ein Präfix für eine Multicast-Gruppe hinzuzufügen, gehen Sie wie folgt vor:

HINWEIS
Es können maximal 20 Gruppenpräfixe für PIM-SM definiert werden.

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie das Präfix für die Multicast-Gruppe hinzu, indem Sie Folgendes eingeben:

   ```
   routing multicast dynamic pim-sm group-prefix prefix
   ```

   Erläuterung: *prefix* ist das Präfix für die Multicast-Gruppe (z. B. 225.1.2.0/24).
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 12.14.9.3

Ein Präfix für eine Multicast-Gruppe löschen

Um ein Präfix für eine Multicast-Gruppe zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie das Präfix der Multicast-Gruppe durch Eingabe von:

   ```
   no routing multicast dynamic pim-sm group-prefix prefix
   ```

   Erläuterung: *prefix* ist das ausgewählte Präfix.
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

13 Netzwerkredundanz

Dieses Kapitel beschreibt Protokolle und Funktionen, die den redundanten Betrieb von RUGGEDCOM ROX II ermöglichen und verhindern, dass das Netzwerk durch Dienstunterbrechungen einzelner Knotenpunkte lahmgelegt wird.

INHALT

- Abschnitt 13.1, „VRRP verwalten“
- Abschnitt 13.2, „Schutz vor Verbindungs-Failover verwalten“

Abschnitt 13.1

VRRP verwalten

VRRP (Virtual Router Redundancy Protocol) ist ein Gateway-Redundanz-Protokoll. Es stellt einen Gateway-Failover-Mechanismus bereit, der für Hosts und andere Geräte, die Verkehr über das Gateway senden, unsichtbar ist.

VRRP eliminiert einen einzelnen Ausfallpunkt, der statisch gerouteten Netzwerken zugeordnet ist, indem ein automatisches Failover mit alternativen Routern bereitgestellt wird. Der RUGGEDCOM ROX II VRRP-Daemon (keepalived) ist eine mit RFC 5798 [http://tools.ietf.org/html/rfc5798] Version 2 und Version 3 kompatible Implementierung von VRRP.

HINWEIS
RFC 5798 legt den Standard für VRRP Version 3 in IPv4 und IPv6 fest. Diese Version von RUGGEDCOM ROX II unterstützt nur IPv4.

INHALT

- Abschnitt 13.1.1, „VRRP-Konzepte“
- Abschnitt 13.1.2, „Status des VRRP anzeigen“
- Abschnitt 13.1.3, „VRRP aktivieren/deaktivieren“
- Abschnitt 13.1.4, „VRRP-Tracker verwalten“
- Abschnitt 13.1.5, „VRRP-Gruppen verwalten“
- Abschnitt 13.1.6, „VRRP-Instanzen verwalten“
- Abschnitt 13.1.7, „VRRP-Überwachungen verwalten“
- Abschnitt 13.1.8, „Track Scripts verwalten“
- Abschnitt 13.1.9, „Virtuelle IP-Adressen verwalten“
- Abschnitt 13.1.10, „Verbindungssynchronisation verwalten“

Abschnitt 13.1.1
VRRP-Konzepte

Dieser Abschnitt beschreibt einige wesentliche Konzepte für die Implementierung des Virtual Router Redundancy Protocol (VRRP) RUGGEDCOM ROX II.

INHALT

- Abschnitt 13.1.1.1, „Statisches Routing vs. VRRP“
- Abschnitt 13.1.1.2, „VRRP-Terminologie“
- Abschnitt 13.1.1.3, „Verbindungssynchronisation“

Abschnitt 13.1.1.1
Statisches Routing vs. VRRP

Bei vielen Netzwerkdesigns wird ein statisch konfiguriertes Standard-Gateway in den Netzwerk-Hosts eingesetzt. Ein statisches Standard-Gateway ist einfach zu konfigurieren, erfordert, wenn überhaupt, einen kleinen Mehraufwand in Bezug auf seinen Betrieb und wird von praktisch jeder IP-Implementierung unterstützt. Bei Einsatz des Protokolls Dynamic Host Configuration (DHCP) akzeptieren Hosts eine Konfiguration möglicherweise für nur ein einziges Standard-Gateway.

Dieser Ansatz schafft jedoch eine einzelne Fehlerstelle. Ein Ausfall des das Standard-Gateway versorgenden Routers oder der WAN-Verbindung des Routers führt zu einer Isolierung der Hosts, die sich auf das Standard-Gateway verlassen.

Es gibt zahlreiche Möglichkeiten, redundante Verbindungen für die Hosts bereitzustellen. Bestimmte Hosts können alternative Gateways konfigurieren, während andere Hosts intelligent genug sind, an dynamischen Routingprotokollen (z. B. Routing Information Protocol (RIP) oder Open Shortest Path First (OSPF)-Routingprotokoll) zu partizipieren. Auch wenn diese Ansätze zwar verfügbar sind, sind sie aufgrund des administrativen und operativen Mehraufwands nicht immer praktikabel.

VRRP löst dieses Problem, indem es die Bildung einer *virtuellen Router-Gruppe* zulässt, die aus mehreren Routern besteht, die eine Gateway-IP bereitstellen. VRRP wendet ein Auswahl-Protokoll für die dynamische Zuweisung der Zuständigkeit für das Gateway an einen der Router der Gruppe an. Dieser Router wird als Master bezeichnet.

Wenn der Master (oder optional eine Bedingung) ausfällt, wählt der alternative (oder Backup-) Router in der Gruppe den neuen Master. Der neue Master besitzt die virtuelle IP-Adresse und gibt ein unaufgefordertes ARP aus, um das Netzwerk zu informieren, wo das Gateway erreichbar ist.

Da sich die Standardroute und MAC-Adresse des Hosts nicht ändern, wird der Paketverlust an den Hosts auf die Zeit begrenzt, die für die Wahl eines neuen Routers erforderlich ist.

Abschnitt 13.1.1.2
VRRP-Terminologie

Jeder physische Router, auf dem VRRP ausgeführt wird, wird als VRRP-Router bezeichnet. Zwei oder mehr VRRP-Router können so konfiguriert werden, dass sie einen *virtuellen Router* bilden. Jeder VRRP-Router kann an einem oder mehreren virtuellen Routern beteiligt sein.

Jeder virtuelle Router hat eine vom Benutzer konfigurierte Kennung des virtuellen Routers (Virtual Router Identifier, VRID) und eine virtuelle IP-Adresse oder einen Satz IP-Adressen auf dem gemeinsamen LAN. Hosts auf dem gemeinsamen LAN sind so konfiguriert, dass sie diese Adressen als Standard-Gateway nutzen.

Jeder Router in der virtuellen Routergruppe hat eine spezifische Priorität, eine Zahl zwischen 1 und 255. Der Router mit der höchsten Priorität (bzw. höchsten Zahl) wird als Master festgelegt, alle anderen Router werden als Backups betrachtet.

Auf RUGGEDCOM RX1400 Geräten mit RUGGEDCOM ROX II v2.3 oder höher kann der Backup-VRRP-Router, wenn sich der Router mit der höchsten Priorität im Fehlerzustand befindet, seinen Wechsel zum Masterrouter verzögern. Die Dauer der Verzögerung ist vom Benutzer definiert.

VRRP kann auch eine angegebene Schnittstelle überwachen und die Steuerung einer Gateway-IP bei Ausfall dieser Schnittstelle einem anderen VRRP-Router überlassen.

Beispiel für VRRP

Im folgenden Beispiel verwendet Host 1 das Gateway 1.1.1.253 und Host 2 verwendet das Gateway 1.1.1.252. Das Gateway 1.1.1.253 wird von VRID 10 bereitgestellt. Bei normalem Betrieb stellt Router 1 diese virtuelle IP bereit, weil seine Priorität für VRID 10 höher ist als die von Router 2. Wenn Router 1 betriebsunfähig wird oder sein w1ppp-Link ausfällt, überlässt er die Steuerung von Gateway IP 1.1.1.253 dem Router 2.

Auf ähnliche Weise kann Host 2 die Gateway-Adresse 1.1.1.252 von VRID 11 verwenden, die normalerweise von Router 2 bereitgestellt wird.

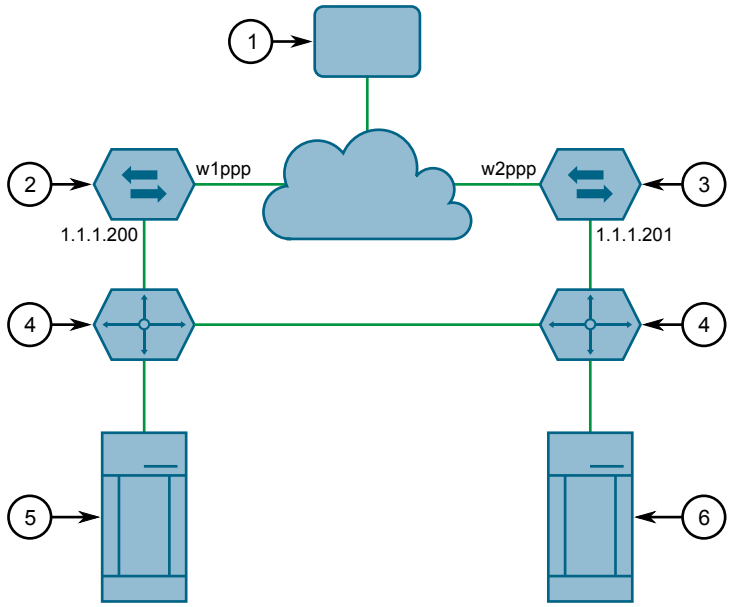


Abbildung 26: Beispiel für VRRP

1. Netzwerk **2.** Entfernter Router 1 **3.** Entfernter Router 2 **4.** Switch **5.** Host 1 **6.** Host 2

In diesem Beispiel sind die entfernten Router wie folgt konfiguriert:

Entfernter Router 1	Entfernter Router 2
• Gateway-IP von VRID10: 1.1.1.253 • Priorität von VRID 10: 100 • Überwachungsschnittstelle von VRID 10: w1ppp • Gateway-IP von VRID11: 1.1.1.252 • Priorität von VRID 11: 50	• Gateway-IP von VRID10: 1.1.1.253 • Priorität von VRID 10: 50 • Gateway-IP von VRID11: 1.1.1.252 • Priorität von VRID 11: 100 • Überwachungsschnittstelle von VRID 11: w2ppp

Datenverkehr von Host 1 wird über Router 1 gesendet, und Datenverkehr von Host 2 wird über Router 2 gesendet. Ein Ausfall einer der beiden Router oder einer der beiden WAN-Links wird von dem jeweils anderen Router abgefangen.

Beachten Sie, dass beide Router von den Hosts stets über ihre *echten* IP-Adressen erreicht werden können.

Zwei oder mehr VRRP-Instanzen können der gleichen VRRP-Gruppe zugeordnet werden, weshalb ein gemeinsames Failover möglich ist.

» Beispiel für VRRP-Gruppen

Im nächsten Beispiel verwenden sowohl Host 1 als auch Host 2 das Gateway 192.168.3.10. Die externe Seite kann über Gateway 192.168.2.10 auf die interne Seite zugreifen. VRID_20 und VRID_21 befinden sich in einer Gruppe. Normalerweise stellt Router 1 ein Gateway für internen und externen Zugriff bereit, da seine Priorität höher ist als die von Router 2. Wenn entweder die interne oder die externe Seite von Router 1 betriebsunfähig wird, übergibt Router 1 die Steuerung beider Gateways, 192.168.2.10 und 192.168.3.10, an Router 2.

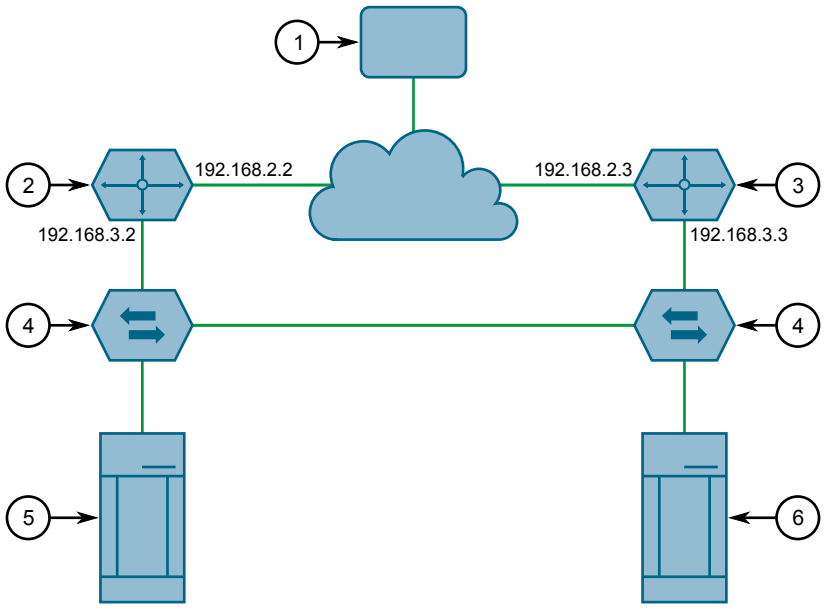


Abbildung 27: Beispiel für VRRP-Gruppen

1. Netzwerk **2.** Entfernter Router 1 **3.** Entfernter Router 2 **4.** Switch **5.** Host 1 **6.** Host 2

In diesem Beispiel sind die entfernten Router wie folgt konfiguriert:

Entfernter Router 1	Entfernter Router 2
• Gateway-IP von VRID_20: 192.168.2.10 • Priorität von VRID_20: 100 • Gateway-IP von VRID_21: 192.168.3.10 • Priorität von VRID_21: 100	• Gateway-IP von VRID_20: 192.168.2.10 • Priorität von VRID_20: 50 • Gateway-IP von VRID_21: 192.168.3.10 • Priorität von VRID_21: 50

Weitere VRRP-Parameter sind das Advertisement Interval und Gratuitous ARP Delay. Das Advertisement Interval ist das Zeitintervall, in dem Ankündigungen gesendet werden. Ein Backup-Router übernimmt die Rolle des Masters drei Ankündigungsintervalle nach Ausfall des Masters. Wenn eine überwachte Schnittstelle ausfällt, signalisiert ein Master-Router sofort eine Auswahl und gestattet es einem Backup-Router, die Master-Rolle zu übernehmen.

Der Router setzt beim Wechseln zwischen Master- und Backup-Rolle einen Satz grundloser ARPs ab. Diese nicht angeforderten ARPs unterrichten die Hosts und Switches im Netzwerk über die mit dem Gateway in Zusammenhang stehende aktuelle MAC-Adresse und den Port. Der Router setzt nach dem vom Parameter Gratuitous ARP Delay angegebenen Zeitraum einen zweiten Satz ARPs ab.

Abschnitt 13.1.1.3
Verbindungssynchronisation

Bei einem Failover müssen die Hosts meist manuell wieder mit der Backup-Firewall verbunden werden oder warten, bis die Verbindung automatisch wiederhergestellt wird. Dies kann manchmal mehrere Minuten dauern.

Ist die Verbindungssynchronisation aktiviert, werden zustandsbezogene Verbindungen beim Ausfall eines VRRP-Master-Routers aufrechterhalten, so dass ein nahtloser Failover zum VRRP-Backup-Router gewährleistet ist. Dies erfolgt durch die Synchronisation der Firewall und NAT-Zustände zwischen den Master- und Backup-Routern.

Im folgenden Beispiel werden bei einem Ausfall des Master-Routers (R1) die Firewall-Verbindung und die NAT-Zustände automatisch für den Backup-Router (R2) initialisiert. Der Backup-Router wird dann zum neuen VRRP-Master.

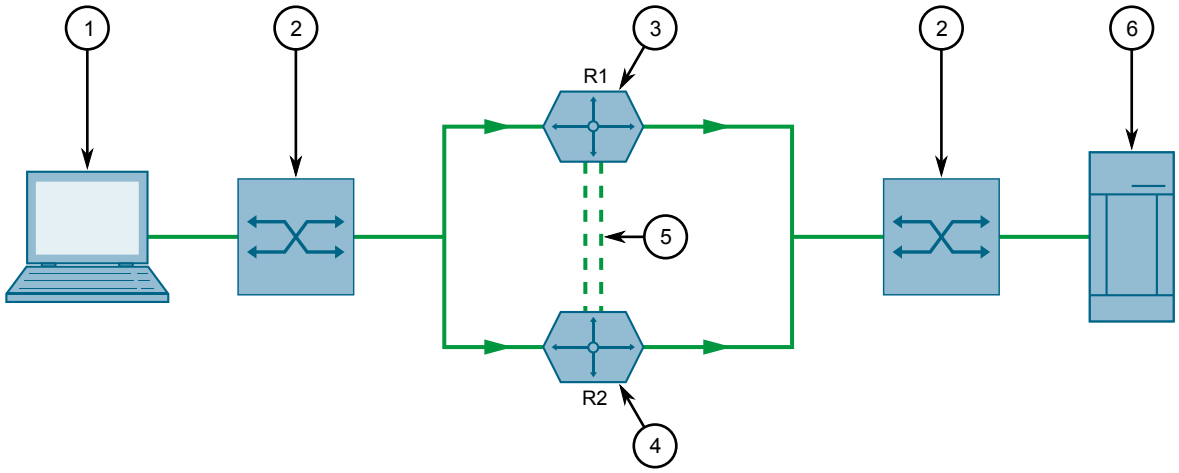


Abbildung 28: Beispiel einer Verbindungssynchronisation

1. Host A **2.** Switch **3.** Primäre(r) VRRP-Firewall und -Router (R1) **4.** Backup-VRRP-Firewall und -Router (R2) **5.** Fest zugeordnete Links **6.** Host B

Abschnitt 13.1.2
Status des VRRP anzeigen

Um den Status des VRRP anzusehen, geben Sie Folgendes ein:

```
show services vrrp status
```

Eine Tabelle oder Liste ähnlich dem folgenden Beispiel wird angezeigt:

```
ruggedcom# show services vrrp status
                                                                MONITOR
                                                  INTERFACE     INTERFACE
```

```
NAME  STATE   PRIORITY  TIME CHANGE                   STATE          STATE
-------------------------------------------------------------------------------
v1    master  100       Sat Feb  2 06:30:41 EST 2013  fe-cm-1 is Up
```

Diese Tabelle oder Liste liefert die folgenden Informationen:

Parameter	Beschreibung
name	**Zusammenfassung:** Eine Zeichenkette Der Name der VRRP-Instanz.
state	**Zusammenfassung:** Eine Zeichenkette Der Status der VRRP-Instanz. Dieser Parameter ist obligatorisch.
priority	**Zusammenfassung:** Eine Zeichenkette Die Priorität der VRRP-Instanz. Dieser Parameter ist obligatorisch.
time-change	**Zusammenfassung:** Eine Zeichenkette Die Zeit, in der in den aktuellen Zustand gewechselt wird. Dieser Parameter ist obligatorisch.
interface-state	**Zusammenfassung:** Eine Zeichenkette Der Status der VRRP-Schnittstelle. Dieser Parameter ist obligatorisch.

Abschnitt 13.1.3
VRRP aktivieren/deaktivieren

Um VRRP zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Aktivieren oder deaktivieren Sie VRRP durch Eingabe von:

   VRRP aktivieren

   ```
   services vrrp enabled
   ```

   VRRP deaktivieren

   ```
   no services vrrp enabled
   ```

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 13.1.4
VRRP-Tracker verwalten

VRRP-Tracker überwachen den Zustand einer Route. Ist die Route nicht verfügbar, verringert VRRP ihre Priorität oder setzt sie in einen Fehlerzustand.

HINWEIS
Die Entscheidung über die Verringerung oder Erhöhung der Priorität einer Route muss in Abstimmung mit VRRP-Backup-Routern erfolgen, da die Priorität darüber entscheidet, ob ein Router zu einem Master oder einem Backup wird. Hat beispielsweise Router X eine Priorität von 150 und Router X eine Priorität von 145, muss die Priorität von Router X um 6 verringert werden, damit er zum Backup-Router wird.

INHALT

- Abschnitt 13.1.4.1, „Eine Liste der VRRP-Tracker anzeigen“
- Abschnitt 13.1.4.2, „Einen VRRP-Tracker hinzufügen“
- Abschnitt 13.1.4.3, „Einen VRRP-Tracker löschen“

Abschnitt 13.1.4.1
Eine Liste der VRRP-Tracker anzeigen

Um eine Liste der VRRP-Tracker anzusehen, geben Sie Folgendes ein:

```
show running-config services vrrp trackers
```

Falls Tracker konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config services vrrp trackers
services
 vrrp
  trackers tracker tracker1
   network   10.0.0.0/8
   interface dummy0
   interval  1
  !
 !
!
```

Falls keine VRRP-Tracker konfiguriert wurden, fügen Sie je nach Bedarf Tracker hinzu. Weitere Informationen finden Sie unter Abschnitt 13.1.4.2, „Einen VRRP-Tracker hinzufügen“.

Abschnitt 13.1.4.2
Einen VRRP-Tracker hinzufügen

Um einen VRRP-Tracker hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den Tracker hinzu, indem Sie Folgendes eingeben:

   ```
   services vrrp trackers name
   ```

   Erläuterung:

   - *name* ist die Bezeichnung des VRRP-Trackers
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
type { type }	**Zusammenfassung:** { route } **Standard:** route

Parameter	Beschreibung
	Die Art des Zustands, die der Tracker prüfen soll.
network { network }	**Zusammenfassung:** Eine Zeichenkette mit 9 bis 18 Zeichen Das zu trackende Netzwerk. Der Tracker sucht in der Routingtabelle nach einer Route zu diesem Netzwerk.
interface { interface }	**Zusammenfassung:** Eine Zeichenkette Die Schnittstelle zum getrackten Netzwerk. Der Tracker steigt nur dann, wenn die Route zum überwachten Netzwerk über diese Schnittstelle führt.
interval { interval }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 1 und 120 Die Anzahl Sekunden, die zwischen Tracker-Abfragen vergehen. Dieser Parameter ist obligatorisch.
weight { weight }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen -254 und 254 Die Anzahl, um die sich die Priorität des Router erhöht oder reduziert. Wenn negativ, verringert sich die Priorität um diese Anzahl, wenn der Tracker sinkt. Wenn positiv, erhöht sich die Priorität um diese Anzahl, wenn der Tracker steigt. Wenn nichts eingestellt ist, wechselt der Zustand in den Fehlzustand, wenn der Tracker sinkt.
rise { rise }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 1 und 65535 Die Anzahl erfolgreicher Tracker-Abfragen vor dem Wechsel der Router-Priorität.
fall { fall }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 1 und 65535 Die Anzahl nicht erfolgreicher Tracker-Abfragen vor dem Wechsel der Router-Priorität.

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 13.1.4.3
Einen VRRP-Tracker löschen

Um einen VRRP-Tracker zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den Tracker durch Eingabe von:

```
no services vrrp trackers name
```

Erläuterung:

- *`name`* ist die Bezeichnung des VRRP-Trackers

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 13.1.5

VRRP-Gruppen verwalten

Zwei oder mehr VRRP-Instanzen können einer VRRP-Gruppe zugeordnet werden und können dann auch gemeinsam ausfallen.

INHALT

- Abschnitt 13.1.5.1, „Eine Liste der VRRP-Gruppen anzeigen“
- Abschnitt 13.1.5.2, „Eine VRRP-Gruppe hinzufügen“
- Abschnitt 13.1.5.3, „Eine VRRP-Gruppe löschen“

Abschnitt 13.1.5.1

Eine Liste der VRRP-Gruppen anzeigen

Um eine Liste der VRRP-Gruppen anzusehen, geben Sie Folgendes ein:

```
show running-config services vrrp group
```

Falls Gruppen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config services vrrp group
services
 vrrp
  group group1
  !
 !
!
```

Falls keine Gruppen konfiguriert wurden, fügen Sie je nach Bedarf Gruppen hinzu. Weitere Informationen finden Sie unter Abschnitt 13.1.5.2, „Eine VRRP-Gruppe hinzufügen“.

Abschnitt 13.1.5.2

Eine VRRP-Gruppe hinzufügen

Um eine VRRP-Gruppe hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Um die Gruppe hinzuzufügen, geben Sie Folgendes ein:

   ```
   services vrrp group name
   ```

   Erläuterung:

   - *name* ist der Name der VRRP-Gruppe
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 13.1.5.3
Eine VRRP-Gruppe löschen

Um eine VRRP-Gruppe zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die Gruppe durch Eingabe von:

   ```
   no services vrrp group name
   ```

   Erläuterung:

   - *name* ist der Name der VRRP-Gruppe
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 13.1.6
VRRP-Instanzen verwalten

VRRP-Instanzen definieren die mit VRRP überwachten Schnittstellen. Zwei oder mehr Instanzen können der gleichen VRRP-Gruppe hinzugefügt werden und können dann auch gemeinsam ausfallen.

INHALT

- Abschnitt 13.1.6.1, „Eine Liste der VRRP-Instanzen anzeigen“
- Abschnitt 13.1.6.2, „Hinzufügen einer VRRP-Instanz“
- Abschnitt 13.1.6.3, „Eine VRRP-Instanz löschen“

Abschnitt 13.1.6.1
Eine Liste der VRRP-Instanzen anzeigen

Um eine Liste der VRRP-Instanzen anzusehen, geben Sie Folgendes ein:

```
show running-config services vrrp instance
```

Falls Instanzen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config services vrrp instance
services
 vrrp
  instance vid20
   interface switch.0001
   vrid      10
   priority  100
   group     group1
   monitor fe-cm-1
   !
   track-script tracker1
   !
   vrip 192.168.0.10/24
   !
  !
 !
!
```

Falls keine VRRP-Instanzen konfiguriert wurden, fügen Sie je nach Bedarf Instanzen hinzu. Weitere Informationen finden Sie unter Abschnitt 13.1.6.2, „Hinzufügen einer VRRP-Instanz“.

Abschnitt 13.1.6.2
Hinzufügen einer VRRP-Instanz

Um eine VRRP-Instanz hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Stellen Sie sicher, dass eine VRRP-Gruppe konfiguriert wurde. Weitere Informationen finden Sie unter Abschnitt 13.1.5.2, „Eine VRRP-Gruppe hinzufügen“.
3. Fügen Sie die Instanz hinzu, indem Sie Folgendes eingeben:

   ```
   services vrrp instance name
   ```

   Erläuterung:

   - *name* ist die Bezeichnung der VRRP-Instanz. Die Bezeichnung darf keine Leerzeichen enthalten.
4. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

   HINWEIS
   Eine Präemption tritt auf, wenn:
   - *ein Backup-VRRP-Router eine höhere Priorität einnimmt und in den Master-Status wechselt*
   - *VRRP initiiert wird und dieser Router eine höhere Priorität hat als ein beliebig anderer VRRP-Router im Netzwerk*

Parameter	Beschreibung
vrrp-version { vrrp-version }	**Zusammenfassung:** Eine vorzeichenlose 8-Bit-Ganzzahl zwischen 2 und 3 **Standard:** 2 VRRP-Version für diese Instanz konfigurieren.
interface { interface }	**Zusammenfassung:** Eine Zeichenkette Die Schnittstelle, die das VRIP hostet, wenn der Router zum VRRP-Master wird. Dieser Parameter ist obligatorisch.
vrid { vrid }	**Zusammenfassung:** Eine vorzeichenlose 8-Bit-Ganzzahl zwischen 1 und 255 Die ID des virtuellen Routers. Alle Router, die dasselbe VRIP bereitstellen, sollten dieselbe VRID haben. Dieser Parameter ist obligatorisch.
priority { priority }	**Zusammenfassung:** Eine vorzeichenlose 8-Bit-Ganzzahl zwischen 0 und 255 Die Priorität der VRRP-Instanz. Bei der Wahl des Masters gewinnt die höchste Priorität. Der konfigurierbare Bereich liegt zwischen 1 und 255. Ein Wert von Null (0) ist ungültig. Dieser Parameter ist obligatorisch.
advert-interval { advert-interval }	**Zusammenfassung:** Eine vorzeichenlose 8-Bit-Ganzzahl zwischen 1 und 255 **Standard:** 1 VRRP2-Ankündigungsintervall, in Sekunden.
advert-interval-millisecond { advert-interval-millisecond }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 20 und 3000 **Standard:** 1000 VRRP3-Ankündigungsintervall in Millisekunden, muss ein Vielfaches von 10 sein.

Parameter	Beschreibung
	HINWEIS *Wert von "advert-interval-millisecond" muss ein Vielfaches von 10 sein.*
garp-delay { garp-delay }	**Zusammenfassung:** Eine vorzeichenlose 8-Bit-Ganzzahl zwischen 1 und 255 **Standard:** 5 Unentgeltliche ARP-Verzögerung Legt die Verzögerung fest, nachdem der Router den Status ändert, bevor ein zweiter Satz unentgeltlicher ARPs gesendet wird.
nopreempt	Wenn aktiviert, behält ein Router mit niedrigerer Priorität seine Rolle als Master, auch wenn dieser Router eine höhere Priorität hat.
preempt-delay { preempt-delay }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 0 und 1000 **Standard:** 0 Die Zeit in Sekunden nach der Inbetriebnahme bis zum Zuvorkommen.
fault-to-master-delay { fault-to-master-delay }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 0 und 1000 **Standard:** 0 Die Verzögerung in Sekunden, bevor ein Übergang vom Fehlerzustand in den Masterzustand erfolgt und damit dem aktuellen Master zuvorgekommen wird.
use-virtual-mac	Wenn aktiviert, verwendet der Router eine virtuelle MAC-Adresse für die VRIP-Schnittstelle.
group { group }	**Zusammenfassung:** Eine Zeichenkette Bindet diese VRRP-Instanz an eine VRRP-Gruppe.

5. Fügen Sie einen oder mehrere VRRP-Monitore hinzu. Weitere Informationen finden Sie unter Abschnitt 13.1.7.2, „Eine VRRP-Überwachung hinzufügen“.
6. Fügen Sie ein oder mehrere Track-Skripte hinzu. Weitere Informationen finden Sie unter Abschnitt 13.1.8.2, „Ein Track-Skript hinzufügen“.
7. Fügen Sie eine oder mehrere virtuelle IP-Adressen hinzu. Weitere Informationen finden Sie unter Abschnitt 13.1.9.2, „Eine virtuelle IP-Adresse hinzufügen“.
8. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 13.1.6.3

Eine VRRP-Instanz löschen

Um eine VRRP-Instanz zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die Instanz durch Eingabe von:

```
no services vrrp instance name
```

Erläuterung:

- *`name`* ist die Bezeichnung der VRRP-Instanz

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 13.1.7

VRRP-Überwachungen verwalten

Eine VRRP-Überwachung wählt eine spezielle Schnittstelle für die Überwachung aus. Ist die Schnittstelle nicht erreichbar, übergibt der Router die Kontrolle über die Gateway-IP-Adresse an einen anderen VRRP-Router.

INHALT

- Abschnitt 13.1.7.1, „Eine Liste der VRRP-Überwachungen anzeigen“
- Abschnitt 13.1.7.2, „Eine VRRP-Überwachung hinzufügen“
- Abschnitt 13.1.7.3, „Eine VRRP-Überwachung löschen“

Abschnitt 13.1.7.1

Eine Liste der VRRP-Überwachungen anzeigen

Um eine Liste der VRRP-Überwachungen anzusehen, geben Sie Folgendes ein:

```
show running-config services vrrp instance name monitor
```

Erläuterung:

- *name* ist die Bezeichnung der VRRP-Instanz

Falls Überwachungen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config services vrrp instance monitor
services
 vrrp
  instance vid20
   monitor fe-cm-1
   !
  !
 !
!
```

Falls keine VRRP-Überwachungen konfiguriert wurden, fügen Sie je nach Bedarf Überwachungen hinzu. Weitere Informationen finden Sie unter Abschnitt 13.1.7.2, „Eine VRRP-Überwachung hinzufügen“.

Abschnitt 13.1.7.2

Eine VRRP-Überwachung hinzufügen

Um eine VRRP-Überwachung hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie die Instanz hinzu, indem Sie Folgendes eingeben:

   ```
   services vrrp instance name monitor interface
   ```

   Erläuterung:

   - *name* ist die Bezeichnung der VRRP-Instanz
   - *interface* die Bezeichnung der zusätzlichen Schnittstelle ist, die überwacht werden soll.
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
weight { weight }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen -254 und 254 Die Anzahl, um die sich die Priorität des Router erhöht oder reduziert. Wenn negativ, verringert sich die Priorität um diese Anzahl, wenn die Schnittstelle sinkt. Wenn positiv, erhöht sich die Priorität um diese Anzahl, wenn die Schnittstelle steigt. Wenn nichts eingestellt ist, wechselt der Zustand in den Fehlzustand, wenn die Schnittstelle sinkt.

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 13.1.7.3
Eine VRRP-Überwachung löschen

Um eine VRRP-Überwachung zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die Überwachung, indem Sie Folgendes eingeben:

```
no services vrrp instance name monitor interface
```

Erläuterung:

- *`name`* ist die Bezeichnung der VRRP-Instanz
- *`interface`* die Bezeichnung der zusätzlichen Schnittstelle ist, die überwacht werden soll.

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 13.1.8
Track Scripts verwalten

Mit Track Scripts werden VRRP-Tracker VRRP-Instanzen zugeordnet.

INHALT

- Abschnitt 13.1.8.1, „Eine Liste der Track Scripts anzeigen“
- Abschnitt 13.1.8.2, „Ein Track-Skript hinzufügen“
- Abschnitt 13.1.8.3, „Ein Track-Skript löschen“

Abschnitt 13.1.8.1
Eine Liste der Track Scripts anzeigen

Um eine Liste der Track Scripts anzusehen, geben Sie Folgendes ein:

```
show running-config services vrrp instance name monitor
```

Erläuterung:

- *`name`* ist die Bezeichnung der VRRP-Instanz

Falls Track Scripts konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config services vrrp instance track-script
services
 vrrp
  instance vid20
   track-script tracker1
   !
  !
 !
!
```

Falls keine VRRP-Überwachungen konfiguriert wurden, fügen Sie je nach Bedarf Überwachungen hinzu. Weitere Informationen finden Sie unter Abschnitt 13.1.7.2, „Eine VRRP-Überwachung hinzufügen“.

Abschnitt 13.1.8.2
Ein Track-Skript hinzufügen

Um ein Track-Skript hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie das Track-Skript hinzu, indem Sie Folgendes eingeben:

   ```
   services vrrp instance name track-script tracker
   ```

   Erläuterung:

   - *name* ist die Bezeichnung der VRRP-Instanz
   - *tracker* ist die Bezeichnung des Trackers, der zur Überwachung der VRRP-Instanz verwendet wird
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
weight { weight }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen -254 und 254 Diese Einstellung überschreibt die Gewichtseinstellung im Tracker. Wenn negativ, verringert sich die Priorität um diese Anzahl, wenn der Tracker sinkt. Wenn positiv, erhöht sich die Priorität um diese Anzahl, wenn der Tracker steigt. Wenn nichts eingestellt ist, wird der Gewichtswert im Tracker verwendet.

4. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 13.1.8.3
Ein Track-Skript löschen

Um ein Track-Skript zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie das Track-Skript, indem Sie Folgendes eingeben:

   ```
   no services vrrp instance name track-script tracker
   ```

   Erläuterung:

   - *name* ist die Bezeichnung der VRRP-Instanz
   - *tracker* ist die Bezeichnung des Trackers, der zur Überwachung der VRRP-Instanz verwendet wird

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 13.1.9
Virtuelle IP-Adressen verwalten

Virtuelle IP-Adressen stellen die Standard-Gateways dar, die von den Hosts im Shared-LAN verwendet werden.

INHALT

- Abschnitt 13.1.9.1, „Eine Liste virtueller IP-Adressen anzeigen“
- Abschnitt 13.1.9.2, „Eine virtuelle IP-Adresse hinzufügen“
- Abschnitt 13.1.9.3, „Eine virtuelle IP-Adresse löschen“

Abschnitt 13.1.9.1
Eine Liste virtueller IP-Adressen anzeigen

Um eine Liste virtueller IP-Adressen anzusehen, geben Sie Folgendes ein:

```
show running-config services vrrp instance name vrip
```

Erläuterung:

- *`name`* ist die Bezeichnung der VRRP-Instanz

Falls Adressen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config services vrrp instance vid20 vrip
services
 vrrp
  instance vid20
   vrip 192.168.0.10/24
   !
  !
 !
!
```

Falls keine virtuellen IP-Adressen konfiguriert wurden, fügen Sie je nach Bedarf Adressen hinzu. Weitere Informationen finden Sie unter Abschnitt 13.1.9.2, „Eine virtuelle IP-Adresse hinzufügen“.

Abschnitt 13.1.9.2
Eine virtuelle IP-Adresse hinzufügen

Um eine virtuelle IP-Adresse hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie die Instanz hinzu, indem Sie Folgendes eingeben:

   ```
   services vrrp instance name vrip address
   ```

   Erläuterung:

   - *`name`* ist die Bezeichnung der VRRP-Instanz

- *address* ist die Adresse und das Subnetz

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 13.1.9.3
Eine virtuelle IP-Adresse löschen

Um eine virtuelle IP-Adresse zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die virtuelle IP-Adresse, indem Sie Folgendes eingeben:

```
no services vrrp instance name vrip address
```

Erläuterung:

- *name* ist die Bezeichnung der VRRP-Instanz
- *address* ist die virtuelle IP-Adresse und Netzmaske

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 13.1.10
Verbindungssynchronisation verwalten

Dieser Abschnitt beschreibt, wie Sie die Verbindungssynchronisation zwischen zwei VRRP-fähigen Routern konfigurieren können.

INHALT

- Abschnitt 13.1.10.1, „Verbindungssynchronisation konfigurieren“
- Abschnitt 13.1.10.2, „Verbindungssynchronisation aktivieren/deaktivieren“
- Abschnitt 13.1.10.3, „Eine Liste fest zugeordneter Links anzeigen“
- Abschnitt 13.1.10.4, „Einen fest zugeordneten Link hinzufügen“
- Abschnitt 13.1.10.5, „Einen fest zugeordneten Link löschen“
- Abschnitt 13.1.10.6, „Einen fest zugeordneten Link auswählen“
- Abschnitt 13.1.10.7, „Anzeigen des Status von jedem fest zugeordneten Link“

Abschnitt 13.1.10.1
Verbindungssynchronisation konfigurieren

Um die Verbindungssynchronisation zu konfigurieren, gehen Sie für *jedes* VRROP-fähige Gerät wie folgt vor:

WICHTIG!
Gut aufgebaute, zustandsbezogene Firewall-Regeln sind erforderlich. Für weitere Informationen siehe Abschnitt 6.7.1.1, „Zustandslose vs. zustandsorientierte Firewalls“.

1. Konfigurieren Sie eine Firewall mit zustandsbezogenen Firewall-Regeln, um den ein- wie ausgehenden Verkehr zu steuern. Für weitere Informationen siehe Abschnitt 6.7.3, „Hinzufügen einer Firewall“.
2. Stellen Sie sicher, dass der VRRP-Service aktiviert ist. Für weitere Informationen siehe Abschnitt 13.1.3, „VRRP aktivieren/deaktivieren“.
3. Konfigurieren Sie VRRP-Instanzen und -Gruppen. Weitere Informationen finden Sie in Abschnitt 13.1.6.2, „Hinzufügen einer VRRP-Instanz“ und Abschnitt 13.1.5.2, „Eine VRRP-Gruppe hinzufügen“.
4. Legen Sie einen oder mehrere fest zugeordnete Links für jede VRRP-Gruppe fest. Für weitere Informationen siehe Abschnitt 13.1.10.4, „Einen fest zugeordneten Link hinzufügen“.
5. Wählen Sie einen Link als voreingestellten, fest zugeordneten Link für jede VRRP-Gruppe aus, die keinem fest zugeordneten Link zugewiesen ist. Für weitere Informationen siehe Abschnitt 13.1.10.6, „Einen fest zugeordneten Link auswählen“.
6. Aktivieren Sie den Service zur Verbindungssynchronisation. Für weitere Informationen siehe Abschnitt 13.1.10.2, „Verbindungssynchronisation aktivieren/deaktivieren“.

Sobald die Konfiguration abgeschlossen ist, prüfen Sie den Status des Services auf beiden Geräten. Für weitere Informationen siehe Abschnitt 13.1.10.7, „Anzeigen des Status von jedem fest zugeordneten Link“.

Abschnitt 13.1.10.2

Verbindungssynchronisation aktivieren/deaktivieren

Um eine Verbindungssynchronisation zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Aktivieren oder deaktivieren Sie die Verbindungssynchronisation durch Eingabe von:

   Aktivieren

   ```
   services conn-sync enabled
   ```

   Deaktivieren

   ```
   no services conn-sync enabled
   ```
3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 13.1.10.3

Eine Liste fest zugeordneter Links anzeigen

Um eine Liste der fest zugeordneten Links anzusehen, geben Sie Folgendes ein:

```
show running-config services conn-sync dedicated-link | tab
```

Falls fest zugeordnete Links konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config services conn-sync dedicated-link | tab
                                                  SEND    RECV
NAME  INTERFACE  IP         MCAST IP    GROUP  BUFFER  BUFFER
-------------------------------------------------------------
3     fe-2-3     100.0.5.1  225.0.0.51  3781   1220    1220
4     fe-2-4     100.1.5.1  225.0.0.52  3782   1220    1220

 !
```

```
!
```

Falls keine fest zugeordneten Links konfiguriert wurden, fügen Sie je nach Bedarf Links hinzu. Weitere Informationen finden Sie unter Abschnitt 13.1.10.4, „Einen fest zugeordneten Link hinzufügen“.

Abschnitt 13.1.10.4
Einen fest zugeordneten Link hinzufügen

Um einen fest zugeordneten Link hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.

   HINWEIS
   RUGGEDCOM ROX II unterstützt bis zu vier fest zugeordnete Links.

2. Fügen Sie einen fest zugeordneten Link hinzu, indem Sie Folgendes eingeben:

   ```
   services conn-sync dedicated-link name
   ```

   Erläuterung: *name* ist die Bezeichnung des fest zugeordneten Links.

3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
interface { interface }	**Zusammenfassung:** Eine Zeichenkette Der Name der Schnittstelle des zugeordneten Links.
ip { ip }	**Zusammenfassung:** Eine Zeichenkette mit 7 bis 15 Zeichen oder eine Zeichenkette mit 6 bis 40 Zeichen Die IPv4- oder IPv6-Adresse der Schnittstelle des zugeordneten Links.
mcast-ip { mcast-ip }	**Zusammenfassung:** Eine Zeichenkette mit 7 bis 15 Zeichen oder eine Zeichenkette mit 7 bis 39 Zeichen **Standard:** 225.0.0.50 Die IPv4- oder IPv6-Multicast-Zieladresse des zugeordneten Links.
group { group }	**Zusammenfassung:** Eine vorzeichenlose 16-Bit-Ganzzahl zwischen 1 und 65535 **Standard:** 3780 Die ID der Multicast-Gruppe des Clusters.
send-buffer { send-buffer }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 64 und 2560 **Standard:** 1220 Die Größe des Puffers des Sendesockels in kB.
recv-buffer { recv-buffer }	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 64 und 2560 **Standard:** 1220 Die Größe des Puffers der Empfangssockel in kB.

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 13.1.10.5
Einen fest zugeordneten Link löschen

Um einen fest zugeordneten Link zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den fest zugeordneten Link durch Eingabe von:

   ```
   no services conn-sync dedicated-link name
   ```

   Erläuterung: *name* ist die Bezeichnung des fest zugeordneten Links.
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 13.1.10.6

Einen fest zugeordneten Link auswählen

Um einen fest zugeordneten Link auszuwählen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Legen Sie den standardmäßig zugeordneten Link fest durch Eingabe von:

   ```
   services conn-sync default-dedicated-link link
   ```

   Erläuterung: *link* ist die Bezeichnung des standardmäßig zugeordneten Links.
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 13.1.10.7

Anzeigen des Status von jedem fest zugeordneten Link

Zum Anzeigen des Status aller fest zugeordneten Links gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Zum Anzeigen des Status aller fest zugeordneten Links geben Sie Folgendes ein:

   ```
   show services conn-sync status
   ```

   Eine Liste ähnlich der Folgenden wird angezeigt:

   ```
   ruggedcom# show services conn-sync status
   status fe-2-3
    state           NO-CARRIER
    role            ACTIVE
    byte sent       3614860
    byte received   0
    packet sent     114224
    packet received 0
    error sent      0
    error received  0
   status fe-2-4
    state           NO-CARRIER
    role            BACKUP
    byte sent       0
    byte received   0
    packet sent     0
    packet received 0
    error sent      0
    error received  0
   ```

   Die Liste liefert die folgenden Informationen:

Parameter	Beschreibung
name	**Zusammenfassung:** Eine Zeichenkette Der Schnittstellen-Name des fest zugeordneten "conn-sync"-Links.
state	**Zusammenfassung:** Eine Zeichenkette Der Status des fest zugeordneten "conn-sync"-Links.
role	**Zusammenfassung:** Eine Zeichenkette Die Rolle des fest zugeordneten "conn-sync"-Links.
byte-sent	**Zusammenfassung:** Eine vorzeichenlose 64-Bit-Ganzzahl Die Anzahl der am fest zugeordneten "conn-sync"-Link gesendeten Bytes.
byte-received	**Zusammenfassung:** Eine vorzeichenlose 64-Bit-Ganzzahl Die Anzahl der am fest zugeordneten "conn-sync"-Link empfangenen Bytes.
packet-sent	**Zusammenfassung:** Eine vorzeichenlose 64-Bit-Ganzzahl Die Anzahl der am fest zugeordneten "conn-sync"-Link gesendeten Pakete.
packet-received	**Zusammenfassung:** Eine vorzeichenlose 64-Bit-Ganzzahl Die Anzahl der am fest zugeordneten "conn-sync"-Link empfangenen Pakete.
error-sent	**Zusammenfassung:** Eine vorzeichenlose 64-Bit-Ganzzahl Die Anzahl der am fest zugeordneten "conn-sync"-Link gesendeten Fehler.
error-received	**Zusammenfassung:** Eine vorzeichenlose 64-Bit-Ganzzahl Die Anzahl der am fest zugeordneten "conn-sync"-Link empfangenen Fehler.

Abschnitt 13.2

Schutz vor Verbindungs-Failover verwalten

Ein Verbindungs-Failover ist eine leicht konfigurierbare Möglichkeit, eine Backup-Verbindung bei Ausfall einer Hauptverbindung zu errichten. Die Haupt- und Backup-Verbindungen können Ethernet und Mobilfunkmodem sein.

Verbindungs-Failover kann mehrere entfernte Standorte sichern und mehrere Haupt-zu-Backup-Verbindungs-Beziehungen verwalten.Wenn es sich bei der Backup-Verbindung um ein Modem handelt, können viele Profile gewählter Nummern existieren, von denen jede als eindeutige Backup-Verbindung dient.

Das Verbindungs-Failover kann eine permanente, schnelle WAN-Verbindung zu einer permanenten, langsamen WAN-Verbindung sichern. Verwenden Sie diese Funktion, wenn OSPF nicht eingesetzt werden kann, z. B. bei öffentlichen Verbindungen.

Ein Verbindungs-Failover kann auch verwendet werden, um die Standardroute von der Hauptverbindung auf die Backup-Verbindung zu migrieren.

Die Zeit nach dem Ausfall einer Hauptverbindung beim Starten der Backup-Verbindung und die Zeit nach der Wiederherstellung einer Hauptverbindung bis zum Stoppen der Backup-Verbindung sind konfigurierbar. Die Verbindungs-Failover-Funktion liefert auch Failover-Statusinformationen und einen Test der Failover-Einstellungen.

INHALT

- Abschnitt 13.2.1, „Anzeigen des Verbindungs-Failover-Protokolls“

- Abschnitt 13.2.2, „Den Status des Verbindungs-Failover anzeigen“
- Abschnitt 13.2.3, „Parameter für Verbindungs-Failover verwalten“
- Abschnitt 13.2.4, „Backup-Schnittstellen für Verbindungs-Failover verwalten“
- Abschnitt 13.2.5, „Ping-Ziele für Verbindungs-Failover verwalten“
- Abschnitt 13.2.6, „Testen des Verbindungs-Failovers“
- Abschnitt 13.2.7, „Einen Verbindungs-Failover-Test abbrechen“

Abschnitt 13.2.1

Anzeigen des Verbindungs-Failover-Protokolls

Um das Verbindungs-Failover-Protokoll anzuzeigen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Zeigen Sie das Protokoll an, indem Sie Folgendes eingeben:

```
services link-failover log
```

Eine Tabelle oder Liste ähnlich dem folgenden Beispiel wird angezeigt:

```
ruggedcom(config)# services link-failover switch.0001 log
link-backup-log /var/log/syslog:Jan 25 09:46:49 R1-RX1512 linkd[4183]: linkd initializing.
/var/log/syslog:Jan 25 09:46:49 R1-RX1512 linkd[4183]: linkd configured and started.
/var/log/syslog:Jan 25 09:46:49 R1-RX1512 linkd[4183]: linkd_interface_up: interface fe-cm-1 is up
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]: creating thread to monitor main=switch.0001
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]: setting new_backup_record
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]: setting new_backup_record done!
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]: dumping backup record:
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]:   main_interface = switch.0001
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]:     main_test_host = 10.10.10.10
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]:     start_delay = 180
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]:     main_path_down_timeout = 60
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]:     main_path_up_timeout = 60
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]:     backup_path_up_timeout = 60
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]:     ping_timeout = 2
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]:     ping_interval = 60
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]:     ping_retry_count = 3
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]:     backup_interface = fe-1-1
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]:       backup gateway = 192.168.1.2
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]:       ondemand = yes
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]:       distance = 1
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]:       transfer default route = yes
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]:     backup_interface = te1-2-1c01ppp
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]:       ondemand = yes
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]:       distance = 1
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]:       transfer default route = yes
/var/log/syslog:Jan 25 09:46:55 R1-RX1512 linkd[4183]: linkd_interface_up: interface fe-1-1 is up
/var/log/syslog:Jan 25 09:46:55 R1-RX1512 linkd[4183]: linkd_interface_down: interface fe-1-1 is
 down
/var/log/syslog:Jan 25 09:46:55 R1-RX1512 linkd[4183]: linkd_interface_up: interface fe-1-1 is up
/var/log/syslog:Jan 25 09:46:55 R1-RX1512 linkd[4183]: linkd_interface_down: interface fe-1-1 is
 down
/var/log/syslog:Jan 25 09:46:55 R1-RX1512 linkd[4183]: linkd_interface_up: interface fe-cm-1 is up
/var/log/syslog:Jan 25 09:46:55 R1-RX1512 linkd[4183]: linkd_interface_up: interface switch.0001 is
 up
/var/log/syslog:Jan 25 09:47:11 R1-RX1512 linkd[4183]: linkd_interface_down: interface switch.0001
 is down
/var/log/syslog:Jan 25 09:47:14 R1-RX1512 linkd[4183]: linkd_interface_up: interface switch.0001 is
 up
```

```
/var/log/syslog:Jan 25 09:49:52 R1-RX1512 linkd[4183]: Start monitoring link backup set:
 "switch.0001"
```

Abschnitt 13.2.2

Den Status des Verbindungs-Failover anzeigen

Das Formular "Link Failover Status" zeigt den aktuellen Status des Verbindungs-Failover. Um den Status des Verbindungs-Failover anzuzeigen, gehen Sie wie folgt vor:

```
show services link-failover status
```

Eine Tabelle oder Liste ähnlich dem folgenden Beispiel wird angezeigt:

```
ruggedcom# show services link-failover status
             MAIN    BACKUP  MAIN                                                BACKUP
             LINK    LINK    PING  TIME OF LAST STATE                            INTERFACE
MAIN         STATUS  STATUS  TEST  CHANGE                    LINK BACKUP STATE   IN USE
-------------------------------------------------------------------------------------------
switch.0001  up      down    ok    Fri Jan 25 09:49:52 2013  Main path is active  fe-1-1
```

Die Tabelle oder Liste liefert die folgenden Informationen:

Parameter	Beschreibung
main-link-status	**Zusammenfassung:** Eine Zeichenkette Der Zustand der Hauptverbindung.
backup-link-status	**Zusammenfassung:** Eine Zeichenkette Der Zustand der Backup-Verbindung.
main-ping-test	**Zusammenfassung:** Eine Zeichenkette Die Ergebnisse des Pingens des Ziels über die Hauptschnittstelle.
time-of-last-state-change	**Zusammenfassung:** Eine Zeichenkette Der Zeitpunkt der letzten Statusänderung.
link-backup-state	**Zusammenfassung:** Eine Zeichenkette Der Zustand der Backup-Verbindung.
backup-interface-in-use	**Zusammenfassung:** Eine Zeichenkette Der Name der Backup-Schnittstelle, die verwendet wird.

Abschnitt 13.2.3

Parameter für Verbindungs-Failover verwalten

Dieser Abschnitt beschreibt, wie Sie die Parametereinstellungen für Verbindungs-Failover verwalten können.

INHALT

- Abschnitt 13.2.3.1, „Eine Liste der Parameter für Verbindungs-Failover anzeigen“
- Abschnitt 13.2.3.2, „Hinzufügen eines Parameters für Verbindungs-Failover“
- Abschnitt 13.2.3.3, „Einen Parameter für Verbindungs-Failover löschen“

Abschnitt 13.2.3.1

Eine Liste der Parameter für Verbindungs-Failover anzeigen

Um eine Liste der Parameter für Verbindungs-Failover anzusehen, geben Sie Folgendes ein:

```
show running-config services link-failover
```

Falls Parameter konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config services link-failover
services
 link-failover switch.0001
  enabled
  backup fe-1-1
   transfer-default-route
   backup-gateway         192.168.1.2
  !
  backup te1-2-1c01ppp
   priority               second
   transfer-default-route
  !
  target 10.10.10.10
  !
 !
!
```

Falls keine Parameter konfiguriert wurden, fügen Sie je nach Bedarf Parameter hinzu. Weitere Informationen finden Sie unter Abschnitt 13.2.3.2, „Hinzufügen eines Parameters für Verbindungs-Failover“.

Abschnitt 13.2.3.2

Hinzufügen eines Parameters für Verbindungs-Failover

Um einen Parameter für Verbindungs-Failover hinzuzufügen, gehen Sie wie folgt vor:

HINWEIS
Die Funktion Verbindungs-Failover kann nur an einer routingfähigen Schnittstelle konfiguriert werden. Damit die Funktion Verbindungs-Failover an einem Switched-Port verwendet werden kann, muss ein anderes VLAN konfiguriert werden (z. B. switch.0002), um den Switched-Port logisch vom standardmäßigen PVID VLAN 1 (switch.0001) zu unterscheiden.

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den Parameter hinzu, indem Sie Folgendes eingeben:

   ```
   services link-failover interface
   ```

   Erläuterung:

   - *interface* ist die Bezeichnung der Schnittstelle
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
enabled	Aktiviert diesen Link-Backup.
ping-timeout { ping-timeout }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 1 und 65536 **Standard:** 2 Das Zeitintervall in Sekunden, unmittelbar bevor ein erneuter Ping-Versuch stattfindet.
ping-interval { ping-interval }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 0 und 65536

Parameter	Beschreibung
	Standard: 60 Das Zeitintervall in Sekunden zwischen Ping-Versuchen.
ping-retry { ping-retry }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 0 und 65536 **Standard:** 3 Die Anzahl an Ping-Versuchen vor Aufbau eines Pfadfehlers.
start-delay { start-delay }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 0 und 65536 **Standard:** 180 Die Verzögerungszeit in Sekunden beim ersten Start des Verbindungs-Failovers.
main-down-timeout { main-down-timeout }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 0 und 65536 **Standard:** 60 Die Verzögerungszeit in Sekunden, während der die Hauptverbindungsleitung nicht verfügbar ("down") ist, bevor die Backup-Leitung startet.
main-up-timeout { main-up-timeout }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 0 und 65536 **Standard:** 60 Die Verzögerungszeit in Sekunden, zur Bestätigung, dass die Hauptverbindungsleitung wieder verfügbar (wieder betriebsbereit) ist, bevor die Backup-Leitung beendet wird.

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 13.2.3.3
Einen Parameter für Verbindungs-Failover löschen

Um einen Parameter für Verbindungs-Failover zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den Parameter durch Eingabe von:

   ```
   no services link-failover interface
   ```

   Erläuterung:

   - *`interface`* ist die Bezeichnung der Schnittstelle
3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 13.2.4
Backup-Schnittstellen für Verbindungs-Failover verwalten

Eine Backup-Schnittstelle ist eine Schnittstelle, auf die bei einem Verbindungs-Failover umgeschaltet wird, wenn die Hauptschnittstelle ausgefallen ist. Sie können für jede Verbindungs-Failover-Konfiguration bis zu drei Backup-Schnittstellen festlegen.

INHALT

- Abschnitt 13.2.4.1, „Eine Liste der Backup-Schnittstellen für Verbindungs-Failover anzeigen“
- Abschnitt 13.2.4.2, „Hinzufügen einer Backup-Schnittstelle für Verbindungs-Failover“

- Abschnitt 13.2.4.3, „Eine Backup-Schnittstelle für Verbindungs-Failover löschen“

Abschnitt 13.2.4.1

Eine Liste der Backup-Schnittstellen für Verbindungs-Failover anzeigen

Um eine Liste der Backup-Schnittstellen für Verbindungs-Failover anzusehen, geben Sie Folgendes ein:

```
show running-config services link-failover interface backup
```

Erläuterung:

- *interface* ist die Bezeichnung der Schnittstelle

Falls Backup-Schnittstellen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config services link-failover switch.0001 backup
services
 link-failover switch.0001
  backup fe-1-1
   transfer-default-route
   backup-gateway         192.168.1.2
  !
  backup te1-2-1c01ppp
   priority               second
   transfer-default-route
  !
 !
!
```

Falls keine Backup-Schnittstellen konfiguriert wurden, fügen Sie je nach Bedarf Schnittstellen hinzu. Weitere Informationen finden Sie unter Abschnitt 13.2.4.2, „Hinzufügen einer Backup-Schnittstelle für Verbindungs-Failover“.

Abschnitt 13.2.4.2

Hinzufügen einer Backup-Schnittstelle für Verbindungs-Failover

Um eine Backup-Schnittstelle für Verbindungs-Failover hinzuzufügen, gehen Sie wie folgt vor:

ACHTUNG!
Konfigurationsrisiko – Gefahr des Verbindungsverlusts Wenn ein RUGGEDCOM APE-Modul installiert ist, vermeiden Sie entweder die Konfiguration von switch.0001 als Backup-Schnittstelle für Verbindungs-Failover oder Sie konfigurieren ein anderes VLAN für das APE-Modul. Standardmäßig nutzen APE-Module das VLAN 1 (switch.0001) und halten die Schnittstelle stets im UP-Zustand. Dies würde den Verbindungs-Failover-Mechanismus beeinträchtigen.

Um ein anderes VLAN für das APE-Modul zu konfigurieren, ändern Sie die PVID für den zugehörigen Switched-Ethernet-Port. Weitere Informationen finden Sie unter Abschnitt 8.1.2, „Einen Switched-Ethernet-Port konfigurieren“.

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie die Backup-Schnittstelle hinzu, indem Sie Folgendes eingeben:

   ```
   services link-failover interface backup backup-interface
   ```

   Erläuterung:

- *interface* ist die Bezeichnung der Schnittstelle
- *backup-interface* ist die Bezeichnung der sekundären Backup-Schnittstelle

3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:



HINWEIS
Konfigurieren Sie den Parameter backup-gateway *nicht für Punkt-zu-Punkt-(P2P)-Verbindungen.*



HINWEIS
Der Parameter on-demand *wird an der Schnittstelle gesetzt.*

Parameter	Beschreibung
priority { priority }	**Zusammenfassung:** { third, second, first } **Standard:** first Die Priorität, die beim Schalten für die Backup-Schnittstelle gilt.
transfer-default-route	Das Standard-Gateway zur Übertragung an der schaltenden Haupt- und Backup-Schnittstelle. Der *Abstand* der Standardroute auf dem Gerät muss größer als eins sein.
backup-gateway { backup-gateway }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 15 Zeichen Die IP-Adresse des Backup-Gateways.
on-demand	**Zusammenfassung:** { true, false } Zeigt den Status der On-Demand-Option der Schnittstelle an. Wenn die Option aktiviert ist, kann das Verbindungs-Failover die Schnittstelle bei Bedarf als verfügbar ("up") oder nicht verfügbar ("down") einstellen. Die Schnittstelle ist nicht verfügbar ("down"), bis vom Verbindungs-Failover benötigt wird. Ist die Option deaktiviert, kann das Verbindungs-Failover die Schnittstelle nicht als verfügbar ("up") oder nicht verfügbar ("down") einstellen. Standardmäßig ist die Schnittstelle immer verfügbar ("up").

Abschnitt 13.2.4.3

Eine Backup-Schnittstelle für Verbindungs-Failover löschen

Um eine Backup-Schnittstelle für Verbindungs-Failover zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die Backup-Schnittstelle, indem Sie Folgendes eingeben:

```
no services link-failover interface backup backup-interface
```

Erläuterung:

- *interface* ist die Bezeichnung der Schnittstelle
- *backup-interface* ist die Bezeichnung der sekundären Backup-Schnittstelle

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 13.2.5
Ping-Ziele für Verbindungs-Failover verwalten

Ein Ping-Ziel für ein Verbindungs-Failover ist eine IP-Adresse für Failover-Pings, mit denen festgestellt wird, ob die Hauptverbindung ausgefallen ist. Diese Adresse kann ein eigens zugewiesener Host oder eine Dummy-Adresse auf einem Router sein. Für jede Verbindungs-Failover-Konfiguration können bis zu drei Ping-Ziele hinzugefügt werden.

INHALT

- Abschnitt 13.2.5.1, „Eine Liste der Ping-Ziele für Verbindungs-Failover anzeigen“
- Abschnitt 13.2.5.2, „Hinzufügen eines Ping-Ziels für Verbindungs-Failover“
- Abschnitt 13.2.5.3, „Ein Ping-Ziel für Verbindungs-Failover löschen“

Abschnitt 13.2.5.1
Eine Liste der Ping-Ziele für Verbindungs-Failover anzeigen

Um eine Liste der Ping-Ziele für Verbindungs-Failover anzusehen, geben Sie Folgendes ein:

```
show running-config services link-failover interface target
```

Erläuterung:

- *interface* ist die Bezeichnung der Schnittstelle

Falls Ping-Ziele konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
R1-RX1512# show running-config services link-failover switch.0001 target
services
 link-failover switch.0001
  target 10.10.10.10
  !
 !
!
```

Falls keine Ping-Ziele konfiguriert wurden, fügen Sie je nach Bedarf Ziele hinzu. Weitere Informationen finden Sie unter Abschnitt 13.2.5.2, „Hinzufügen eines Ping-Ziels für Verbindungs-Failover“.

Abschnitt 13.2.5.2
Hinzufügen eines Ping-Ziels für Verbindungs-Failover

Um ein Ping-Ziel für Verbindungs-Failover hinzuzufügen, gehen Sie wie folgt vor:

HINWEIS
Die Verbindungs-Failover-Funktion sendet separate Ping-Anfragen an jedes Ziel. Wenn alle Ziele ausgefallen sind, dann wird die Hauptverbindung als ausgefallen betrachtet und es erfolgt ein Failover zur Backup-Schnittstelle. Backup-Verbindungen werden in der Reihenfolge ihrer Priorität (erste, zweite und dann dritte) und zwar immer beginnend mit der Schnittstelle erster Priorität verwendet. Wenn eine Schnittstelle einer höheren Priorität wieder verfügbar ist, dann schaltet das System zur Schnittstelle mit der höheren Priorität zurück. Wenn beispielsweise die Schnittstelle zweiter Priorität aktiv ist, schaltet das System zur Schnittstelle erster Priorität zurück, wenn die Schnittstelle erster Priorität wieder verfügbar ist.

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie das Ping-Ziel hinzu, indem Sie Folgendes eingeben:

   ```
   services link-failover interface target address
   ```

   Erläuterung:

   - *interface* ist die Bezeichnung der Schnittstelle
   - *address* ist die IP-Adresse des Ziel-Hosts zum Prüfen des Hauptpfads
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
{ host-ip }	**Zusammenfassung:** Eine Zeichenkette mit 7 bis 15 Zeichen Die IP-Adresse des Ziel-Hosts zum Prüfen des Hauptpfads.

Abschnitt 13.2.5.3

Ein Ping-Ziel für Verbindungs-Failover löschen

Um ein Ping-Ziel für Verbindungs-Failover zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die Backup-Schnittstelle, indem Sie Folgendes eingeben:

   ```
   no services link-failover interface target address
   ```

   Erläuterung:

   - *interface* ist die Bezeichnung der Schnittstelle
   - *address* ist die IP-Adresse des Ziel-Hosts zum Prüfen des Hauptpfades
3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 13.2.6

Testen des Verbindungs-Failovers

Die Verbindungs-Failover-Einstellungen können zur Bestätigung getestet werden, dass jede Verbindungs-Failover-Konfiguration ordnungsgemäß funktioniert. Um den Test zu starten, geben Sie an, wie lange das System an der Backup-Schnittstelle betrieben werden soll, und wie lange das System verzögern soll, bevor es mit dem Test beginnt. Ein Abbruch des Tests versetzt die Schnittstellen in den Zustand vor dem Test.

Überwachen Sie im laufenden Test den Status des Tests, um den Status der Haupt- und Backup-Verbindung, die Ergebnisse des Pingtests, eine Statusänderung, den Backup-Zustand und Informationen zur Backup-Schnittstelle zu verfolgen. Im Verlauf des Tests ändern sich diese Informationen, da das Link-Failover von der Hauptschnittstelle zur Backup-Schnittstelle umschaltet. Weitere Informationen über das Formular **Link Fail Over Status** finden Sie in Abschnitt 13.2.2, „Den Status des Verbindungs-Failover anzeigen“.

Um einen Verbindungs-Failover-Test zu starten, gehen Sie wie folgt vor:

HINWEIS
Der Verbindungs-Failover-Test kann jederzeit abgebrochen werden. Weitere Informationen über das Abbrechen eines Verbindungs-Failover-Tests finden Sie in Abschnitt 13.2.7, „Einen Verbindungs-Failover-Test abbrechen“.

Ein Abbruch des Tests versetzt die Schnittstellen in den Zustand vor dem Test.

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Starten Sie den Test, indem Sie Folgendes eingeben:

```
services link-failover interface start-test start-test-delay delay test-duration duration
```

Erläuterung:

- *interface* ist die Bezeichnung der Schnittstelle
- *delay* ist die Zeit (in Sekunden), die abgewartet wird, bevor der Test gestartet wird
- *duration* ist die maximale Dauer (in Minuten), die der Test ausgeführt wird, bevor der Dienst im Haupt-Trunk wiederhergestellt wird

Abschnitt 13.2.7

Einen Verbindungs-Failover-Test abbrechen

Um einen Verbindungs-Failover-Test abzubrechen, geben Sie Folgendes ein:

```
services link-failover interface cancel-test
```

Erläuterung:

- *interface* ist die Bezeichnung der Schnittstelle

14 Netzwerkerkennung und -management

RUGGEDCOM ROX II unterstützt die folgenden Protokolle für die automatische Netzwerkerkennung, -überwachung und das Gerätemanagement:

- **LLDP (Link Layer Device Protocol)**
  Mit LLDP können Sie die Netzwerkfunktionen und die Konfiguration des Geräts an andere Geräte im Netzwerk senden und Sendungen von anderen Geräten empfangen.
- **Simple Network Management Protocol (SNMP)**
  Mit SNMP können Sie ausgewählte Benutzer oder Gruppen über bestimmte Ereignisse benachrichtigen, die während des Gerätebetriebs auftreten, wie beispielsweise Änderungen der Netzwerktopologie, des Verbindungsstatus, der Spanning Tree Root usw.
- **Network Configuration Protocol (NETCONF)**
  Mit NETCONF können Sie Konfigurationsdaten in das Gerät laden, ändern, löschen und aus dem Gerät hochladen.

INHALT

- Abschnitt 14.1, „Verwalten von LLDP“
- Abschnitt 14.2, „Verwalten von SNMP“
- Abschnitt 14.3, „NETCONF verwalten“

Abschnitt 14.1

Verwalten von LLDP

Der RUGGEDCOM ROX II unterstützt das Link Layer Discovery-Protokoll (LLDP), ein Layer-2-Protokoll für die automatische Netzwerkerkennung.

LLDP ist ein im IEEE-Standard definiertes Protokoll (IEEE 802.11AB), das einem mit dem Netzwerk verbundenen Gerät erlaubt, eigene Basisinformationen über Netzwerkfähigkeiten und Konfiguration anzukündigen. Es kann dazu beitragen, die Fehlerbehebung in komplexen Netzwerken zu vereinfachen und kann von Netzwerkmanagementsystemen (NMS) zum Abrufen und Überwachen detaillierter Informationen über die Topologie eines Netzwerks verwendet werden. LLDP-Daten werden über SNMP (durch Unterstützung von LLDP-MIB) verfügbar gemacht.

LLDP erlaubt einem vernetzten Gerät, anhand eines Standardmechanismus seine Nachbarn über angeschaltete Netzwerkverbindungen zu erkennen. Geräte, die LLDP unterstützen, können Informationen über sich ankündigen, darunter Informationen über Fähigkeiten, Konfiguration, Verschaltungen und zur Identifikation.

Der LLDP-Agent-Betrieb wird üblicherweise in Form von zwei Modulen implementiert: das LLDP-Sendemodul und das LLDP-Empfangsmodul. Das LLDP-Sendemodul sendet im aktivierten Zustand regelmäßig Informationen des lokalen Geräts im 802.1AB-Standardformat. Wenn das Sendemodul deaktiviert ist, überträgt es eine LLDPDU (LLDP Data Unit) mit einem Time-To-Live (TTL) TLV, der den Wert *0* im Informationsfeld enthält. Dadurch können

dezentrale Geräte die mit dem lokalen Gerät verknüpften Informationen in ihren Datenbanken löschen. Das LLDP-Empfangsmodul empfängt im aktivierten Zustand Informationen über dezentrale Geräte und aktualisiert seine LLDP-Datenbank der dezentralen Systeme. Wenn neue oder aktualisierte Informationen empfangen werden, initiiert das Empfangsmodul einen Timer für die gültige Dauer, die von dem TTL TLV in der empfangenen LLDPDU angegeben wird. Die Informationen des dezentralen Systems werden aus der Datenbank entfernt, wenn eine LLDPDU empfangen wird mit einem TTL TLV, der den Wert *0* im Informationsfeld enthält.

ACHTUNG!
Sicherheitsgefahr – Risiko des unbefugten Zugriffs und/oder Missbrauchs. LLDP ist der Definition nach nicht sicher. Vermeiden Sie die Aktivierung von LLDP auf mit externen Netzwerken verbundenen Geräten. Siemens empfiehlt die Verwendung von LLDP ausschließlich in sicheren Umgebungen, die innerhalb eines Sicherheitsumfelds betrieben werden.

HINWEIS
LLDP wird implementiert, um Aufzeichnungen über ein einziges Gerät pro Ethernet-Port vorzunehmen. Wenn demzufolge mehrere Geräte existieren, die LLDP-Informationen an einen Switchport senden, an dem LLDP aktiviert ist, dann werden sich die Informationen über den Nachbarn an diesem Port permanent ändern.

INHALT

- Abschnitt 14.1.1, „Das LLDP konfigurieren“
- Abschnitt 14.1.2, „Anzeigen der globalen Statistik und bekanntgegebener Systeminformationen“
- Abschnitt 14.1.3, „Statistiken für LLDP-Nachbarn anzeigen“
- Abschnitt 14.1.4, „Anzeigen der Statistik für LLDP-Ports“

Abschnitt 14.1.1

Das LLDP konfigurieren

Um das Link Layer Discovery Protocol (LLDP) zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***switch » net-discovery » lldp*** und konfigurieren Sie den/die folgenden Parameter nach Bedarf:

Parameter	Beschreibung
enabled	**Zusammenfassung:** { true, false } **Standard:** true Aktiviert das Link Layer Discovery Protocol (LLDP). Beachten Sie, dass LLDP an einem Port aktiviert ist, wenn es global aktiviert und im Menü "Port LLDP Parameters" je Port eingestellt ist.
tx-interval { tx-interval }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 5 und 32768 **Standard:** 30 Das Intervall, in dem Link Layer Discovery Protocol (LLDP)-Frames im Auftrag des LLDP Agent übertragen werden.
tx-hold { tx-hold }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 2 und 10 **Standard:** 4 Der Multiplikator des Parameters "Tx Interval", der den tatsächlichen in einer LLDPU verwendeten Lebenszeit (TTL, en time-to-live)-Wert bestimmt. Der tatsächliche TTL-Wert

Parameter	Beschreibung
	kann durch die folgende Gleichung angegeben werden: TTL = MIN(65535, (Tx Interval * Tx Hold))
reinit-delay { reinit-delay }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 1 und 10 **Standard:** 2 Die Verzögerung in Sekunden, zwischen dem Zeitpunkt, wenn der Wert des Parameters "Admin Status" eines bestimmten Ports deaktiviert wird ('Disbled'), und dem Zeitpunkt, zu dem der Versuch einer erneuten Initialisierung erfolgt.
tx-delay { tx-delay }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 1 und 8192 **Standard:** 2 Die Verzögerung in Sekunden zwischen aufeinanderfolgenden Übertragungen von LLDP-Frames, die von einem veränderten Wert oder Status ausgelöst werden. Der empfohlene Wert ergibt sich durch die folgende Gleichung: 1 ist kleiner als oder gleich txDelay kleiner oder gleich (0,25 * Tx Interval)
notification-interval { notification-interval }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 5 und 3600 **Standard:** 5 Steuert die Übertragung von LLDP-Traps. Der Agent darf in einem vorgegebenen Zeitraum nicht mehr als ein Trap erzeugen.

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 14.1.2

Anzeigen der globalen Statistik und bekanntgegebener Systeminformationen

Um die globale Statistik für LLDP anzuzeigen, geben Sie Folgendes ein:

```
show switch net-discovery lldp global-statistics
```

Eine Tabelle oder Liste ähnlich dem folgenden Beispiel wird angezeigt:

```
ruggedcom# show switch net-discovery lldp global-statistics
global-statistics
 inserts          21
 deletes          20
 drops            0
 ageouts          8
 last change time 3D14m19s
```

Diese Tabelle oder Liste zeigt die folgenden Informationen:

Parameter	Beschreibung
inserts	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 0 und 4294967295 Die Anzahl der Einträge in die Tabelle "LLDP Neighbor Information". Dieser Parameter ist obligatorisch.
deletes	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 0 und 4294967295 Die Anzahl der Löschungen eines Eintrags aus der Tabelle "LLDP Neighbor Information". Dieser Parameter ist obligatorisch.
drops	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 0 und 4294967295

Parameter	Beschreibung
	Die Anzahl der Löschungen eines Eintrags aus der Tabelle "LLDP Neighbor Information", weil das Intervall für die Rechtzeitigkeit der Informationen abgelaufen ist. Dieser Parameter ist obligatorisch.
ageouts	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 0 und 4294967295 Die Anzahl aller verworfenen TLV. Dieser Parameter ist obligatorisch.
last-change-time	**Zusammenfassung:** Eine Zeichenkette Die Zeitdauer zwischen Einschalten und Empfang dieser Informationen. Dieser Parameter ist obligatorisch.

Um die den Nachbarn angekündigten Systeminformationen anzuzeigen, geben Sie Folgendes ein:

```
show switch net-discovery lldp local-system
```

Eine Tabelle oder Liste ähnlich dem folgenden Beispiel wird angezeigt:

```
ruggedcom#  show switch net-discovery lldp local-system
local-system
 local chassis subtype     macAddress
 local chassis id          00:0a:dc:ff:9a:00
 local system name         R12.localdomain
 local system desc         RX5000-R-MNT-HI-HI-SM61-CM01-L3SEC-16TX01-XX-XX-XX-4FG50-XX
 local system caps         bridge,router
 local system caps enabled bridge,router
```

Diese Tabelle oder Liste zeigt die folgenden Informationen:

Parameter	Beschreibung
local-chassis-subtype	**Zusammenfassung:** { chassisComponent, interfaceAlias, portComponent, macAddress, networkAddress, interfaceName, local } local-chassis-subtype Dieser Parameter ist obligatorisch.
local-chassis-id	**Zusammenfassung:** Eine Zeichenkette mit 17 Zeichen local-chassis-id Dieser Parameter ist obligatorisch.
local-system-name	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 255 Zeichen local-system-name Dieser Parameter ist obligatorisch.
local-system-desc	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 255 Zeichen local-system-desc Dieser Parameter ist obligatorisch.
local-system-caps	**Zusammenfassung:** { other, repeater, bridge, wlanAccessPoint, router, telephone, docsisCableDevice, stationOnly } local-system-caps Dieser Parameter ist obligatorisch.
local-system-caps-enabled	**Zusammenfassung:** { other, repeater, bridge, wlanAccessPoint, router, telephone, docsisCableDevice, stationOnly } local-system-caps-enabled Dieser Parameter ist obligatorisch.

Abschnitt 14.1.3

Statistiken für LLDP-Nachbarn anzeigen

Um Statistiken für LLDP-Nachbarn anzuzeigen, geben Sie Folgendes ein:

```
show switch net-discovery lldp port-lldp-neighbors
```

Eine Tabelle oder Liste ähnlich dem folgenden Beispiel wird angezeigt:

```
ruggedcom# show switch net-discovery lldp port-lldp-neighbors port-lldp-neighbors swport 1 chassis id
 "" port id "" system name "" system desc "" port desc "" man address "" man address if id 0 system
 caps "" system caps enabled "" chassis subtype macAddress port subtype interfaceName man address
 subtype other man address if subtype unknown last update 0s
```

Diese Tabelle oder Liste liefert die folgenden Informationen:

Parameter	Beschreibung
slot	**Zusammenfassung:** { { --- }{ pm1, pm2, main }{ sm, lm1, lm2, lm3, lm4, lm5, lm6, swport, eth, serport, celport, wlanport }{ cm, em }{ trnk } } Der Steckplatz des Moduls, das diesen Port enthält.
port	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 1 und 16 Die Portnummer, wie auf der Frontscheibe des Switch aufgedruckt.
chassis-id	**Zusammenfassung:** Eine Zeichenkette mit 17 Zeichen Die von einem entfernten Link Layer Discovery Protocol (LLDP) Agent erhaltenen Angaben zur Chassiskennung.
port-id	**Zusammenfassung:** Eine Zeichenkette mit 17 Zeichen Die von einem entfernten Link Layer Discovery Protocol (LLDP) Agent erhaltenen Angaben zur Port-ID (MAC).
system-name	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 255 Zeichen Die von einem entfernten Link Layer Discovery Protocol (LLDP) Agent erhaltenen Angaben zum Systemnamen.
system-desc	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 255 Zeichen Die von einem entfernten Link Layer Discovery Protocol (LLDP) Agent erhaltenen Angaben zum System-Deskriptor.
port-desc	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 255 Zeichen Die von einem entfernten Link Layer Discovery Protocol (LLDP) Agent erhaltenen Angaben zur Port-Beschreibung.
man-address	**Zusammenfassung:** Eine Zeichenkette mit 31 Zeichen Die von einem entfernten Link Layer Discovery Protocol (LLDP) Agent erhaltene Verwaltungsadresse.
man-address-if-id	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl Die von einem entfernten Link Layer Discovery Protocol (LLDP) Agent erhaltene Schnittstellen-ID der Verwaltungsadresse.
system-caps	**Zusammenfassung:** { other, repeater, bridge, wlanAccessPoint, router, telephone, docsisCableDevice, stationOnly } Die vom entfernten Gerät angekündigte Systemkapazität.
system-caps-enabled	**Zusammenfassung:** { other, repeater, bridge, wlanAccessPoint, router, telephone, docsisCableDevice, stationOnly } Aktiviert/deaktiviert die Funktion "System Capabilities".

Parameter	Beschreibung
chassis-subtype	**Zusammenfassung:** { chassisComponent, interfaceAlias, portComponent, macAddress, networkAddress, interfaceName, local } Die von einem entfernten Link Layer Discovery Protocol (LLDP) Agent erhaltenen Angaben zum Chassis-Subtyp.
port-subtype	**Zusammenfassung:** { interfaceAlias, portComponent, macAddress, networkAddress, interfaceName, agentCircuitId, local } Die von einem entfernten Link Layer Discovery Protocol (LLDP) Agent erhaltenen Angaben zum Port-Subtyp.
man-address-subtype	**Zusammenfassung:** { other, ipV4, ipV6, nsap, hdlc, bbn1822, all802, e163, e164, f69, x121, ipx, appleTalk, decnetIV, banyanVines, e164withNsap, dns, distinguishedName, asNumber, xtpOverIpv4, xtpOverIpv6, xtpNativeModeXTP, fibreChannelWWPN, fibreChannelWWNN, gwid, afi, reserved } Der von einem entfernten Link Layer Discovery Protocol (LLDP) Agent erhaltene Subtyp der Verwaltungsadresse.
man-address-if-subtype	**Zusammenfassung:** { unknown, ifIndex, systemPortNumber } Der von einem entfernten Link Layer Discovery Protocol (LLDP) Agent erhaltene Schnittstellen-Subtyp der Verwaltungsadresse.
last-update	**Zusammenfassung:** Eine Zeichenkette Die Zeitdauer zwischen Einschalten und Empfang dieser Informationen.

Abschnitt 14.1.4

Anzeigen der Statistik für LLDP-Ports

Um die Statistik für LLDP-Ports anzuzeigen, geben Sie Folgendes ein:

```
show switch net-discovery lldp port-lldp-stats
```

Eine Tabelle oder Liste ähnlich dem folgenden Beispiel wird angezeigt:

```
ruggedcom# show switch net-discovery lldp port-lldp-stats FRM ERR FRM FRM TLVS TLVS SLOT PORT DRP FRM
 IN OUT AGEOUTS DROP UNKNOWN ------------------------------------------------------------ swport 1 0 0 0
 0 0 0 0 swport 2 0 0 0 0 0 0 0 swport 3 0 0 0 0 0 0 0 swport 4 0 0 208 209 0 0 0 swport 5 0 0 0 0 0 0
 0 swport 6 0 0 0 0 0 0 0
```

Diese Tabelle oder Liste zeigt die folgenden Informationen:

Parameter	Beschreibung
slot	**Zusammenfassung:** { { --- }{ pm1, pm2, main }{ sm, lm1, lm2, lm3, lm4, lm5, lm6, swport, eth, serport, celport, wlanport }{ cm, em }{ trnk } } Der Steckplatz des Moduls, das diesen Port enthält.
port	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 1 und 16 Die Portnummer, wie auf der Frontscheibe des Switch aufgedruckt.
frm-drp	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 0 und 4294967295 Eine Zählung aller verworfenen Link Layer Discovery Protocol (LLDP)-Frames Dieser Parameter ist obligatorisch.
err-frm	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 0 und 4294967295 Eine Zählung aller erhaltenen Link Layer Discovery Protocol Units (LLDPUs) mit erkennbaren Fehlern.

Parameter	Beschreibung
	Dieser Parameter ist obligatorisch.
frm-in	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 0 und 4294967295 Eine Zählung aller erhaltenen Link Layer Discovery Protocol Units (LLDPUs). Dieser Parameter ist obligatorisch.
frm-out	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 0 und 4294967295 Eine Zählung aller übertragenen Link Layer Discovery Protocol Units (LLDPUs). Dieser Parameter ist obligatorisch.
ageouts	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 0 und 4294967295 Eine Zählung der Male, bei denen die Informationen eines Nachbarn aus dem Link Layer Discovery Protocol (LLDP)-MIB des entfernten Systems gelöscht wurden, weil der Timer "txinfoTTL" abgelaufen ist. Dieser Parameter ist obligatorisch.
tlvs-drop	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 0 und 4294967295 Eine Zählung aller verworfenen TLV. Dieser Parameter ist obligatorisch.
tlvs-unknown	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl zwischen 0 und 4294967295 Eine Zählung aller am Port empfangenen TLV, die nicht vom lokalen Link Layer Discovery Protocol (LLDP) Agent erkannt wurden. Dieser Parameter ist obligatorisch.

Abschnitt 14.2

Verwalten von SNMP

Das Simple Network Management-Protokoll (SNMP) wird von Netzwerkmanagementsystemen und den Geräten verwendet, die diese verwalten. Es wird zum Melden von Alarmbedingungen und weiteren Ereignissen verwendet, die auf den Geräten auftreten, die es verwaltet.

Der RUGGEDCOM ROX II unterstützt zusätzlich zu SNMPv1 und SNMPv2 auch SNMPv3, das folgende Funktionen bietet:

- Ermöglicht das Senden einer Benachrichtigung zu einem Ereignis über *Traps*. Traps sind unquittierte UDP-Nachrichten, die bei der Übertragung verloren gehen können.
- Bietet die Möglichkeit einer Benachrichtigung per so genannter *Informs*. Die "Informs" ergänzen den Trap-Prozess um Quittierungen, d.h. der Trap wird erneut gesendet, wenn er nicht rechtzeitig quittiert wurde.
- Verschlüsselt alle übertragenen Daten durch Chiffrieren des Inhalts aller Pakete, damit diese nicht von einer unbefugten Quelle gesehen werden. Die Verschlüsselungsprotokolle AES CFB 128 und DES3 werden unterstützt.
- Authentifiziert alle Nachrichten zwecks Prüfung, dass diese von einer gültigen Quelle stammen.
- Überprüft die Integrität aller Nachrichten, indem sichergestellt wird, dass Pakete während der Übertragung nicht manipuliert wurden.

Außerdem bietet SNMPv3 Sicherheitsmodelle und Sicherheitsstufen. Bei einem Sicherheitsmodell handelt es sich um eine Authentifizierungsstrategie, die für einen Benutzer und die Gruppe, in der sich der Benutzer befindet, erstellt wird. Eine Sicherheitsstufe ist eine zulässige Sicherheitsstufe innerhalb eines Sicherheitsmodells. Eine Kombination aus Sicherheitsmodell und Sicherheitsstufe legt fest, welcher Sicherheitsmechanismus bei der Handhabung von SNMP-Paketen eingesetzt wird.

Beachten Sie vor der Konfiguration von SNMP Folgendes:

- jeder Benutzer gehört zu einer Gruppe
- eine Gruppe legt die Grundregel für den Zugriff für einen Satz Benutzer fest
- eine Grundregel für den Zugriff legt fest, auf welche SNMP-Objekte zum Lesen, Schreiben und Erstellen von Benachrichtigungen zugegriffen werden darf
- eine Gruppe legt die Liste der Benachrichtigungen fest, die ihre Benutzer empfangen können
- eine Gruppe legt auch das Sicherheitsmodell und die Sicherheitsstufe für ihre Benutzer fest

INHALT

- Abschnitt 14.2.1, „MIB-Dateien und SNMP-Traps“
- Abschnitt 14.2.2, „Aktivieren und Konfigurieren von SNMP-Sitzungen“
- Abschnitt 14.2.3, „Statistiken für SNMP anzeigen“
- Abschnitt 14.2.4, „IDs von SNMP-Protokoll-Engines finden“
- Abschnitt 14.2.5, „SNMP-Communities verwalten“
- Abschnitt 14.2.6, „SNMP-Zieladressen verwalten“
- Abschnitt 14.2.7, „SNMP-Benutzer verwalten“
- Abschnitt 14.2.8, „Zuordnung des SNMP-Sicherheitsmodells verwalten“
- Abschnitt 14.2.9, „SNMP-Gruppenzugang verwalten“

Abschnitt 14.2.1

MIB-Dateien und SNMP-Traps

Die vom RUGGEDCOM ROX II unterstützten aktuellen MIB-Dateien können unter https://www.siemens.com/ruggedcom heruntergeladen werden.

HINWEIS
SNMP-Traps sind im RUGGEDCOM ROX II nicht konfigurierbar.

Die MIB-Dateien unterstützen folgende SNMP-Traps:

Standard	MIB	Trap und Beschreibung
RFC 3418	SNMPv2-MIB	**authenticationFailure** Ein "authenticationFailure"-Trap bedeutet, dass die SNMP-Einheit eine Protokollnachricht empfangen hat, die nicht ordnungsgemäß authentifiziert wurde. Während alle Implementierungen von SNMP-Einheiten diesen Trap generieren KÖNNEN, gibt das "snmpEnableAuthenTraps"-Objekt an, ob dieser Trap generiert wird.
		coldStart Ein "coldStart"-Trap bedeutet, dass die SNMP-Einheit, die eine Benachrichtigungsherkunft-Anwendung unterstützt, sich selbst reinitialisiert und dass deren Konfiguration möglicherweise geändert wurde.

Standard	MIB	Trap und Beschreibung
		warmStart Ein "warmStart"-Trap bedeutet, dass die SNMP-Einheit, die eine Benachrichtigungsherkunft-Anwendung unterstützt, sich selbst reinitialisiert und deren Konfiguration dabei nicht ändert.
RFC 4188	BRIDGE-MIB	**newRoot** Der "newRoot"-Trap gibt an, dass der sendende Agent die neue Wurzel (Root) des Spannbaums wurde. Der Trap wird von einer Bridge kurz nach seiner Wahl als neue Root (z. B. nach Ablauf des Topology Change Timer) unmittelbar nach seiner Wahl gesendet. Die Implementierung dieses Trap ist optional.
		topologyChange Ein "topologyChange"-Trap wird von einer Bridge gesendet, wenn einer ihrer konfigurierten Ports vom "Learning"-Zustand in den "Forwarding"-Zustand bzw. vom "Forwarding"-Zustand in den "Blocking"-Zustand übergeht. Der Trap wird nicht gesendet, wenn ein "newRoot"-Trap für denselben Übergang gesendet wird. Die Implementierung dieses Trap ist optional.
IEEE Std 802.1AB-2005	LLDP-MIB	**lldpRemTablesChange** Eine "lldpRemTablesChange"-Benachrichtigung wird gesendet, wenn sich der Wert von "lldpStatsRemTableLastChangeTime" ändert. Sie kann vom Netzwerkmanagementsystem (NMS) verwendet werden, um Wartungsabfragen auszulösen. Beachten Sie, dass die Übertragung von "lldpRemTablesChange"-Benachrichtigungen vom Agenten gedrosselt werden, wie vom "lldpNotificationInterval"-Objekt vorgegeben.
RFC 1229, 2863, 2233, 1573	IF-MIB	**linkUp** Ein "linkUp"-Trap bedeutet, dass die SNMP-Einheit, die eine Agentenfunktion ausübt, erkannt hat, dass das "ifOperStatus"-Objekt für eine seiner Kommunikationsverbindungen den "down"-Zustand verlassen und in einen anderen Zustand (jedoch nicht in den "notPresent"-Zustand) übergegangen ist. Dieser andere Zustand wird vom in "ifOperStatus" enthaltenen Wert angegeben.
		linkDown Ein "linkDown"-Trap bedeutet, dass die SNMP-Einheit, die eine Agentenfunktion ausübt, erkannt hat, dass das "ifOperStatus"-Objekt für eine seiner Kommunikationsverbindungen von einem anderen Zustand (jedoch nicht vom "notPresent"-Zustand) in den "down"-Zustand übergeht. Dieser andere Zustand wird vom in "ifOperStatus" enthaltenen Wert angegeben.
RuggedCom	RUGGEDCOM-TRAPS-MIB	**trapGenericTrap** Der Haupt-Unterbaum für generische Traps des RUGGEDCOM. Wird ausschließlich für *Benutzer-Authentifizierungsereignisse* verwendet.
		trapPowerSupplyTrap Der Haupt-Unterbaum für Stromversorgungs-Traps des RUGGEDCOM.
		trapSwUpgradeTrap Der Haupt-Unterbaum für Softwareaktualisierungs-Traps des RUGGEDCOM.
		trapCfgChangeTrap Der Haupt-Unterbaum für Konfigurationsänderungs-Traps des RUGGEDCOM.
		trapFanBankTrap Der Haupt-Unterbaum für Lüfterbank-Traps des RUGGEDCOM.
		trapHotswapModuleStateChangeTrap Der Haupt-Unterbaum für Traps des RUGGEDCOM in Verbindung mit Zustandsänderungen des Hot-Swap-Lüftermoduls.

Standard	MIB	Trap und Beschreibung
RFC 3895	DS1-MIB	**ds1LineStatusChange** Ein "ds1LineStatusChange"-Trap wird gesendet, wenn sich der Zustand der "dsx1Line"-Instanz ändert. Der Wert des Trap ist der Wert einer oder mehrerer der folgenden Instanzen: • **dsx1RcvFarEndLOF** – Far End Loss of Frames (d.h. gelber Alarm oder RAI) • **dsx1RcvAIS** – Far End Sending AIS • **dsx1LossOfFrame** – Near End Loss of Frame (d.h. roter Alarm) • **dsx1LossofSignal** – Near End Loss of Signal • **dsx1OtherFailure** – Out of Frame • **dsx1NoAlarm**

Abschnitt 14.2.2

Aktivieren und Konfigurieren von SNMP-Sitzungen

Um SNMP-Sitzungen zu aktivieren und zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***admin » snmp*** und konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

WICHTIG!
Um den gesamten SNMP-Verkehr für eine bestimmte Schnittstelle zu generieren, stellen Sie sicher, dass die IP-Adresse für die gewünschte Schnittstelle für den `Listen IP` *und* `Source IP für Traps` *– Parameter gesetzt ist.*

Parameter	Beschreibung
enabled	**Zusammenfassung:** { true, false } **Standard:** false Ermöglicht es, SNMP-Funktionen am Gerät zu konfigurieren.
listen-ip { listen-ip }	**Zusammenfassung:** Eine Zeichenkette **Standard:** 0.0.0.0 Die IP-Adresse, an der der SNMP Agent SNMP-Anfragen empfängt.
port { port }	**Zusammenfassung:** Eine vorzeichenlose 16-Bit-Ganzzahl zwischen 0 und 65535 **Standard:** 161 Der Port, an dem der SNMP Agent SNMP-Anfragen empfängt.
extra-ip-ports { extra-ip-ports }	**Zusammenfassung:** Eine Zeichenkette Der SNMP Agent empfängt auch an diesen IP-Adressen. Fügen Sie bei Port-Werten ':#' hinzu, um die nicht voreingestellten Port-Werte einzustellen (d. h. xxx.xxx.xxx.xxx:19343 [::] [::]:16000). Bei Verwendung der Standardadresse legen Sie keine empfangende Adresse mit dem gleichen Port fest.
max-sessions { max-sessions }	**Zusammenfassung:** eine vorzeichenlose 32-Bit-Ganzzahl **Standard:** 30 Die maximale Anzahl gleichzeitiger SNMP-Sitzungen.
snmp-engine-id { snmp-engine-id }	**Zusammenfassung:** Eine Zeichenkette Bietet eine spezifische Kennung für die Maschine/das Gerät. Standardmäßig ist dieser Wert so eingestellt, dass die MAC-Basisadresse innerhalb des Engine ID-Werts verwendet wird.

Parameter	Beschreibung
	Bei SNMPv3: Wenn Sie diesen Wert ändern, müssen Sie ebenso den Wert der User SNMP Engine ID für SNMP-Benutzer ändern.
source-ip { source-ip }	**Zusammenfassung:** Eine Zeichenkette Falls eingestellt muss/müssen der gesamte Verkehr/alle Traps von diesem Gerät die konfigurierte IP-Adresse für die Quell-IP verwenden.
auth-failure-trap-notify { auth-failure-trap-notify }	**Zusammenfassung:** { none, snmpv1_trap, snmpv2_trap, snmpv2_inform, snmpv3_trap, snmpv3_inform } **Standard:** none Wenn der SNMP Agent die Standardmeldung authenticationFailure sendet, wird diese an die Management-Ziele geliefert, die für den snmpNotifyName in der Tabelle snmpNotify in SNMP-NOTIFICATION-MIB (RFC3413) festgelegt sind. Falls authenticationFailureNotifyName (standardmäßig) die leere Zeichenkette ist, wird die Meldung an alle Management-Ziele gesendet.
authen-traps-enabled	**Zusammenfassung:** { true, false } **Standard:** false Aktiviert Authentifizierung-Traps, die vom SNMP Agent zu senden sind.
dscp { dscp }	**Zusammenfassung:** Eine vorzeichenlose 8-Bit-Ganzzahl zwischen 0 und 63 **Standard:** 0 Unterstützung zur Einstellung des differenzierten Dienst-Kodierungspunkts (6-Bit) für Verkehr, der vom SNMP Agent stammt.

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 14.2.3
Statistiken für SNMP anzeigen

Um die Statistiken für SNMP anzusehen, geben Sie Folgendes ein:

```
show admin snmp statistics
```

Wenn Statistiken vorhanden sind, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show admin snmp statistics
statistics
 unsupported sec levels 1
 not in time windows    1
 unknown user names     1
 unknown engine ids     4
 wrong digests          1
 decryption errors      1
```

Diese Tabelle oder Liste liefert die folgenden Informationen:

Parameter	Beschreibung
unsupported-sec-levels	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Gesamtzahl der vom SNMP Engine empfangenen Pakete, die verworfen wurden, weil sie ein securityLevel angefordert haben, das dem SNMP Engine unbekannt oder anderweitig nicht verfügbar war. Dieser Parameter ist obligatorisch.
not-in-time-windows	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl

Parameter	Beschreibung
	Die Gesamtzahl der vom SNMP Engine empfangenen Pakete, die verworfen wurden, weil sie außerhalb des Fensters des autoritativen SNMP Engines erschienen. Dieser Parameter ist obligatorisch.
unknown-user-names	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Gesamtzahl der vom SNMP Engine empfangenen Pakete, die verworfen wurden, weil sie auf einen Benutzer verwiesen, der dem SNMP Engine unbekannt war. Dieser Parameter ist obligatorisch.
unknown-engine-ids	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Gesamtzahl der vom SNMP Engine empfangenen Pakete, die verworfen wurden, weil sie auf eine snmpEngineID verwiesen, die dem SNMP Engine unbekannt war. Dieser Parameter ist obligatorisch.
wrong-digests	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Gesamtzahl der vom SNMP Engine empfangenen Pakete, die verworfen wurden, weil sie nicht den erwarteten Digest-Wert enthielten. Dieser Parameter ist obligatorisch.
decryption-errors	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Gesamtzahl der vom SNMP Engine empfangenen Pakete, die verworfen wurden, weil sie nicht entschlüsselt werden konnten. Dieser Parameter ist obligatorisch.

Abschnitt 14.2.4
IDs von SNMP-Protokoll-Engines finden

Um eine ID einer entfernten SNMP-Protokoll-Engine zu finden, gehen Sie wie folgt vor:

1. Geben Sie auf Aufforderung den folgenden Befehl ein:

```
admin snmp snmp-discover
```

2. Bei Aufforderung geben Sie die IP-Adresse der entfernten SNMP-Protokoll-Engine ein.

```
ruggedcom# admin snmp snmp-discover
Value for 'address' (<string, min: 7 chars, max: 15 chars>): ip-address
```

Nach der Erkennung wird die ID angezeigt. Beispiel:

```
snmp-discover-return-string 80:00:3A:9C:03:94:B8:C5:FF:F6:00
```

Abschnitt 14.2.5
SNMP-Communities verwalten

Dieser Abschnitt beschreibt, wie Sie SNMP-Communities verwalten können.

INHALT

- Abschnitt 14.2.5.1, „Eine Liste der SNMP-Communities anzeigen“
- Abschnitt 14.2.5.2, „Eine SNMP-Community hinzufügen“

- Abschnitt 14.2.5.3, „Eine SNMP-Community löschen“

Abschnitt 14.2.5.1
Eine Liste der SNMP-Communities anzeigen

Um eine Liste der im Gerät konfigurierten SNMP-Communities anzusehen, geben Sie Folgendes ein:

```
show running-config admin snmp snmp-community name
```

Falls Communities konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config admin snmp snmp-community | tab
COMMUNITY  USER
NAME       NAME
------------------
private    oper
public     guest

 !
!
```

Standardmäßig sind private und öffentliche Communities vorkonfiguriert. Werden zusätzliche Communities benötigt, können diese je nach Bedarf hinzugefügt werden. Weitere Informationen finden Sie unter Abschnitt 14.2.5.2, „Eine SNMP-Community hinzufügen“.

Abschnitt 14.2.5.2
Eine SNMP-Community hinzufügen

Um eine SNMP-Community hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie die SNMP-Community hinzu, indem Sie Folgendes eingeben:

   ```
   admin snmp snmp-community name
   ```

   Erläuterung:

   - *name* ist die Bezeichnung der Community
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
{ community-name }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 32 Zeichen Der SNMP-Community-Name.
user-name { user-name }	**Zusammenfassung:** Eine Zeichenkette Der SNMP-Community-Sicherheitsname. Dieser Parameter ist obligatorisch.

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 14.2.5.3
Eine SNMP-Community löschen

Um eine SNMP-Community zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die SNMP-Community durch Eingabe von:

   ```
   no admin snmp snmp-community name
   ```

   Erläuterung:

   - *name* ist die Bezeichnung der Community
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 14.2.6
SNMP-Zieladressen verwalten

Dieser Abschnitt beschreibt, wie Sie SNMP-Zieladressen verwalten können.

INHALT

- Abschnitt 14.2.6.1, „Eine Liste der SNMP-Zieladressen anzeigen“
- Abschnitt 14.2.6.2, „Eine SNMP-Zieladresse hinzufügen“
- Abschnitt 14.2.6.3, „Eine SNMP-Zieladresse löschen“

Abschnitt 14.2.6.1
Eine Liste der SNMP-Zieladressen anzeigen

Um eine Liste der SNMP-Zieladressen, die auf einem Gerät konfiguriert sind, anzuzeigen, geben Sie Folgendes ein:

```
show running-config admin snmp snmp-target-address
```

Falls Zieladressen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config admin snmp snmp-target-address | tab
                            TARGET          TRAP  SECURITY  USER   SECURITY
TARGET NAME          ENABLED  ADDRESS         PORT  MODEL     NAME   LEVEL
-------------------------------------------------------------------------------
127.0.0.1 v1         true     127.0.0.1       162   v1        oper   noAuthNoPriv
127.0.0.1 v2         true     127.0.0.1       162   v2c       oper   noAuthNoPriv
127.0.0.1 v3.guest   true     127.0.0.1       162   v3        admin  noAuthNoPriv
127.0.0.1 v3.inform  true     127.0.0.1       162   v3        admin  authPriv
127.0.0.1 v3.trap    true     127.0.0.1       162   v3        admin  authNoPriv
target               true     192.168.0.111   162   v2c       admin  noAuthNoPriv

 !
!
```

Falls keine SNMP-Zieladressen konfiguriert wurden, fügen Sie je nach Bedarf Zieladressen hinzu. Weitere Informationen finden Sie unter Abschnitt 14.2.6.2, „Eine SNMP-Zieladresse hinzufügen“.

Abschnitt 14.2.6.2

Eine SNMP-Zieladresse hinzufügen

Um eine SNMP-Zieladresse hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***admin » snmp » snmp-target-address*** und konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
{ target-name }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 32 Zeichen Aussagekräftiger Name für das Ziel (d. h. 'Corportate NMS').
enabled	**Zusammenfassung:** { true, false } **Standard:** true Aktiviert/deaktiviert dieses spezifische Ziel.
target-address { target-address }	**Zusammenfassung:** Eine Zeichenkette Eine IPv4- oder IPv6-Adresse für das entfernte Ziel. Dieser Parameter ist obligatorisch.
trap-port { trap-port }	**Zusammenfassung:** Eine vorzeichenlose 16-Bit-Ganzzahl zwischen 0 und 65535 **Standard:** 162 Der UDP-Port, an dem das entfernte Ziel Traps empfangen soll.
security-model { security-model }	**Zusammenfassung:** { v1, v2c, v3 } **Standard:** v2c Das SNMP-Sicherheitsmodell, dass verwendet werden soll: SNMPv1, SNMPv2c oder USM/ SNMPv3.
user-name { user-name }	**Zusammenfassung:** Eine Zeichenkette Der Benutzername, der für die Kommunikation mit diesem Ziel zu verwenden ist. Dieser Parameter ist obligatorisch.
security-level { security-level }	**Zusammenfassung:** { noAuthNoPriv, authNoPriv, authPriv } **Standard:** noAuthNoPriv Das SNMP-Security-Level: • authPriv: Kommunikation mit Authentifikation und Datenschutz. • authNoPriv: Kommunikation mit Authentifikation und ohne Datenschutz. • noAuthnoPriv: Kommunikation ohne Authentifikation und Datenschutz.
control-community { control-community }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 32 Zeichen Beschränkt eingehende SNMP-Anfragen von der IPv4- oder IPv6-Adresse, die zu dieser Community gehört.
tag-list { tag-list }	**Zusammenfassung:** { snmpv1_trap, snmpv2_trap, snmpv2_inform, snmpv3_trap, snmpv3_inform } **Standard:** snmpv2_trap Wählt die Art der Trap-Kommunikation aus, die an dieses Ziel gesendet wird. **HINWEIS** *Mehrere Optionen können gewählt werden.*
inform-timeout { inform-timeout }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 0 und 2147483647 **Standard:** 6000 Das Timeout für zuverlässige Informationsübertragungen (Sekunden*100).

Parameter	Beschreibung
inform-retries { inform-retries }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 0 und 255 **Standard:** 3 Die Anzahl an Versuchen für zuverlässige Informationsübertragungen.
target-engine-id { target-engine-id }	**Zusammenfassung:** Eine Zeichenkette Die lokale SNMP Engine-ID des Ziels. Dieses Feld kann leer gelassen werden.

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 14.2.6.3
Eine SNMP-Zieladresse löschen

Um eine SNMP-Zieladresse zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die SNMP-Zieladresse durch Eingabe von:

```
no admin snmp snmp-target-address target-name
```

Erläuterung:

- *`target-name`* ist ein aussagekräftiger Name für das Ziel (z. B. *Corporate NMS*)

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 14.2.7
SNMP-Benutzer verwalten

Dieser Abschnitt beschreibt, wie Sie SNMP-Benutzer verwalten können.

INHALT

- Abschnitt 14.2.7.1, „Eine Liste der SNMP-Benutzer anzeigen“
- Abschnitt 14.2.7.2, „Hinzufügen eines SNMP-Benutzers“
- Abschnitt 14.2.7.3, „Einen SNMP-Benutzer löschen“

Abschnitt 14.2.7.1
Eine Liste der SNMP-Benutzer anzeigen

Um eine Liste der im Gerät konfigurierten SNMP-Benutzer anzusehen, geben Sie Folgendes ein:

```
show running-config admin snmp snmp-user
```

Falls Benutzer konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config admin snmp snmp-user | tab
                                 USER    AUTH
USER ENGINE ID                   NAME    PROTOCOL  AUTH KEY
```

```
--------------------------------------------------------------------------------
80:00:3a:9c:03:00:0a:dc:ff:9a:00  oper   sha1      $4$kNxlPIYMx2xJhYYI0d4IDw==
80:00:3a:9c:03:00:0a:dc:ff:9a:00  admin  none      -
80:00:3a:9c:03:00:0a:dc:ff:9a:00  guest  md5       $4$kNxlPIYMx2xJhYYI0d4IDw==

 !
!
```

Falls keine SNMP-Benutzer konfiguriert wurden, fügen Sie nach Bedarf Benutzer hinzu. Weitere Informationen finden Sie unter Abschnitt 14.2.7.2, „Hinzufügen eines SNMP-Benutzers“.

Abschnitt 14.2.7.2

Hinzufügen eines SNMP-Benutzers

Um einen SNMP-Benutzer hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den SNMP-Benutzer hinzu, indem Sie Folgendes eingeben:

   ```
   admin snmp snmp-user id name
   ```

   Erläuterung:

   - *id* ist die ID für den Benutzer
   - *name* ist die Bezeichnung des Benutzers

   ACHTUNG!
   Sicherheitsgefahr – Risiko des unbefugten Zugriffs und/oder Missbrauchs. Verwenden Sie bei der Konfiguration von SNMP-Benutzern ausschließlich starke Passwörter mit mindestens:

   - *Einem Kleinbuchstaben*
   - *Einem Großbuchstaben*
   - *Einer Ziffer*
   - *Einem Sonderzeichen (z. B. !@#$%^&*()_+-={}[];:',<.>/?\|`~)*

   *Vermeiden Sie schwache Passwörter (z. B. **password1**, **123456789**, **abcdefgh**) oder sich wiederholende Zeichen (z. B. **abcabc**).*

3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
{ user-engine-id }	**Zusammenfassung:** Eine Zeichenkette Die verwaltungstechnisch eindeutige Kennung für den SNMP Engine, ein Wert im Format nn:nn:nn:nn:nn:...:nn, wobei nn eine 2-stellige Hexadezimalzahl ist. Die minimale Länge sind 5 Oktetts. Die maximale Länge sind 32 Oktetts. Jedes Oktett ist durch einen Doppelpunkt (:) zu trennen.
{ user-name }	**Zusammenfassung:** Eine Zeichenkette Der Benutzer für den SNMP-Schlüssel. Einen Benutzernamen aus der Liste auswählen.
auth-protocol { auth-protocol }	**Zusammenfassung:** { none, md5, sha1 } **Standard:** none Das Authentifizierungsprotokoll, das beim SNMP-Austausch zwischen Benutzer und SNMP Engine für Datenintegrität und Authentifizierung sorgt.
auth-key { auth-key }	**Zusammenfassung:** Eine Zeichenkette

Parameter	Beschreibung
	Die Passphrase zur Authentifizierung. Die Passphrase muss mindestens 8 Zeichen lang sein.
privacy-protocol { privacy-protocol }	**Zusammenfassung:** { none, des3cbc, aescfb128 } **Standard:** none Das Symmetric Privacy Protocol, das beim SNMP-Austausch zwischen Benutzer und SNMP Engine für Datenver- und entschlüsselung sorgt.
privacy-key { privacy-key }	**Zusammenfassung:** Eine Zeichenkette Die Datenschutz-Passphrase Die Passphrase muss mindestens 8 Zeichen lang sein.

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 14.2.7.3
Einen SNMP-Benutzer löschen

Um einen SNMP-Benutzer zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den SNMP-Benutzer durch Eingabe von:

```
no admin snmp snmp-user id name
```

   Erläuterung:

   - *`id`* ist die ID für den Benutzer
   - *`name`* ist der Name des Benutzers

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 14.2.8
Zuordnung des SNMP-Sicherheitsmodells verwalten

Dieser Abschnitt beschreibt, wie Sie die Zuordnung von SNMP-Sicherheitsmodellen verwalten können.

INHALT

- Abschnitt 14.2.8.1, „Eine Liste der SNMP-Sicherheitsmodelle anzeigen“
- Abschnitt 14.2.8.2, „Hinzufügen eines SNMP-Sicherheitsmodells“
- Abschnitt 14.2.8.3, „Ein SNMP-Sicherheitsmodell löschen“

Abschnitt 14.2.8.1
Eine Liste der SNMP-Sicherheitsmodelle anzeigen

Um eine Liste der im Gerät konfigurierten SNMP-Sicherheitsmodelle anzusehen, geben Sie Folgendes ein:

```
show running-config admin snmp snmp-security-to-group
```

Falls Zieladressen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config admin snmp snmp-security-to-group | tab
SECURITY  USER
MODEL     NAME   GROUP
----------------------------
v1        oper   all-rights
v1        guest  all-rights
v2c       oper   all-rights
v2c       admin  testgroup
v2c       guest  all-rights
v3        admin  initial

 !
!
```

Falls keine SNMP-Sicherheitsmodelle konfiguriert wurden, fügen Sie je nach Bedarf Sicherheitsmodelle hinzu. Weitere Informationen finden Sie unter Abschnitt 14.2.8.2, „Hinzufügen eines SNMP-Sicherheitsmodells“.

Abschnitt 14.2.8.2
Hinzufügen eines SNMP-Sicherheitsmodells

Um ein SNMP-Sicherheitsmodell hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie das SNMP-Sicherheitsmodell hinzu, indem Sie Folgendes eingeben:

   ```
   admin snmp snmp-security-to-group model name { group | group }
   ```

   Erläuterung:

   - *model* ist das Sicherheitsmodell. Optionen sind u.a. `range`, `v1`, `v2c` und `v3`.
   - *name* ist die Bezeichnung des zugehörigen Benutzerprofils. Optionen sind u.a. `admin`, `guest` und `oper`.
   - *group* ist die Bezeichnung der zugehörigen SNMP-Gruppe. Wenn keine Gruppe definiert ist, dann werden dem Benutzer standardmäßig alle Zugriffsrechte gewährt.
3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 14.2.8.3
Ein SNMP-Sicherheitsmodell löschen

Um ein SNMP-Sicherheitsmodell zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie das SNMP-Sicherheitsmodell, indem Sie Folgendes eingeben:

   ```
   no admin snmp snmp-security-to-group model name
   ```

   Erläuterung:

   - *model* ist das Sicherheitsmodell
   - *name* ist die Bezeichnung des zugehörigen Benutzerprofils
3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 14.2.9
SNMP-Gruppenzugang verwalten

Dieser Abschnitt beschreibt, wie Sie den Zugang für SNMP-Gruppen verwalten können.

INHALT

- Abschnitt 14.2.9.1, „Eine Liste der SNMP-Gruppen anzeigen“
- Abschnitt 14.2.9.2, „Hinzufügen einer SNMP-Gruppe“
- Abschnitt 14.2.9.3, „Eine SNMP-Gruppe löschen“

Abschnitt 14.2.9.1
Eine Liste der SNMP-Gruppen anzeigen

Um eine Liste der SNMP-Gruppen, die auf einem Gerät konfiguriert sind, anzuzeigen, geben Sie Folgendes ein:

```
show running-config admin snmp snmp-access
```

Falls SMNP-Gruppen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config admin snmp snmp-access | tab
            SECURITY  SECURITY      READ VIEW   WRITE VIEW  NOTIFY
GROUP       MODEL     LEVEL         NAME        NAME        VIEW NAME
-------------------------------------------------------------------------
initial     any       noAuthNoPriv  all-of-mib  all-of-mib  all-of-mib
initial     any       authNoPriv    all-of-mib  all-of-mib  all-of-mib
initial     any       authPriv      all-of-mib  all-of-mib  all-of-mib
testgroup   v2c       noAuthNoPriv  all-of-mib  all-of-mib  all-of-mib
all-rights  any       noAuthNoPriv  all-of-mib  all-of-mib  all-of-mib

 !
!
```

Falls keine Gruppen konfiguriert wurden, fügen Sie je nach Bedarf Gruppen hinzu. Weitere Informationen finden Sie unter Abschnitt 14.2.9.2, „Hinzufügen einer SNMP-Gruppe“.

Abschnitt 14.2.9.2
Hinzufügen einer SNMP-Gruppe

Um eine SNMP-Gruppe hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie die SNMP-Gruppe hinzu, indem Sie Folgendes eingeben:

   ```
   admin snmp snmp-access group model level
   ```

   Erläuterung:

   - *group* ist die Bezeichnung der Gruppe
   - *model* ist das Sicherheitsmodell für die Gruppe. Optionen sind u.a.: any, v1, v2coder v3.
   - *level* ist die Sicherheitsstufe für die Gruppe. Optionen sind u.a.:
     - authPriv – Kommunikation mit Authentifizierung und Datenschutz.
     - authNoPriv – Kommunikation mit Authentifizierung und ohne Datenschutz.

- `noAuthnoPriv` – Kommunikation ohne Authentifizierung und Datenschutz.

3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
read-view-name { read-view-name }	**Zusammenfassung:** { no-view, v1-mib, restricted, all-of-mib } **Standard:** all-of-mib Der Name der Leseansicht, auf die die SNMP-Gruppe Zugriff hat: all-of-mib, restricted, v1-mib oder no-view.
write-view-name { write-view-name }	**Zusammenfassung:** { no-view, v1-mib, restricted, all-of-mib } **Standard:** all-of-mib Der Name der Schreibansicht, auf die die SNMP-Gruppe Zugriff hat: all-of-mib, restricted, v1-mib oder no-view.
notify-view-name { notify-view-name }	**Zusammenfassung:** { no-view, v1-mib, restricted, all-of-mib } **Standard:** all-of-mib Der Name der Benachrichtigungsansicht, auf die die SNMP-Gruppe Zugriff hat: all-of-mib, restricted, v1-mib oder no-view.

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 14.2.9.3
Eine SNMP-Gruppe löschen

Um eine SNMP-Gruppe zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die SNMP-Gruppe, indem Sie Folgendes eingeben:

```
no admin snmp snmp-access group model level
```

Erläuterung:

- *`group`* ist die Bezeichnung der Gruppe
- *`model`* ist das Sicherheitsmodell für die Gruppe
- *`level`* ist die Sicherheitsstufe für die Gruppe

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 14.3
NETCONF verwalten

NETCONF (Network Configuration Protocol) ist ein Netzwerkkonfigurationsprotokoll, das von der Internet Engineering Task Force (IETF) entwickelt wurde. NETCONF stellt Funktionen zum Herunterladen, Hochladen, Ändern und Löschen der Konfigurationsdaten in Netzwerkgeräten bereit. RUGGEDCOM ROX II-Geräte unterstützen auch die Datenerfassung und direkte Aktionen im Gerät wie zum Beispiel Neubooten des Geräts, Löschen von Statistiken und Neustarten von Diensten.

HINWEIS
Weitere Informationen über NETCONF und seine Verwendung enthält der NETCONF Reference Guide für RUGGEDCOM ROX II v2.11 .

INHALT

- Abschnitt 14.3.1, „Aktivieren und Konfigurieren von NETCONF-Sitzungen“
- Abschnitt 14.3.2, „NETCONF-Statistiken anzeigen“

Abschnitt 14.3.1

Aktivieren und Konfigurieren von NETCONF-Sitzungen

Um NETCONF-Sitzungen zu aktivieren und zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.

ACHTUNG!
Sicherheitsgefahr – Risiko des unbefugten Zugriffs/Missbrauchs. Konfigurieren Sie einen Idle-Timeout-Zeitraum für NETCONF zur Vermeidung eines unbefugten Zugriffs (z. B. ein Benutzer verlässt seinen Arbeitsplatz, ohne diesen zu schützen) bzw. einer Zugriffsverweigerung (z. B. ein Gastbenutzer sperrt einen Admin-Benutzer durch Öffnen der maximalen Anzahl an NETCONF-Sitzungen).

WICHTIG!
Stellen Sie vor der Konfiguration eines Idle Timeouts auf einem vom RUGGEDCOM NMS verwalteten Gerät sicher, dass NMS so konfiguriert ist, dass es einen Timeout-Zeitraum für NETCONF-Sitzungen unterstützt.

2. Navigieren Sie zu ***admin » netconf*** und konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
enabled	**Zusammenfassung:** { true, false } **Standard:** true Ermöglicht es, NETCONF-Funktionen am Gerät zu konfigurieren.
listen-ip { listen-ip }	**Zusammenfassung:** Eine Zeichenkette **Standard:** 0.0.0.0 Die IP-Adresse, an der die CLI NETCONF-Anfragen empfängt.
port { port }	**Zusammenfassung:** Eine vorzeichenlose 16-Bit-Ganzzahl zwischen 0 und 65535 **Standard:** 830 Der Port, an dem NETCONF NETCONF-Anfragen empfängt.
extra-ip-ports { extra-ip-ports }	**Zusammenfassung:** Eine Zeichenkette Zusätzliche IP-Adressen und Ports, an denen NETCONF NETCONF-Anfragen empfängt. Sie können IP-Adressen und Ports in den folgenden Formaten festlegen: • nnn.nnn.nnn.nnn:port steht für eine IPv4-Adresse, gefolgt von einem Doppelpunkt und der Portnummer. 192.168.10.12:19343 • 0.0.0.0 beispielsweise steht für die voreingestellte IPv4-Adresse und die voreingestellte Portnummer. Dies ist die Standardkonfiguration. • [::]:port steht für eine IPv6-Adresse, gefolgt von einem Doppelpunkt und der Portnummer. Zum Beispiel, [fe80::5eff:35ff]:16000

Parameter	Beschreibung
	• Bei Verwendung der Standardadresse legen Sie keine empfangende Adresse mit dem gleichen Port fest.
max-sessions { max-sessions }	**Zusammenfassung:** eine vorzeichenlose 32-Bit-Ganzzahl **Standard:** 10 Die maximale Anzahl gleichzeitiger NETCONF-Sitzungen.
idle-timeout { idle-timeout }	**Zusammenfassung:** Eine Zeichenkette **Standard:** PT0S Das maximale Zeitintervall des betriebsfreien Zustands, bevor eine NETCONF-Sitzung beendet wird. Wartet die Sitzung auf Meldungen oder steht ein bestätigtes Commit aus, wird kein Timeout für das Zeitintervall des betriebsfreien Zustands verwendet. Ein Wert von 0 bedeutet, dass kein Timeout erfolgt.

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.
4. [Optional] Aktivieren Sie das NETCONF-Summary-Protokoll (gespeichert unter `/var/log/netconf.log`) um alle NETCONF-Protokolltransaktionen aufzuzeichnen. Weitere Informationen finden Sie unter Abschnitt 4.13.4.3, „Aktivieren/Deaktivieren des NETCONF-Summary-Protokolls“.
5. [Optional] Aktivieren Sie das NETCONF-Trace-Protokoll (gespeichert unter `/var/log/netconf-trace.log`) um den Text jeder vom Gerät empfangenen und gesendeten NETCONF XML-Meldung aufzuzeichnen. Weitere Informationen finden Sie unter Abschnitt 4.13.4.4, „Aktivieren/Deaktivieren des NETCONF-Trace-Protokolls“.

Abschnitt 14.3.2

NETCONF-Statistiken anzeigen

Um NETCONF-bezogene Statistiken anzusehen, geben Sie Folgendes ein:

```
show admin netconf
```

Eine Tabelle oder Liste ähnlich dem folgenden Beispiel wird angezeigt:

```
ruggedcom# show admin netconf
netconf
 statistics
  in bad hellos     0
  in sessions       0
  dropped sessions  0
  in rpcs           0
  in bad rpcs       0
  out rpc errors    0
  out notifications 0
```

Dieses Diese Tabelle oder Liste liefert die folgenden Informationen:

Parameter	Beschreibung
in-bad-hellos	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Gesamtzahl an Sitzungen, die gelöscht wurden, da eine ungültige 'hello'-Nachricht empfangen wurde. Dazu zählen 'hello'-Nachrichten mit einem 'session-id'-Attribut, ungeeignetem Namensraum und ungeeigneten Kapazitätsangaben. Dieser Parameter ist obligatorisch.
in-sessions	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl

Parameter	Beschreibung
	Die Gesamtzahl der NETCONF-Sitzungen, die zum NETCONF-Peer gestartet wurden. inSessions - inBadHellos = 'The number of correctly started NETCONF sessions.' (Die Anzahl korrekt gestarteter NETCONF-Sitzungen) Dieser Parameter ist obligatorisch.
dropped-sessions	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Gesamtzahl der verworfenen NETCONF-Sitzungen. inSessions - inBadHellos = 'The number of correctly started NETCONF sessions.' Dieser Parameter ist obligatorisch.
in-rpcs	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Gesamtzahl der empfangenen RPC-Anfragen. Dieser Parameter ist obligatorisch.
in-bad-rpcs	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Gesamtzahl der RPCs, die korrekt geparst wurden, aber nicht bedient werden konnten, da sie ungültige XML enthielten. Dieser Parameter ist obligatorisch.
out-rpc-errors	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Gesamtzahl der 'rpc-reply'-Nachrichten mit gesendetem 'rpc-error'. Dieser Parameter ist obligatorisch.
out-notifications	**Zusammenfassung:** Eine vorzeichenlose 32-Bit-Ganzzahl Die Gesamtzahl der gesendeten 'notification'-Nachrichten. Dieser Parameter ist obligatorisch.

15 Verkehrssteuerung und -klassifizierung

Mit den Teilsystemen für Verkehrssteuerung und -klassifizierung können Sie den Datenpaketfluss zu angeschalteten Netzwerkschnittstellen kontrollieren.

INHALT

- Abschnitt 15.1, „Verwalten der Port-Spiegelung“
- Abschnitt 15.2, „Verkehrssteuerung verwalten“
- Abschnitt 15.3, „Verwalten von Berechtigungsklassen“

Abschnitt 15.1

Verwalten der Port-Spiegelung

Die Port-Spiegelung ist ein Tool für die Fehlerbehebung, das den gesamten Verkehr kopiert bzw. spiegelt, der an einem bestimmten Port zu einem anderen Mirror-Port empfangen oder übertragen wurde. Wenn ein Protokollanalysegerät an den Zielport angeschlossen ist, wird der Verkehrsstrom gültiger Frames an einem beliebigen Quellport zu Analysezwecken zur Verfügung gestellt.

Wählen Sie einen Zielport, der eine höhere Geschwindigkeit als der Quellport hat. Die Spiegelung eines 100-MBit/s-Ports auf einen 10-MBit/s-Port führt möglicherweise zu einem nicht ordnungsgemäß gespiegelten Strom.

Frames werden verworfen, wenn die Vollduplexrate der Frames am Quellport die Übertragungsrate des Zielports überschreitet. Da sowohl übertragene als auch empfangene Frames am Quellport auf den Zielport gespiegelt werden, werden Frames verworfen, falls der Verkehr die Übertragungsrate des Zielports überschreitet. Dieses Problem erreicht sein Extrem, wenn Verkehr an einem 100 MBit/s-Vollduplexport auf einen 10 MBit/s-Halbduplexport gespiegelt wird.

Auf dem Quellport empfangene ungültige Frames werden nicht gespiegelt. Hierzu zählen u.a. CRC-Fehler, über- und unterdimensionierte Pakete, Fragmente, Jabbers, Collisions, Late Collisions und verworfene Ereignisse).

HINWEIS

Die Port-Spiegelung unterliegt den folgenden Einschränkungen:

- *Gelegentlich kann der Zielport fälschlicherweise das markierte (getaggte) oder nicht markierte (nicht getaggte) VLAN-Format der gespiegelten Frames anzeigen.*
- *Netzwerk-Management-Frames (z. B. RSTP, GVRP usw.) können nicht gespiegelt werden.*
- *Vom Switch generierte Switch-Management-Frames (z. B. Telnet, HTTP, SNMP usw.) können nicht gespiegelt werden.*

INHALT

- Abschnitt 15.1.1, „Port-Spiegelung konfigurieren“

- Abschnitt 15.1.2, „Ausgehende Quellports verwalten“
- Abschnitt 15.1.3, „Eingehende (ingress) Quellports verwalten“

Abschnitt 15.1.1
Port-Spiegelung konfigurieren

Um die Port-Spiegelung zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***switch » port-mirroring***.
3. Konfigurieren Sie die Port-Spiegelung für einen bestimmten Port, indem Sie Folgendes eingeben:

   ```
   switch port-mirroring enabled target-slot swport target-port port egress-src egress ingress-src ingress
   ```

   Erläuterung:

   - *port* ist die Nummer des Ports (oder eine Liste von Ports, wenn sie in einem Port-Trunk gebündelt sind)
   - *egress* ist die Nummer des abgehenden Ports
   - *ingress* ist die Nummer des eingehenden Ports
4. Fügen Sie ausgehende (egress) und eingehende (ingress) Quellports hinzu. Für weitere Informationen siehe Abschnitt 15.1.2.2, „Einen ausgehenden (egress) Quellport hinzufügen“ und Abschnitt 15.1.3.2, „Einen eingehenden (ingress) Quellport hinzufügen“.
5. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 15.1.2
Ausgehende Quellports verwalten

Dieser Abschnitt beschreibt, wie Sie ausgehende Quellports für die Port-Spiegelung konfigurieren und verwalten können.

INHALT

- Abschnitt 15.1.2.1, „Eine Liste ausgehender (egress) Quellports anzeigen“
- Abschnitt 15.1.2.2, „Einen ausgehenden (egress) Quellport hinzufügen“
- Abschnitt 15.1.2.3, „Einen ausgehenden (egress) Quellport löschen“

Abschnitt 15.1.2.1
Eine Liste ausgehender (egress) Quellports anzeigen

Um eine Liste der ausgehenden (egress) Quellports für die Port-Spiegelung anzusehen, geben Sie Folgendes ein:

```
show running-config switch port-mirroring egress-src
```

Falls ausgehende (egress) Quellports konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config switch port-mirroring egress-src
switch port-mirroring
 egress-src swport 1
 !
!
```

Falls keine ausgehenden (egress) Quellports konfiguriert wurden, fügen Sie je nach Bedarf ausgehende Ports hinzu. Weitere Informationen finden Sie unter Abschnitt 15.1.2.2, „Einen ausgehenden (egress) Quellport hinzufügen“.

Abschnitt 15.1.2.2

Einen ausgehenden (egress) Quellport hinzufügen

Um einen ausgehenden (egress) Quellport zur Port-Spiegelung hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den ausgehenden (egress) Quellport hinzu, indem Sie Folgendes eingeben:

   ```
   switch port-mirroring egress-src swport port
   ```

   Erläuterung:

   - *port* ist die Nummer des Ports (oder eine Liste von Ports, wenn sie in einem Port-Trunk gebündelt sind) für das Modul.
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 15.1.2.3

Einen ausgehenden (egress) Quellport löschen

Um einen ausgehenden (egress) Quellport zur Port-Spiegelung zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die Adresse, indem Sie Folgendes eingeben:

   ```
   no switch port-mirroring egress-src swport port
   ```

   Erläuterung:

   - *port* ist die Nummer des Ports (oder eine Liste von Ports, wenn sie in einem Port-Trunk gebündelt sind) für das Modul.
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 15.1.3
Eingehende (ingress) Quellports verwalten

Dieser Abschnitt beschreibt, wie Sie ausgehende Quellports für die Port-Spiegelung konfigurieren und verwalten können.

INHALT

- Abschnitt 15.1.3.1, „Eine Liste der eingehenden (ingress) Quellports anzeigen“
- Abschnitt 15.1.3.2, „Einen eingehenden (ingress) Quellport hinzufügen“
- Abschnitt 15.1.3.3, „Einen eingehenden (ingress) Quellport löschen“

Abschnitt 15.1.3.1
Eine Liste der eingehenden (ingress) Quellports anzeigen

Um eine Liste der eingehenden Quellports für die Port-Spiegelung anzusehen, geben Sie Folgendes ein:

```
show running-config switch port-mirroring ingress-src
```

Falls eingehende Quellports konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config switch port-mirroring ingress-src
switch port-mirroring
 ingress-src swport 1
 !
!
```

Falls keine eingehenden Quellports konfiguriert wurden, fügen Sie je nach Bedarf Ports hinzu. Weitere Informationen finden Sie unter Abschnitt 15.1.3.2, „Einen eingehenden (ingress) Quellport hinzufügen“.

Abschnitt 15.1.3.2
Einen eingehenden (ingress) Quellport hinzufügen

Um einen eingehenden (ingress) Quellport zur Port-Spiegelung hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den eingehenden (ingress) Quellport hinzu, indem Sie Folgendes eingeben:

   ```
   switch port-mirroring ingress-src swport port
   ```

   Erläuterung:

   - *port* ist die Nummer des Ports (oder eine Liste von Ports, wenn sie in einem Port-Trunk gebündelt sind) für das Modul.
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 15.1.3.3

Einen eingehenden (ingress) Quellport löschen

Um einen eingehenden (ingress) Quellport zur Port-Spiegelung zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die Adresse, indem Sie Folgendes eingeben:

   ```
   no switch port-mirroring ingress-src swport port
   ```

   Erläuterung:

   - *port* ist die Nummer des Ports (oder eine Liste von Ports, wenn sie in einem Port-Trunk gebündelt sind) für das Modul.
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 15.2

Verkehrssteuerung verwalten

Verkehrssteuerung ist ein Firewall-Subsystem, das die Menge an Bandbreite für jede Netzwerkschnittstelle verwaltet, die verschiedene Arten von Datenverkehr nutzen dürfen. Damit eine Verkehrssteuerungskonfiguration funktioniert, muss eine Firewall konfiguriert werden.

HINWEIS
Weitere Informationen über Firewalls finden Sie unter Abschnitt 6.7, „Verwalten von Firewalls“.

RUGGEDCOM ROX II ermöglicht bis zu 4 verschiedene Firewall-Konfigurationen, so dass Benutzer schnell zwischen den Konfigurationen wechseln können. Die Benutzer können schnell verschiedene Konfigurationen bewerten, ohne dass ein Teil der Konfiguration gespeichert und neu geladen werden muss. Im Gegensatz dazu gibt es nur eine Verkehrssteuerungskonfiguration. Eine Verkehrssteuerungskonfiguration wird, sofern aktiviert, mit der aktuellen Firewall-Konfiguration verwendet. Eine aktuelle Firewall-Konfiguration ist als eine Konfiguration festgelegt, die entweder in work-config und/oder active-config angegeben wird. Sie muss zur Validierung nicht aktiviert werden.

HINWEIS
Wenn die Layer-3-Hardwarebeschleunigung aktiviert ist, ist die Verkehrssteuerung für Ethernet-Datenverkehr auf keinem Line-Modul verfügbar. Sie ist nur für den Einsatz an WAN-Schnittstellen vorgesehen.

INHALT

- Abschnitt 15.2.1, „Aktivieren und Konfigurieren der Verkehrssteuerung“
- Abschnitt 15.2.2, „Verkehrssteuerungsschnittstellen verwalten“
- Abschnitt 15.2.3, „Verkehrssteuerungsprioritäten verwalten“
- Abschnitt 15.2.4, „Verkehrssteuerungsklassen verwalten“
- Abschnitt 15.2.5, „Verkehrssteuerungsgeräte verwalten“
- Abschnitt 15.2.6, „Verkehrssteuerungsregeln verwalten“
- Abschnitt 15.2.7, „QoS-Mapping für VLANs verwalten“

- Abschnitt 15.2.8, „Egress-Marker für QoS-Maps verwalten“
- Abschnitt 15.2.9, „QoS-Statistiken anzeigen“

Abschnitt 15.2.1

Aktivieren und Konfigurieren der Verkehrssteuerung

Die Verkehrssteuerungs-Funktionen werden in zwei Modi unterteilt:

- **Basic-Modus**
  Im Basic-Modus ist ein begrenzter Satz von Optionen und Parametern verfügbar. Verwenden Sie diesen Modus, um die ausgehende Bandbreite für eine Schnittstelle, die Schnittstellenpriorität (hoch, mittel oder niedrig) und bestimmte einfache Merkmale der Verkehrssteuerung einzustellen. Das grundlegende Traffic Shaping wirkt sich auf Verkehr aus, der anhand von Protokoll, Portnummer, Adresse und Schnittstelle identifiziert wurde. Beachten Sie, dass einige dieser Optionen sich gegenseitig ausschließen. Beachten Sie die Angaben zu den einzelnen Optionen.

  Im Basic-Modus wird ein Paket basierend auf dem Inhalt seines Felds "Type of Service (ToS)" kategorisiert, wenn es mit keiner der definierten Klassen übereinstimmt.

- **Advanced-Modus**
  Im Advanced-Modus wird jeder zu verwaltenden Schnittstelle eine Gesamtbandbreite für eingehenden und ausgehenden Datenverkehr zugewiesen. Anschließend werden die Klassen für jede Schnittstelle definiert, jede mit einer eigenen minimal zugesicherten Bandbreite und einer maximal zulässigen Bandbreite. Das kombinierte Minimum der Klassen an einer Schnittstelle darf nicht mehr sein als die ausgehende Gesamtbandbreite, die für die Schnittstelle festgelegt ist. Jeder Klasse wird eine Priorität zugewiesen, und Bandbreite, die übrig ist, nachdem jede Klasse eine Mindestzuweisung (bei Bedarf) erhalten hat, wird der niedrigsten Prioritätsklasse zugewiesen, bis die maximale Bandbreite erreicht ist. Danach wird der nächsten Priorität mehr Bandbreite zugewiesen. Wenn die angegebene Gesamtbandbreite für die Schnittstelle erreicht ist, werden keine weiteren Pakete gesendet, und weitere Pakete werden möglicherweise verworfen, wenn die Schnittstellen-Warteschlangen voll sind.

  Pakete werden Klassen an der ausgehenden Schnittstelle zugewiesen. Diese Zuweisung basiert entweder auf einer dem Paket zugewiesenen Kennzeichnung oder auf dem Feld "Type of Service (ToS)" im IP-Header. Wenn das ToS-Feld mit einer definierten Klasse übereinstimmt, wird das Paket dieser Klasse zugeordnet. Andernfalls wird es einer beliebigen Klasse zugeordnet, die mit der dem Paket zugewiesenen Kennzeichnung übereinstimmt. Falls keine Klasse mit der Kennzeichnung übereinstimmt, wird das Paket der Standardklasse zugewiesen.

  Kennzeichnungen werden Paketen durch Verkehrssteuerungsregeln zugewiesen, die auf zahlreichen Parametern (z. B. IP-Adresse, Portnummer, Protokoll, Paketlänge usw.) basieren.

Ein gleichzeitiger Zugriff auf beide Modi ist nicht möglich. Es kann nur auf den aktuell konfigurierten Modus zugegriffen werden.

Um die Verkehrssteuerung zu aktivieren und zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
enabled	Aktiviert/deaktiviert die Verkehrssteuerung (TC, en: Traffic Control) für die aktuelle Firewall-Konfiguration. Festgeschrieben wird die aktuelle Firewall-Konfiguration. Wenn eine aktive Konfiguration in das System übertragen wird, wird eine **aktivierte** TC-Konfiguration hinzugefügt. Wenn eine Arbeitskonfiguration übertragen wird, wird die **aktivierte** TC-Konfiguration in die Arbeitskonfiguration aufgenommen. **Eine TC-Konfiguration benötigt eine Firewall-Konfiguration, um zu funktionieren**.

Parameter	Beschreibung
mode-choice { mode-choice }	**Zusammenfassung:** { basic, advanced } **Standard:** basic Wählen Sie als Konfigurationsmodus entweder 'simple' oder 'advanced'. Klicken Sie nach Ihrer Wahl erneut auf "traffic-control".

3. Wenn der Basic-Modus aktiviert ist, gehen Sie wie folgt vor:
   a. Fügen Sie Verkehrssteuerungs-Schnittstellen hinzu. Weitere Informationen finden Sie unter Abschnitt 15.2.2.2, „Eine Verkehrssteuerungsschnittstelle hinzufügen“.
   b. Fügen Sie Verkehrssteuerungs-Prioritäten hinzu. Weitere Informationen finden Sie unter Abschnitt 15.2.3.2, „Eine Verkehrssteuerungspriorität hinzufügen“.
4. Wenn der Advanced-Modus aktiviert ist, gehen Sie wie folgt vor:
   a. Fügen Sie Verkehrssteuerungs-Klassen hinzu. Weitere Informationen finden Sie unter Abschnitt 15.2.4.2, „Hinzufügen einer Verkehrssteuerungsklasse“.
   b. Fügen Sie Verkehrssteuerungs-Geräte hinzu. Weitere Informationen finden Sie unter Abschnitt 15.2.5.2, „Ein Verkehrssteuergerät hinzufügen“.
   c. Fügen Sie Verkehrssteuerungs-Regeln hinzu. Weitere Informationen finden Sie unter Abschnitt 15.2.6.2, „Hinzufügen einer Verkehrssteuerungsregel“.
5. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 15.2.2

Verkehrssteuerungsschnittstellen verwalten

Verkehrssteuerungsschnittstellen sind Schnittstellen für die Verkehrsformung, die hauptsächlich für ausgehende Bandbreite und ausgehende Geräte verwendet werden.

HINWEIS
Verkehrssteuerungsschnittstellen können nur im Basisbetrieb konfiguriert werden. Weitere Informationen über die Einstellung der Verkehrssteuerung finden Sie unter Abschnitt 15.2.1, „Aktivieren und Konfigurieren der Verkehrssteuerung“.

INHALT

- Abschnitt 15.2.2.1, „Eine Liste der Verkehrssteuerungsschnittstellen anzeigen“
- Abschnitt 15.2.2.2, „Eine Verkehrssteuerungsschnittstelle hinzufügen“
- Abschnitt 15.2.2.3, „Eine Verkehrssteuerungsschnittstelle löschen“

Abschnitt 15.2.2.1

Eine Liste der Verkehrssteuerungsschnittstellen anzeigen

Um eine Liste der Verkehrssteuerungsschnittstellen anzusehen, geben Sie Folgendes ein:

```
show running-config qos traffic-control basic-configuration tcinterfaces
```

Falls Schnittstellen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config qos traffic-control basic-configuration tcinterfaces
qos
 traffic-control
  basic-configuration
   tcinterfaces te1-2-1c01ppp
    type         external
    inbandwidth  1500
    in-unit      kilobits
    outbandwidth 1500
    out-unit     kilobits
    description  "TC on T1 Link"
   !
  !
 !
!
```

Falls keine Schnittstellen konfiguriert wurden, fügen Sie je nach Bedarf Schnittstellen hinzu. Weitere Informationen finden Sie unter Abschnitt 15.2.2.2, „Eine Verkehrssteuerungsschnittstelle hinzufügen“.

Abschnitt 15.2.2.2

Eine Verkehrssteuerungsschnittstelle hinzufügen

Um eine neue Verkehrssteuerungsschnittstelle hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie die Schnittstelle hinzu, indem Sie Folgendes eingeben:

   ```
   qos traffic-control basic-configuration tcinterfaces interface
   ```

   Erläuterung:

   - *interface* ist die Bezeichnung der Verkehrssteuerungsschnittstelle
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
{ interface }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 15 Zeichen Eine Schnittstelle, für die Verkehrsformung gilt. Alphanumerische Kleinbuchstaben sowie die Zeichen '.' und '-' sind zulässig.
iptype { iptype }	**Zusammenfassung:** { ipv4, ipv6, ipv4ipv6 } **Standard:** ipv4 Typ des Internetprotokolls - beide verwenden, wenn keine Adressen eingesetzt sind, ansonsten IPv4- und IPv6-Regeln für jede Art von verwendeten Adressen definieren.
type { type }	**Zusammenfassung:** { internal, external, none } **Standard:** none (optional) 'external' (in Richtung Internet) oder 'internal' (in Richtung eines lokalen Netzwerks). 'external' sorgt dafür, dass der von jeder einzelnen IP-Quelladresse erzeugte Datenverkehr wie ein einziger Datenfluss behandelt wird. 'internal' sorgt dafür, dass der durch jede eindeutige IP-Zieladresse erzeugte Datenverkehr wie ein einziger Datenfluss behandelt wird. Interne Schnittstellen haben selten Vorteile von einfacher Verkehrsformung.
inbandwidth { inbandwidth }	**Zusammenfassung:** Eine vorzeichenlose 16-Bit-Ganzzahl (optional) Die eingehende Bandbreite dieser Schnittstelle. Wenn eingehender Datenverkehr die angegebene Rate überschreitet, werden empfangene Pakete nach Zufallsprinzip gelöscht. Wenn nichts festgelegt ist, wird von der Höchstgeschwindigkeit ausgegangen. Hier nur die Nummer spezifizieren. Die Einheit (Kilobits, Megabits) wird in der "in-unit" festgelegt.

Parameter	Beschreibung
in-unit { in-unit }	**Zusammenfassung:** { none, kilobits, megabits } **Standard:** none Die Einheit für "inbandwidth", je Sekunde.
outbandwidth { outbandwidth }	**Zusammenfassung:** Eine vorzeichenlose 16-Bit-Ganzzahl Die ausgehende Bandbreite für diese Schnittstelle. Hier nur die Nummer angeben. Die Einheit (Kilobits, Megabits) wird in der "out-unit" festgelegt. Dieser Parameter ist obligatorisch.
out-unit { out-unit }	**Zusammenfassung:** { kilobits, megabits } **Standard:** megabits Die Einheit für die ausgehende Bandbreite, je Sekunde.
description { description }	**Zusammenfassung:** Eine Zeichenkette Eine Beschreibung für diese Konfigurationseinheit.

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 15.2.2.3
Eine Verkehrssteuerungsschnittstelle löschen

Um eine Verkehrssteuerungsschnittstelle zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die Verkehrssteuerungsschnittstelle, indem Sie Folgendes eingeben:

   ```
   no qos traffic-control basic-configuration tcinterfaces interface
   ```

   Erläuterung:

   - *`interface`* ist die Bezeichnung der Verkehrssteuerungsschnittstelle
3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 15.2.3
Verkehrssteuerungsprioritäten verwalten

Verkehrssteuerungsprioritäten sind Prioritäten für die Verkehrsformung.

HINWEIS
Verkehrssteuerungsprioritäten können nur im Basisbetrieb konfiguriert werden. Weitere Informationen über die Einstellung der Verkehrssteuerung finden Sie unter Abschnitt 15.2.1, „Aktivieren und Konfigurieren der Verkehrssteuerung“.

INHALT

- Abschnitt 15.2.3.1, „Eine Liste der Verkehrssteuerungsprioritäten anzeigen“
- Abschnitt 15.2.3.2, „Eine Verkehrssteuerungspriorität hinzufügen“
- Abschnitt 15.2.3.3, „Eine Verkehrssteuerungspriorität löschen“

Abschnitt 15.2.3.1
Eine Liste der Verkehrssteuerungsprioritäten anzeigen

Um eine Liste der Verkehrssteuerungsprioritäten anzusehen, geben Sie Folgendes ein:

```
show running-config qos traffic-control basic-configuration tcpriorities
```

Falls Prioritäten konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config qos traffic-control basic-configuration tcpriorities
qos
 traffic-control
  basic-configuration
   tcpriorities high
    band        high
    protocol    tcp
    port        80
    description "High priority traffic"
   !
   tcpriorities medium
    protocol    udp
    port        1500
    description "Medium priority traffic"
   !
   tcpriorities low
    band        low
    protocol    icmp
    description "Low priority traffic"
   !
  !
 !
!
```

Falls keine Prioritäten konfiguriert wurden, fügen Sie je nach Bedarf Prioritäten hinzu. Weitere Informationen finden Sie unter Abschnitt 15.2.3.2, „Eine Verkehrssteuerungspriorität hinzufügen“.

Abschnitt 15.2.3.2
Eine Verkehrssteuerungspriorität hinzufügen

Um eine neue Verkehrssteuerungspriorität hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie die statische MAC-Adresse hinzu, indem Sie Folgendes eingeben:

   ```
   qos traffic-control basic-configuration tcpriority name
   ```

   Erläuterung:

   - *name* ist die Bezeichnung des Prioritäteintrags für die Verkehrssteuerung
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
iptype { iptype }	**Zusammenfassung:** { ipv4, ipv6, ipv4ipv6 } **Standard:** ipv4 Typ des Internetprotokolls - beide verwenden, wenn keine Adressen eingesetzt sind, ansonsten IPv4- und IPv6-Regeln für jede Art von verwendeten Adressen definieren.
band { band }	**Zusammenfassung:** { high, medium, low } **Standard:** medium

Parameter	Beschreibung
	Priorität (Bandbreite): "high", "medium", "low"... **Hohe Bandbreite umfasst:** Verzögerung verringern (md) (0x10), md + Kosten verringern (mmc) (0x12), md + Zuverlässigkeit erhöhen (mr) (0x14), mmc+md+mr (0x16). **Mittlere Bandbreite umfasst:** Bestimmungsgemäßer Betrieb (0x0), mr (0x04), mmc+mr (0x06), md + Datendurchsatz erhöhen (mt) (0x18), mmc+mt+md (0x1a), mr+mt+md (0x1c), mmc +mr+mt+md (0x1e). **Niedrige Bandbreite umfasst:** mmc (0x02), mt (0x08), mmc+mt (0x0a), mr+mt (0x0c), mmc+mr+mt (0x0e).
protocol { protocol }	**Zusammenfassung:** { tcp, udp, icmp, all } oder eine Zeichenkette (Auswahl) Ein zielgerichtetes Protokoll.
port { port }	**Zusammenfassung:** Eine Zeichenkette (Auswahl) Quellport - kann **nur** festgelegt werden, wenn das Protokoll TCP, UDP, DCCP, SCTP oder UDPlite ist **HINWEIS** *Eine Portnummer kann nur festgelegt werden, wenn das Protokoll entweder TCP, UDP, DCCP, SCTP oder UDPlite ist*
address { address }	**Zusammenfassung:** Eine Zeichenkette (Auswahl) Die Quelladresse. Dies kann **nur** festgelegt werden, wenn das Protokoll, der Port und die Adresse nicht definiert sind. **HINWEIS** *Eine Adresse kann nur festgelegt werden, wenn weder ein Protokoll oder Port noch eine Schnittstelle spezifiziert sind.*
interface { interface }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 15 Zeichen (Auswahl) Die Quellschnittstelle. Dies kann **nur** festgelegt werden, wenn das Protokoll, der Port und die Adresse nicht definiert sind. Alphanumerische Kleinbuchstaben sowie die Zeichen '.' und '-' sind zulässig. **HINWEIS** *Eine Schnittstelle kann nur festgelegt werden, wenn weder ein Protokoll, ein Port noch eine Adresse spezifiziert sind.*
description { description }	**Zusammenfassung:** Eine Zeichenkette (optional) Eine Beschreibung für diese Konfiguration.

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 15.2.3.3
Eine Verkehrssteuerungspriorität löschen

Um eine Verkehrssteuerungspriorität zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die Verkehrssteuerungspriorität, indem Sie Folgendes eingeben:

```
no qos traffic-control basic-configuration tcpriority name
```

Erläuterung:

- *`name`* ist die Bezeichnung des Prioritäteintrags für die Verkehrssteuerung

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 15.2.4
Verkehrssteuerungsklassen verwalten

Verkehrssteuerungsklassen legen Klassen für die Verkehrsformung fest. Optional können sie auch Parameter für Type of Service (ToS) festlegen, ein Acht-Bit-Feld im IPv4-Header. Die Verkehrssteuerung kann den ToS-Wert eines eingehenden IP-Frames prüfen und den Verkehr klassifizieren, um in der ausgehenden Warteschlange bevorzugte Dienste bereitzustellen. Die Klassifizierung des Verkehrs basiert auf dem ToS-Wert und den für jede Verkehrssteuerungsklasse und -regel definierten ToS-Optionen. IP-Verkehr, der mit den ToS-Optionen übereinstimmt, hat Vorrang vor den Kennzeichnungsregeln.

HINWEIS
Für jede Netzwerkschnittstelle muss eine Verkehrssteuerungsklasse hinzugefügt werden.

HINWEIS
Der Type of Service (ToS) ist von der Internet Engineering Task Force (IETF) festgelegt. Weitere Informationen über ToS finden Sie in RFC 1349 [http://tools.ietf.org/html/rfc1349].

INHALT

- Abschnitt 15.2.4.1, „Eine Liste der Verkehrssteuerungsklassen anzeigen“
- Abschnitt 15.2.4.2, „Hinzufügen einer Verkehrssteuerungsklasse“
- Abschnitt 15.2.4.3, „Eine Verkehrssteuerungsklasse löschen“

Abschnitt 15.2.4.1
Eine Liste der Verkehrssteuerungsklassen anzeigen

Um eine Liste der Verkehrssteuerungsklassen anzusehen, geben Sie Folgendes ein:

```
show running-config qos traffic-control advanced-configuration tcclasses
```

Falls Klassen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config qos traffic-control advanced-configuration tcclasses
qos
 traffic-control
  advanced-configuration
   tcclasses TCP
    interface     te1-2-1c01ppp
    mark          1
    min-bandwidth full/2
    max-bandwidth full
    priority      1
   !
  !
 !
!
```

Falls keine Klassen konfiguriert wurden, fügen Sie je nach Bedarf Klassen hinzu. Weitere Informationen finden Sie unter Abschnitt 15.2.4.2, „Hinzufügen einer Verkehrssteuerungsklasse“.

Abschnitt 15.2.4.2

Hinzufügen einer Verkehrssteuerungsklasse

Um eine neue Verkehrssteuerungsklasse hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie die statische MAC-Adresse hinzu, indem Sie Folgendes eingeben:

   ```
   qos traffic-control advanced-configuration tcclasses name
   ```

   Erläuterung:

   - *name* ist die Bezeichnung des Klasseneintrags zur Verkehrssteuerung
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
iptype { iptype }	**Zusammenfassung:** { ipv4, ipv6, ipv4ipv6 } **Standard:** ipv4 Typ des Internetprotokolls - beide verwenden, wenn keine Adressen eingesetzt sind, ansonsten IPv4- und IPv6-Regeln für jede Art von verwendeten Adressen definieren.
interface { interface }	**Zusammenfassung:** Eine Zeichenkette Die Schnittstelle, für die die Klasse zutrifft. Jede Schnittstelle darf nur einmal aufgelistet sein. Alphanumerische Kleinbuchstaben sowie die Zeichen '.' und '-' sind zulässig. Dieser Parameter ist obligatorisch.
mark { mark }	**Zusammenfassung:** Eine vorzeichenlose 16-Bit-Ganzzahl zwischen 1 und 255 Eine Kennzeichnung, die Verkehr zu dieser Klasse kennzeichnet. Dies ist eine einmalige Ganzzahl zwischen 1 und 255. Jede Klasse muss ihre eigene eindeutige Kennzeichnung haben. Dieser Parameter ist obligatorisch.
min-bandwidth { min-bandwidth }	**Zusammenfassung:** Eine Zeichenkette Die kleinste Bandbreite sollte diese Klasse haben, wenn die Verkehrsbelastung ansteigt. Dies kann entweder ein Zahlenwert oder ein berechneter Ausdruck anhand der Bandbreite der Schnittstelle sein. Ein fester Zahlenwert darf nur eine Nummer sein - seine Einheit ist in "Minbw-unit" festgelegt. Ein berechneter Ausdruck basiert auf einem Anteil der 'vollen' Bandbreite, wie z. B.: • 'full/3' für ein Drittel der Bandbreite und • 'full*9/10' für neun Zehntel der Bandbreite. Legen Sie in diesem Fall "minbw-unit" nicht fest. Dieser Parameter ist obligatorisch.
minbw-unit { minbw-unit }	**Zusammenfassung:** { none, kilobits, megabits } **Standard:** none (je Sekunde) Nur wenn die minimale Bandbreite ein einzelner Zahlenwert ist.
max-bandwidth { max-bandwidth }	**Zusammenfassung:** Eine Zeichenkette Die zulässige maximale Bandbreite dieser Klasse, sofern die Verbindung betriebsbereit ist. Dies kann entweder ein Zahlenwert oder ein berechneter Ausdruck anhand der Bandbreite der Schnittstelle sein. Ein fester Zahlenwert darf nur eine Nummer sein - seine Einheit ist in "Maxbw-unit" festgelegt. Ein berechneter Ausdruck basiert auf einem Anteil der 'vollen' Bandbreite, wie z. B.: • 'full/3' für ein Drittel der Bandbreite und • 'full*9/10' für neun Zehntel der Bandbreite. Legen Sie in diesem Fall "maxbw-unit" nicht fest. Dieser Parameter ist obligatorisch.

Parameter	Beschreibung
maxbw-unit { maxbw-unit }	**Zusammenfassung:** { none, kilobits, megabits } **Standard:** none (je Sekunde) nur wenn "max-bandwidth" ein **einzelner Zahlenwert** ist.
priority { priority }	**Zusammenfassung:** Eine vorzeichenlose 16-Bit-Ganzzahl zwischen 0 und 7 **Standard:** 0 Die Priorität, nach der Klassen bedient werden. Klassen mit höherer Priorität verzeichnen weniger Verzögerung, da sie zuerst bedient werden. Prioritätswerte werden in aufsteigender Reihenfolge behandelt (z. B. 0 hat höhere Priorität als 1. Minimum: 7).
description { description }	**Zusammenfassung:** Eine Zeichenkette Eine Beschreibung für diese Konfigurationseinheit.

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 15.2.4.3
Eine Verkehrssteuerungsklasse löschen

Um eine Verkehrssteuerungsklasse zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die Verkehrssteuerungsklasse, indem Sie Folgendes eingeben:

```
no qos traffic-control advanced-configuration tcclasses name
```

Erläuterung:

- *`name`* ist die Bezeichnung des Klasseneintrags zur Verkehrssteuerung

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 15.2.5
Verkehrssteuerungsgeräte verwalten

Verkehrssteuerungsgeräte sind Geräte für die Verkehrsformung.

HINWEIS
Verkehrssteuerungsgeräte können nur im erweiterten Betrieb konfiguriert werden. Weitere Informationen über die Einstellung der Verkehrssteuerung finden Sie unter Abschnitt 15.2.1, „Aktivieren und Konfigurieren der Verkehrssteuerung“.

INHALT

- Abschnitt 15.2.5.1, „Eine Liste der Verkehrssteuerungsgeräte anzeigen“
- Abschnitt 15.2.5.2, „Ein Verkehrssteuergerät hinzufügen“
- Abschnitt 15.2.5.3, „Ein Verkehrssteuergerät löschen“

Abschnitt 15.2.5.1

Eine Liste der Verkehrssteuerungsgeräte anzeigen

Um eine Liste der Verkehrssteuerungsgeräte anzusehen, geben Sie Folgendes ein:

```
show running-config qos traffic-control advanced-configuration tcdevices
```

Falls Geräte konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config qos traffic-control advanced-configuration tcdevices
qos
 traffic-control
  advanced-configuration
   tcdevices te1-2-1c01ppp
    inbandwidth  1500
    in-unit      kilobits
    outbandwidth 1500
    out-unit     kilobits
   !
  !
 !
!
```

Falls keine Geräte konfiguriert wurden, fügen Sie je nach Bedarf Geräte hinzu. Weitere Informationen finden Sie unter Abschnitt 15.2.5.2, „Ein Verkehrssteuergerät hinzufügen“.

Abschnitt 15.2.5.2

Ein Verkehrssteuergerät hinzufügen

Um ein neues Verkehrssteuergerät hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie das Verkehrssteuergerät hinzu, indem Sie Folgendes eingeben:

   ```
   qos traffic-control advanced-configuration tcdevices name
   ```

   Erläuterung:

   - *name* ist die Bezeichnung der Schnittstelle, für die Verkehrsformung gilt. Alphanumerische Kleinbuchstaben sowie die Zeichen ‚.‘ und ‚-‘ sind zulässig.
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
{ interface }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 15 Zeichen Eine Schnittstelle, für die Verkehrsformung gilt. Alphanumerische Kleinbuchstaben sowie die Zeichen '.' und '-' sind zulässig.
iptype { iptype }	**Zusammenfassung:** { ipv4, ipv6, ipv4ipv6 } **Standard:** ipv4 Typ des Internetprotokolls - beide verwenden, wenn keine Adressen eingesetzt sind, ansonsten IPv4- und IPv6-Regeln für jede Art von verwendeten Adressen definieren.
inbandwidth { inbandwidth }	**Zusammenfassung:** Eine vorzeichenlose 16-Bit-Ganzzahl **Standard:** 0 Eingehende Bandbreite. Default: 0 = ignore ingress. Bestimmt den maximalen Verkehr, der insgesamt für diese Schnittstelle zulässig ist. Ist die Rate überschritten, werden die Pakete verworfen.
in-unit { in-unit }	**Zusammenfassung:** { none, kilobits, megabits }

Parameter	Beschreibung
	Standard: none Einheit für "inbandwidth", je Sekunde.
outbandwidth { outbandwidth }	**Zusammenfassung:** Eine vorzeichenlose 16-Bit-Ganzzahl Maximale ausgehende Bandbreite... Die Höchstgeschwindigkeit, die verarbeitet werden kann. Zusätzliche Pakete werden verworfen. Dies ist die Bandbreite, die beim Festlegen der Klassen als 'full' bezeichnet werden kann. Dieser Parameter ist obligatorisch.
out-unit { out-unit }	**Zusammenfassung:** { kilobits, megabits } **Standard:** megabits Einheit für die ausgehende Bandbreite, je Sekunde.
description { description }	**Zusammenfassung:** Eine Zeichenkette Eine Beschreibung für diese Konfigurationseinheit.

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 15.2.5.3
Ein Verkehrssteuergerät löschen

Um eine Verkehrssteuergerät zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie das Verkehrssteuergerät hinzu, indem Sie Folgendes eingeben:

```
no qos traffic-control advanced-configuration tcdevices name
```

   Erläuterung:

   - *`name`* ist die Bezeichnung der Schnittstelle, für die Verkehrsformung gilt.

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 15.2.6
Verkehrssteuerungsregeln verwalten

Verkehrssteuerungsregeln sind Regeln für die Paketkennzeichnung.

HINWEIS
Verkehrssteuerungsregeln können nur im erweiterten Betrieb konfiguriert werden. Weitere Informationen über die Einstellung der Verkehrssteuerung finden Sie unter Abschnitt 15.2.1, „Aktivieren und Konfigurieren der Verkehrssteuerung“.

INHALT

- Abschnitt 15.2.6.1, „Eine Liste der Verkehrssteuerungsregeln anzeigen“
- Abschnitt 15.2.6.2, „Hinzufügen einer Verkehrssteuerungsregel“
- Abschnitt 15.2.6.3, „QoS-Kennzeichnungen konfigurieren“

- Abschnitt 15.2.6.4, „Eine Verkehrsteuerungsregel löschen“

Abschnitt 15.2.6.1

Eine Liste der Verkehrssteuerungsregeln anzeigen

Um eine Liste der Verkehrssteuerungsregeln anzusehen, geben Sie Folgendes ein:

```
show running-config qos traffic-control advanced-configuration tcrules
```

Falls Regeln konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config qos traffic-control advanced-configuration tcrules
qos
 traffic-control
  advanced-configuration
   tcrules rule1
    mark-choice set
     mark 1
    !
    source       all
    destination  all
    protocol     tcp
    source-ports 80
   !
  !
 !
!
```

Falls keine Regeln konfiguriert wurden, fügen Sie je nach Bedarf Regeln hinzu. Weitere Informationen finden Sie unter Abschnitt 15.2.6.2, „Hinzufügen einer Verkehrssteuerungsregel“.

Abschnitt 15.2.6.2

Hinzufügen einer Verkehrssteuerungsregel

Um eine neue Verkehrssteuerungsregel hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie die Verkehrssteuerungsregel hinzu, indem Sie Folgendes eingeben:

   ```
   qos traffic-control advanced-configuration tcrule name
   ```

   Erläuterung:

   - *name* ist die Bezeichnung des Eintrags zur Verkehrssteuerungsregel
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
{ name }	**Zusammenfassung:** Eine Zeichenkette Ein eindeutiger Name für diese Regel.
iptype { iptype }	**Zusammenfassung:** { ipv4, ipv6, ipv4ipv6 } **Standard:** ipv4 Typ des Internetprotokolls - beide verwenden, wenn keine Adressen eingesetzt sind, ansonsten IPv4- und IPv6-Regeln für jede Art von verwendeten Adressen definieren.
source { source }	**Zusammenfassung:** Eine Zeichenkette

Parameter	Beschreibung
	IF-Name, kommaseparierte Liste der Hosts oder IPs, MAC-Adressen oder 'all'. Bei Verwendung von MAC-Adressen '~' als Präfix und '-' als Separator verwenden. Beispiel: ~00-1a-6b-4a-72-34,~00-1a-6b-4a-71-42 Dieser Parameter ist obligatorisch.
destination { destination }	**Zusammenfassung:** Eine Zeichenkette IF-Name, kommaseparierte Liste der Hosts, IPs oder 'all'. Dieser Parameter ist obligatorisch.
protocol { protocol }	**Zusammenfassung:** { tcp, udp, icmp, all } oder eine Zeichenkette **Standard:** all Protokoll, das die Regel erfüllen muss.
destination-ports { destination-ports }	**Zusammenfassung:** Eine Zeichenkette (Optional) Eine kommaseparierte Liste von Portnamen, Portnummern oder Portbereichen.
source-ports { source-ports }	**Zusammenfassung:** Eine Zeichenkette (Optional) Eine kommaseparierte Liste von Portnamen, Portnummern oder Portbereichen.
test { test }	**Zusammenfassung:** Eine Zeichenkette (Optional) Definiert einen Test am bestehenden Paket oder dem Verbindungskennzeichen. Die Voreinstellung ist eine Paketkennzeichnung. Zum Testen eines Verbindungskennzeichens ':C' an das Ende des Prüfwerts anfügen. Beispiel: Prüfen, ob das Paketkennzeichen nicht null ist: **!0** Prüfen, ob das Verbindungskennzeichen nicht null ist: **!0:C**
length { length }	**Zusammenfassung:** Eine Zeichenkette (Optional) Gleicht die Länge eines Pakets mit einem bestimmten Wert oder Wertebereich ab... Größer als und kleiner als sowie Bereiche werden im Format min:max unterstützt. Beispiel: Gleich 64 **64** Größer oder gleich 65 **65:** Weniger oder gleich 65 **:65** Zwischen 64 und 768 **64:768**
tos { tos }	**Zusammenfassung:** { minimize-delay, maximize-throughput, maximize-reliability, minimize-cost, normal-service } oder eine Zeichenkette (Optional) Type of Service. Ein vordefinierter ToS-Wert oder ein Zahlenwert. Der Zahlenwert ist hexadezimal. Beispiel: 0x38
description { description }	**Zusammenfassung:** Eine Zeichenkette Eine Beschreibung für diese Konfigurationseinheit.

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 15.2.6.3
QoS-Kennzeichnungen konfigurieren

Eine QoS-Kennzeichnung (Quality of Service) markiert wichtige Datenpakete, die auf ihrem Weg durch das Netzwerk bevorzugt behandelt werden sollen. Für jede Verkehrssteuerungsregel ist nur ein QoS-Kennzeichen zugelassen. Mögliche Optionen sind:

- **Set:** Gibt an, ob dem Paket oder der Verbindung ein QoS-Kennzeichen zugeordnet ist.
- **Modify:** Ändert den Wert des QoS-Kennzeichens mittels AND- oder OR-Argument.
- **Save/Restore:** Ersetzt den Wert des QoS-Kennzeichens der Verbindung durch einen zugeordneten Wert.
- **Continue:** Bei Übereinstimmung des Pakets werden keine weiteren Verkehrssteuerungsregeln geprüft und das Paket wird automatisch an die angegebene Kette weitergeleitet.
- **DSCP Marking:** Legt fest, ob dem Paket das DSCP-Kennzeichen zugeordnet wird.

Um das QoS-Kennzeichen für eine Verkehrssteuerungsregel zu konfigurieren, gehen Sie wie folgt vor:

» Konfigurieren des Kennzeichens "Set"

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Wählen Sie die Option Set durch folgende Eingabe:

```
qos traffic-control advanced-configuration tcrules name mark-choice set
```

   Erläuterung:

   - *name* ist die Bezeichnung der Verkehrssteuerungsregel

3. Konfigurieren Sie den/die folgende Parameter:



HINWEIS
Der Parameter `chain-options` *gibt die Kette an, in der die Regel verarbeitet wird.*

- ***Pre-Routing - Verbindung in der Kette PREROUTING kennzeichnen.***
  Kann mit DNAT-, SNAT- und Masquerading-Regeln in der Firewall verwendet werden. Ein Beispiel für eine solche Regel ist ***Source.IP:192.168.2.101, Chain-option: preroute oder default****, doch die eigentliche Source.NAT-Adresse ist 2.2.2.2.*
- ***Post-Routing - Verbindung in der Kette POSTROUTING kennzeichnen.***
  Kann mit DNAT-, SNAT- und Masquerading-Regeln in der Firewall verwendet werden. Ein Beispiel für eine solche Regel ist ***Destination.IP:192.168.3.101, Chain-option:preroute oder default****. In diesem Fall ist die tatsächliche Zieladresse 192.168.3.101, doch sie wird von DNAT in 192.168.3.33 übersetzt. Ein weiteres Beispiel für eine Verkehrssteuerungsregel ist* ***Destination.IP:192.168.3.33, Chain-option:postrouting****.*
- ***Forward - Verbindung in der Kette FORWARD kennzeichnen.***
  Dies ist die Standard-Kettenoption und kann für normalen IP-Verkehr ohne Adress- oder Portübersetzung verwendet werden.

Parameter	Beschreibung
object { object }	**Zusammenfassung:** { packet, connection } **Standard:** packet Kennzeichnet entweder ein Paket oder eine Verbindung.
mark { mark }	**Zusammenfassung:** Eine Zeichenkette Eine Kennzeichnung, die einer Klassenkennzeichnung entspricht (Dezimalwert).
mask { mask }	**Zusammenfassung:** Eine Zeichenkette (optional) Eine Maske, um zu bestimmen, welche Markierungsbits festgelegt werden.
chain-options { chain-options }	**Zusammenfassung:** { forward, postrouting, prerouting } **Standard:** forward Eine Kette, in der die festgelegte Operation erfolgen wird.

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

» Konfigurieren eines Kennzeichens "Modify"

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Wählen Sie die Option Modify durch folgende Eingabe:

```
qos traffic-control advanced-configuration tcrules name mark-choice modify
```

Erläuterung:

- *`name`* ist die Bezeichnung der Verkehrssteuerungsregel

3. Konfigurieren Sie den/die folgende Parameter:

Parameter	Beschreibung
logic-op { logic-op }	**Zusammenfassung:** { and, or } Eine logische Operation, die an der aktuellen Kennzeichnung auszuführen ist: UND/ ODER.
mark-value { mark-value }	**Zusammenfassung:** Eine Zeichenkette Eine Kennzeichnung, mit der die Operation auszuführen ist (Dezimalwert).
modify-chain { modify-chain }	**Zusammenfassung:** { forward, postrouting, prerouting } **Standard:** forward Eine Kette, in der die Operation erfolgen wird.

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

» Konfigurieren eines Kennzeichens "Save"

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Konfigurieren Sie die Option "Save" durch folgende Eingabe:

```
qos traffic-control advanced-configuration tcrules name mark-choice save
```

Erläuterung:

- *`name`* ist die Bezeichnung der Verkehrssteuerungsregel

3. Konfigurieren Sie den/die folgende Parameter:

Parameter	Beschreibung
value-mask { value-mask }	**Zusammenfassung:** Eine Zeichenkette Maske, mit der die Kennzeichnung zu verarbeiten ist.
op-chain { op-chain }	**Zusammenfassung:** { forward, prerouting } **Standard:** forward Eine Kette, in der die Operation erfolgen wird.

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Konfigurieren eines Kennzeichens "Restore"

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Wählen Sie die Option Restore durch folgende Eingabe:

```
qos traffic-control advanced-configuration tcrules name mark-choice restore
```

   Erläuterung:

   - *name* ist die Bezeichnung der Verkehrssteuerungsregel

3. Konfigurieren Sie den/die folgende Parameter:

Parameter	Beschreibung
value-mask { value-mask }	**Zusammenfassung:** Eine Zeichenkette Eine Maske, mit der die Kennzeichnung zu verarbeiten ist.
op-chain { op-chain }	**Zusammenfassung:** { forward, prerouting } **Standard:** forward Eine Kette, in der die Operation erfolgen wird.

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Konfigurieren eines Kennzeichens "Continue"

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Wählen Sie die Option Continue durch folgende Eingabe:

```
qos traffic-control advanced-configuration tcrules name mark-choice continue
```

   Erläuterung:

   - *name* ist die Bezeichnung der Verkehrssteuerungsregel

3. Konfigurieren Sie den/die folgende Parameter:

Parameter	Beschreibung
continue-chain { continue-chain }	**Zusammenfassung:** { forward, prerouting } **Standard:** forward Eine Kette, in der die Operation erfolgen wird.

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Konfigurieren eines DSCP-Kennzeichens

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Wählen Sie die Option "DSCP Marking" durch folgende Eingabe:

```
qos traffic-control advanced-configuration tcrules name mark-choice dscpmarking
```

   Erläuterung:

   - *name* ist die Bezeichnung der Verkehrssteuerungsregel

3. Konfigurieren Sie den/die folgende Parameter:

Parameter	Beschreibung
dscp-mark { dscp-mark }	**Zusammenfassung:** { BE, AF11, AF12, AF13, AF21, AF22, AF23, AF31, AF32, AF33, AF41, AF42, AF43, CS1, CS2, CS3, CS4, CS5, CS6, CS7, EF } Ein Wert der DSCP-Klasse, der aus einer vorgegebenen Liste ausgewählt ist.
dscpchain { dscpchain }	**Zusammenfassung:** { forward, postrouting, prerouting } **Standard:** forward Eine Kette, in der die DSCP-Kennzeichnung erfolgen wird.

4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 15.2.6.4
Eine Verkehrsteuerungsregel löschen

Um eine Verkehrsteuerungsregel zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die Verkehrssteuerungsregel, indem Sie Folgendes eingeben:

```
no qos traffic-control advanced-configuration tcrule name
```

Erläuterung:

- *`name`* ist die Bezeichnung des Eintrags zur Verkehrssteuerungsregel

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 15.2.7
QoS-Mapping für VLANs verwalten

Mit QoS-(Quality of Service)-Mapping wird der QoS-Verkehr zugeordnet. Dem eingehenden IP-Verkehr wird eine Kontrollmarkierung anhand des Prioritätswerts eines getaggten Frames zugewiesen. Der eingehende Verkehr wird dann klassifiziert und in den Prioritätswarteschlagen nach den in der markierten Regel festgelegten Verkehrssteuerungsregeln eingeordnet. Die Verkehrssteuerung kann ferner den gleichen oder einen anderen Prioritätswert zuordnen, wenn ein Frame mit einem VLAN-Tag durch eine Verkehrssteuerungsschnittstelle gesendet werden soll.

QoS-Maps können für VLAN-Verbindungen an virtuellen Switches konfiguriert werden.

INHALT

- Abschnitt 15.2.7.1, „Anzeigen einer Liste der QoS-Maps für VLANs“
- Abschnitt 15.2.7.2, „Hinzufügen einer QoS-Map“
- Abschnitt 15.2.7.3, „Löschen einer QoS-Map“

Abschnitt 15.2.7.1

Anzeigen einer Liste der QoS-Maps für VLANs

Um eine Liste der QoS-Maps für VLAN-Verbindungen anzuzeigen, geben Sie Folgendes ein:

- **Bei Switched-Ethernet-Ports**

  ```
  show running-config switch vlans all-vlans id qosmap
  ```

  Erläuterung:

  - *id* ist die ID für das VLAN

- **Bei virtuellen Switches**

  ```
  show running-config interface virtualswitch id vlan  vlan-id qosmap
  ```

  Erläuterung:

  - *id* die ID des virtuellen Switch
  - *vlan-id* ist die ID für das VLAN

Falls QoS-Maps konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config interface virtualswitch vlan 100 qosmap
interface
 virtualswitch 1
  vlan 100
   qosmap 2
    ingress 10
   !
  !
 !
!
```

Falls keine QoS-Maps konfiguriert wurden, fügen Sie je nach Bedarf Maps hinzu. Weitere Informationen finden Sie unter Abschnitt 15.2.7.2, „Hinzufügen einer QoS-Map“.

Abschnitt 15.2.7.2

Hinzufügen einer QoS-Map

Um einer VLAN-Verbindung eine QoS-Map hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie die QoS-Map hinzu, indem Sie Folgendes eingeben:
   - **Bei Switched-Ethernet-Ports**

     ```
     switch vlans all-vlans id qosmap priority
     ```

     Erläuterung:

     - *id* ist die ID für das VLAN
     - *priority* ist die der QoS-Map zugeordnete Priorität

   - **Bei virtuellen Switches**

     ```
     interface virtualswitch id vlan  vlan-id qosmap priority
     ```

     Erläuterung:

     - *id* die ID des virtuellen Switch
     - *vlan-id* ist die ID für das VLAN

- *priority* ist die der QoS-Map zugeordnete Priorität

3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
ingress { ingress }	**Zusammenfassung:** Eine vorzeichenlose 8-Bit-Ganzzahl zwischen 0 und 255 Zu kennzeichnender Map-Eingang. Dieser Parameter ist obligatorisch.

4. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 15.2.7.3
Löschen einer QoS-Map

Um eine QoS-Map aus einer VLAN-Verbindung zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die QoS-Map aus der VLAN-Verbindung, indem Sie Folgendes eingeben:
   - **Bei Switched-Ethernet-Ports**

     ```
     no switch vlans all-vlans id qosmap priority
     ```

     Erläuterung:
     - *id* ist die ID für das VLAN
     - *priority* ist die der QoS-Map zugeordnete Priorität
   - **Bei virtuellen Switches**

     ```
     no interface virtualswitch id vlan  vlan-id qosmap priority
     ```

     Erläuterung:
     - *id* die ID des virtuellen Switch
     - *vlan-id* ist die ID für das VLAN
     - *priority* ist die der QoS-Map zugeordnete Priorität
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 15.2.8
Egress-Marker für QoS-Maps verwalten

Egress-Marker für QoS-Maps werden verwendet, um Verkehr, der den gleichen Marker wie einer der für das Gerät konfigurierten Egress-Marker trägt, vorrangig zu behandeln.

INHALT

- Abschnitt 15.2.8.1, „Anzeigen einer Liste der ausgehenden (egress) Kennzeichnungen“
- Abschnitt 15.2.8.2, „Hinzufügen einer ausgehenden (egress) Kennzeichnung“
- Abschnitt 15.2.8.3, „Löschen einer ausgehenden (egress) Kennzeichnung“

Abschnitt 15.2.8.1

Anzeigen einer Liste der ausgehenden (egress) Kennzeichnungen

Um eine Liste der ausgehenden (egress) Kennzeichnungen für eine QoS-Map anzuzeigen, geben Sie Folgendes ein:

- **Bei Switched-Ethernet-Ports**

  ```
  show running-config interface switch vlans all-vlans id qosmap priority egress
  ```

  Erläuterung:

  - *id* ist die ID für das VLAN
  - *priority* ist die der QoS-Map zugeordnete Priorität

- **Bei virtuellen Switches**

  ```
  show running-config interface virtualswitch id vlan vlan-id qosmap priority egress
  ```

  Erläuterung:

  - *slot* ist die Bezeichnung des Modul-Einbauorts
  - *port* ist die Nummer des Ports (oder eine Liste von Ports, wenn sie in einem Port-Trunk gebündelt sind) für das Modul.
  - *id* ist die ID für das VLAN
  - *priority* ist die der QoS-Map zugeordnete Priorität

Falls Kennzeichnungen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
show running-config interface virtualswitch vs1 vlan 100 qosmap 2 egress
interface
 virtualswitch vs1
  vlan 100
   qosmap 2
    egress 11
    !
   !
  !
 !
!
```

Falls keine ausgehenden (egress) Kennzeichnungen konfiguriert wurden, fügen Sie je nach Bedarf ausgehende Kennzeichnungen hinzu. Weitere Informationen finden Sie unter Abschnitt 15.2.8.2, „Hinzufügen einer ausgehenden (egress) Kennzeichnung“.

Abschnitt 15.2.8.2

Hinzufügen einer ausgehenden (egress) Kennzeichnung

Um eine ausgehende (egress) Kennzeichnung zu einer QoS-Map hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie die QoS-Map hinzu, indem Sie Folgendes eingeben:
   - **Bei Switched-Ethernet-Ports**

     ```
     switch vlans all-vlans id qosmap priority egress mark
     ```

     Erläuterung:

     - *id* ist die ID für das VLAN

- *priority* ist die der QoS-Map zugeordnete Priorität
- *mark* ist der Wert der ausgehenden (egress) Kennzeichnung

- **Bei virtuellen Switches**

```
interface virtualswitch id vlan vlan-id qosmap priority egress mark
```

Erläuterung:

- *slot* ist die Bezeichnung des Modul-Einbauorts
- *port* ist die Nummer des Ports (oder eine Liste von Ports, wenn sie in einem Port-Trunk gebündelt sind) für das Modul.
- *id* ist die ID für das VLAN
- *priority* ist die der QoS-Map zugeordnete Priorität
- *mark* ist der Wert der ausgehenden (egress) Kennzeichnung

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 15.2.8.3

Löschen einer ausgehenden (egress) Kennzeichnung

Um eine ausgehende (egress) Kennzeichnung für eine QoS-Map zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die QoS-Map aus der VLAN-Verbindung, indem Sie Folgendes eingeben:

- **Bei Switched-Ethernet-Ports**

```
no switch vlans all-vlans id qosmap priority egress mark
```

Erläuterung:

- *id* ist die ID für das VLAN
- *priority* ist die der QoS-Map zugeordnete Priorität
- *mark* ist der Wert der ausgehenden (egress) Kennzeichnung

- **Bei virtuellen Switches**

```
no interface virtualswitch id vlan vlan-id qosmap priority egress mark
```

Erläuterung:

- *slot* ist die Bezeichnung des Modul-Einbauorts
- *port* ist die Nummer des Ports (oder eine Liste von Ports, wenn sie in einem Port-Trunk gebündelt sind) für das Modul.
- *id* ist die ID für das VLAN
- *priority* ist die der QoS-Map zugeordnete Priorität
- *mark* ist der Wert der ausgehenden (egress) Kennzeichnung

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 15.2.9

QoS-Statistiken anzeigen

RUGGEDCOM ROX II liefert Statistiken für den Verkehr, der jede konfigurierte Klasse passiert. Die Zuordnung von Paketen zu Klassen an der ausgehenden Schnittstelle erfolgt regelbasiert. Wenn ein Paket den angegebenen Kriterien entspricht, wird es als Mitglied der Klasse betrachtet und an diese weitergeleitet. Wenn das Paket keiner Regel entspricht, wird es an die voreingestellte Klasse weitergeleitet.

Weitere Informationen über Verkehrssteuerungsklassen finden Sie unter Abschnitt 15.2.4, „Verkehrssteuerungsklassen verwalten“.

HINWEIS
Statistiken sind nur verfügbar, wenn die Verkehrssteuerung im erweiterten Modus aktiviert ist. Weitere Informationen über das Aktivieren der Verkehrssteuerung finden Sie unter Abschnitt 15.2.1, „Aktivieren und Konfigurieren der Verkehrssteuerung“.

Um die QoS-Statistiken anzuzeigen, geben Sie Folgendes ein:

```
show qos statistics
```

Eine Tabelle oder Liste ähnlich dem folgenden Beispiel wird angezeigt:

```
ruggedcom# show qos statistics | tab
           MIN         MAX
CLASSNAME  BANDWIDTH   BANDWIDTH   SENTBYTES   SENTPACKETS   DROPPEDPACKETS   RATE        AVERAGE
-------------------------------------------------------------------------------------------
High       1200Kbit    1500Kbit    4956594     9953          0                446104bit   112pps
Default    300000bit   1500Kbit    3029832     6084          3869             270088bit   68pps
```

Diese Tabelle liefert die folgenden Informationen:

Parameter	Beschreibung
classname	**Zusammenfassung:** Eine Zeichenkette
min-bandwidth	**Zusammenfassung:** Eine Zeichenkette Die minimal gewährleistete Bandbreite. Dies basiert auf den definierten Merkmalen des Geräts.
max-bandwidth	**Zusammenfassung:** Eine Zeichenkette Die maximal gewährleistete Bandbreite, wenn es keinen höher priorisierten Verkehr gibt. Dies basiert auf den definierten Merkmalen des Geräts.
sentbytes	**Zusammenfassung:** Eine Zeichenkette Die Anzahl an Bytes, die durch diese Klasse gesendet wurden.
sentpackets	**Zusammenfassung:** Eine Zeichenkette Die Anzahl an Paketen, die durch diese Klasse gesendet wurden.
droppedpackets	**Zusammenfassung:** Eine Zeichenkette Die Anzahl der in dieser Klasse verworfenen Pakete.
rate	**Zusammenfassung:** Eine Zeichenkette Auf Grundlage eines 10-Sekunden-Durchschnitts.
average	**Zusammenfassung:** Eine Zeichenkette Auf Grundlage eines 10-Sekunden-Durchschnitts.

Abschnitt 15.3

Verwalten von Berechtigungsklassen

Berechtigungsklassen (Classes of Service, CoS) besitzen die Fähigkeit, die Übertragung bestimmter Frames und des Portverkehrs gegenüber anderen zu beschleunigen. Die CoS eines Frames kann auf "Normal", "Mittel", "Hoch" oder "Kritisch" gesetzt werden. Der RUGGEDCOM ROX II erzwingt "Normal CoS" standardmäßig für den gesamten Datenverkehr.

WICHTIG!
Verwenden Sie die höchste unterstützte CoS-Stufe mit Vorsicht, da diese immer vom Switch für die Handhabung des Netzwerkmanagement-Verkehrs (z. B. RSTP BPDUs) verwendet wird.

Falls diese CoS für den regulären Netzwerkverkehr verwendet wird, können bei Netzwerkauslastungen (Bursts) einige Netzwerkmanagement-Frames verloren gehen, was wiederum zu einem Verlust der Konnektivität über das Netzwerk führen kann.

Der Prozess der CoS-basierten Steuerung des Datenverkehrs erfolgt in zwei Phasen:

- **Überprüfungsphase**
  Während der Überprüfungsphase wird die CoS-Priorität eines empfangenen Frames anhand Folgendem bestimmt:
  - Eine bestimmte CoS basierend auf der MAC-Quelladresse und -Zieladresse (gemäß der Tabelle der statischen MAC-Adressen)
  - Das Prioritätsfeld in den 802.1Q-Tags
  - Die Differentiated Services Code Point (DSCP)-Komponente des Type Of Service (TOS)-Felds, falls der Frame eine IP ist
  - Die voreingestellte CoS für den Port

  Die CoS aller Frames wird bestimmt, sobald der erste geprüfte Parameter im Frame gefunden wurde.

  Empfangene Frames werden zuerst geprüft, um zu bestimmen, ob deren MAC-Ziel- oder -Quelladresse in der Tabelle der statischen MAC-Adressen gefunden wurde. Wenn ja, dann wird die für die statische MAC-Adresse konfigurierte CoS verwendet. Wenn weder die MAC-Quelladresse noch die MAC-Zieladresse in der Tabelle der statischen MAC-Adressen enthalten ist, wird der Frame auf 802.1Q-Tags geprüft und das Prioritätenfeld wird auf eine CoS abgebildet. Ist kein Tag vorhanden, wird der Frame geprüft, um zu ermitteln, ob es sich um einen IP-Frame handelt. Wenn der Frame ein IP-Frame und Inspecting TOS aktiviert ist, wird die CoS vom DSCP-Feld aus bestimmt. Wenn der Frame kein IP-Frame und Inspecting TOS deaktiviert ist, wird die Standard-CoS für den Port verwendet.

  Nach der Prüfung wird der Frame an den ausgehenden (egress) Port zur Übertragung weitergeleitet.

- **Weiterleitungsphase**
  Sobald die CoS des Frames bestimmt ist, wird der Frame an den ausgehenden (egress) Port weitergeleitet, wo er in eine der Prioritäts-Warteschlangen gemäß der zugewiesenen CoS eingeordnet wird.

  Anhand einer CoS-Gewichtung kann der Grad der bevorzugten Behandlung festgelegt werden, der verschiedenen Prioritäts-Warteschlangen zugeordnet ist. Das Verhältnis zwischen der Anzahl an höherrangigen CoS zu übertragenen niederrangigen CoS-Frames ist konfigurierbar. Falls gewünscht, kann der Benutzer niederrangigere CoS-Frames so konfigurieren, dass diese erst übertragen werden, nachdem alle höherrangigen Frames abgearbeitet wurden.

INHALT

- Abschnitt 15.3.1, „Berechtigungsklassen (Classes of Service, CoS) konfigurieren“
- Abschnitt 15.3.2, „Priority-to-CoS-Mapping verwalten“

- Abschnitt 15.3.3, „DSCP-to-CoS-Mapping verwalten“

Abschnitt 15.3.1

Berechtigungsklassen (Classes of Service, CoS) konfigurieren

Um Berechtigungsklassen zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Konfigurieren Sie die CoS-Bewertung, indem Sie Folgendes eingeben:

   ```
   switch classes-of-service cos-weighting weighting
   ```

   Erläuterung:

   - *weighting* ist der Bewertungsalgorithmus für die Übermittlung von Datenübertragungsblöcken unterschiedlicher CoS. Bei Verkehrsblöcken können Datenübertragungsblöcke, die sich in der Warteschlange des Switch befinden, während die Übertragung auf einem Port ansteht, unterschiedliche CoS-Prioritäten haben.
3. Falls erforderlich, konfigurieren Sie das CoS-Mapping entweder auf der Grundlage der Priorität IEEE 802.1p oder des Felds Differentiated Services (DS), das im IP-Header für jedes Paket festgelegt ist. Weitere Informationen finden Sie in Abschnitt 15.3.2.2, „Einen Priority-zu-CoS Mapping-Eintrag hinzufügen“ oder Abschnitt 15.3.3.2, „Hinzufügen eines DSCP-zu-CoS Mapping-Eintrags“.
4. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 15.3.2

Priority-to-CoS-Mapping verwalten

Die Zuordnung von CoS zu verschiedenen IEEE 802.1p Prioritätswerten im Frame erfolgt durch die Festlegung von Einträgen in der Priority-to-CoS-Mapping-Tabelle.

INHALT

- Abschnitt 15.3.2.1, „Eine Liste der Priority-to-CoS-Mapping-Einträge anzeigen“
- Abschnitt 15.3.2.2, „Einen Priority-zu-CoS Mapping-Eintrag hinzufügen“
- Abschnitt 15.3.2.3, „Einen Priority-zu-CoS Mapping-Eintrag löschen“

Abschnitt 15.3.2.1

Eine Liste der Priority-to-CoS-Mapping-Einträge anzeigen

Um eine Liste der Priority-to-CoS-Mapping-Einträge anzusehen, geben Sie Folgendes ein:

```
show running-config switch class-of-service priority-to-cos
```

Falls Einträge konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config switch class-of-service priority-to-cos | tab
PRIORITY  COS
------------------
0         normal
```

```
1          normal
2          normal
3          medium
4          medium
5          medium
6          high
7          high

!
```

Falls keine Einträge konfiguriert wurden, fügen Sie je nach Bedarf Einträge hinzu. Weitere Informationen finden Sie unter Abschnitt 15.3.2.2, „Einen Priority-zu-CoS Mapping-Eintrag hinzufügen“.

Abschnitt 15.3.2.2
Einen Priority-zu-CoS Mapping-Eintrag hinzufügen

Um einen Priority-zu-CoS Mapping-Eintrag hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den Eintrag hinzu, indem Sie Folgendes eingeben:

   ```
   switch class-of-service priority-to-cos priority
   ```

   Erläuterung:

   - *priority* ist der Wert der IEEE 802.1p-Priorität
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
cos { cos }	**Zusammenfassung:** { normal, medium, high, crit } **Standard:** normal Die Berechtigungsklasse (CoS, Class of Service), die empfangenen Frames, die mit dem angegebenen IEEE 802.1p-Prioritätswert markiert sind, zugeordnet ist.

4. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 15.3.2.3
Einen Priority-zu-CoS Mapping-Eintrag löschen

Um einen Priority-zu-CoS Mapping-Eintrag zu löschen, gehen Sie wie folgt vor:

HINWEIS
Durch Löschen des Eintrags wird CoS auf Normal eingestellt.

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den Eintrag, indem Sie Folgendes eingeben:

   ```
   no switch class-of-service priority-to-cos priority
   ```

   Erläuterung:

   - *priority* ist der Wert der IEEE 802.1p-Priorität

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 15.3.3
DSCP-to-CoS-Mapping verwalten

Die Zuweisung von CoS zu verschiedenen Werten in Feld DSCP (Differentiated Services Code Point) im IP-Header empfangener Pakete erfolgt durch die Festlegung von Einträgen in der DSCP-to-CoS-Mappingtabelle.

INHALT

- Abschnitt 15.3.3.1, „Eine Liste der DSCP-to-CoS-Mapping-Einträge anzeigen“
- Abschnitt 15.3.3.2, „Hinzufügen eines DSCP-zu-CoS Mapping-Eintrags“
- Abschnitt 15.3.3.3, „Einen DSCP-zu-CoS Mapping-Eintrag löschen“

Abschnitt 15.3.3.1
Eine Liste der DSCP-to-CoS-Mapping-Einträge anzeigen

Um eine Liste der Prioritäten anzusehen, geben Sie Folgendes ein:

```
show running-config switch class-of-service dscp-to-cos
```

Falls Einträge konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config switch class-of-service dscp-to-cos | tab
DSCP  COS
--------------
1     normal
3     high
4     medium
6     normal
7     normal

!
```

Falls keine Einträge konfiguriert wurden, fügen Sie je nach Bedarf Einträge hinzu. Weitere Informationen finden Sie unter Abschnitt 15.3.3.2, „Hinzufügen eines DSCP-zu-CoS Mapping-Eintrags“.

Abschnitt 15.3.3.2
Hinzufügen eines DSCP-zu-CoS Mapping-Eintrags

Um einen DSCP-zu-CoS Mapping-Eintrag hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den Eintrag hinzu, indem Sie Folgendes eingeben:

   ```
   switch class-of-service dscp-to-cos dscp
   ```

   Erläuterung:

   - *`dscp`* ist der Wert des Feldes 6 bit DiffServ im Feld Type-Of-Service (TOS) des IP-Headers.
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
cos { cos }	**Zusammenfassung:** { normal, medium, high, crit } **Standard:** normal Die Berechtigungsklasse (CoS, Class of Service), die empfangenen Frames mit dem angegebenen DSCP zugeordnet ist.

4. Konfigurieren Sie die CoS-Parameter je nach Bedarf an ausgewählten Switched-Ethernet-Ports und/oder Trunk-Schnittstellen. Weitere Informationen finden Sie unter Abschnitt 8.1.2, „Einen Switched-Ethernet-Port konfigurieren“ und/oder Abschnitt 8.2.2, „Hinzufügen einer Ethernet-Trunk-Schnittstelle“.
5. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 15.3.3.3

Einen DSCP-zu-CoS Mapping-Eintrag löschen

Um einen DSCP-zu-CoS Mapping-Eintrag zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den Eintrag, indem Sie Folgendes eingeben:

```
no switch class-of-service dscp-to-cos dscp
```

   Erläuterung:

   - *`dscp`* ist der Wert des Felds "6 bit DiffServ" im Feld "Type-Of-Service (TOS)" des IP-Headers.

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

16 Uhrzeitdienste

RUGGEDCOM ROX II bietet die folgenden Zeiterfassungs- und Zeitsynchronisationsfunktionen:

- Zeiterfassung und Zeitzonenmanagement für die lokale Hardware
- NTP (Network Time Protocol) Client und Server

INHALT

- Abschnitt 16.1, „Die Einstellungen zur Zeitsynchronisation konfigurieren“
- Abschnitt 16.2, „Systemzeit und -datum konfigurieren“
- Abschnitt 16.3, „Die Systemzeitzone konfigurieren“
- Abschnitt 16.4, „Ortszeit-Einstellungen konfigurieren“
- Abschnitt 16.5, „Den NTP-Service aktivieren und konfigurieren“
- Abschnitt 16.6, „Anzeigen des Status des NTP-Diensts“
- Abschnitt 16.7, „Status der Referenzuhren anzeigen“
- Abschnitt 16.8, „NTP-Server verwalten“
- Abschnitt 16.9, „NTP-Broadcast-/Multicast-Clients verwalten“

Abschnitt 16.1

Die Einstellungen zur Zeitsynchronisation konfigurieren

Um die Einstellungen zur Zeitsynchronisation zu konfigurieren, gehen Sie wie folgt vor:

1. Konfigurieren Sie Systemzeit und -datum. Für weitere Informationen siehe Abschnitt 16.2, „Systemzeit und -datum konfigurieren“.
2. Konfigurieren Sie die Systemzeitzone. Für weitere Informationen siehe Abschnitt 16.3, „Die Systemzeitzone konfigurieren“.
3. Konfigurieren Sie die Ortszeit-Einstellungen. Für weitere Informationen siehe Abschnitt 16.4, „Ortszeit-Einstellungen konfigurieren“.
4. Wenn Multicast-Adressen für den NTP-Server konfiguriert werden, aktivieren und konfigurieren Sie den NTP-Multicast-Client. Für weitere Informationen siehe Abschnitt 16.9.1, „NTP-Multicast-Clients aktivieren und konfigurieren“.
5. Wenn Broadcast-Adressen für den NTP-Server konfiguriert werden, aktivieren und konfigurieren Sie den NTP-Broadcast-Client. Für weitere Informationen siehe Abschnitt 16.9.2, „NTP-Broadcast-Clients aktivieren und konfigurieren“.

6. Fügen Sie einen entfernten NTP-Server hinzu. Für weitere Informationen siehe Abschnitt 16.8.3, „Hinzufügen eines NTP-Servers“.
7. Fügen Sie für den NTP-Server Broadcast-/Multicast-Adressen hinzu. Für weitere Informationen siehe Abschnitt 16.9.3.2, „Eine Broadcast-/Multicast-Adresse hinzufügen“.
8. Fügen Sie, sofern erforderlich, Authentifizierungsschlüssel für den Server hinzu. Für weitere Informationen siehe Abschnitt 16.8.5.2, „Einen Server-Schlüssel hinzufügen“.
9. Fügen Sie Einschränkungen für die entfernten NTP-Server hinzu. Für weitere Informationen siehe Abschnitt 16.8.6.2, „Hinzufügen einer Servereinschränkung“.
10. Aktivieren und konfigurieren Sie den NTP-Service. Für weitere Informationen siehe Abschnitt 16.5, „Den NTP-Service aktivieren und konfigurieren“.
11. Zeigen Sie den Status des NTP-Services an. Für weitere Informationen siehe Abschnitt 16.6, „Anzeigen des Status des NTP-Diensts“.

Abschnitt 16.2
Systemzeit und -datum konfigurieren

Um Systemzeit und -datum zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Stellen Sie Systemzeit und -datum ein, indem Sie Folgendes eingeben:

```
admin set-system-clock time time-date
```

   Erläuterung:

   - *time-date* ist Datum und Uhrzeit im Format JJJJ-MM-TT HH:MM:SS

3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 16.3
Die Systemzeitzone konfigurieren

Um die Systemzeitzone zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Stellen Sie die Systemzeitzone ein, indem Sie Folgendes eingeben:

   HINWEIS
   Die Etc/GMT-Zeitzonen entsprechen dem POSIX-Format und haben im Vergleich zur allgemeinen Nutzung gegenteilige Vorzeichen. Im POSIX-Format haben die Zeitzonen westlich der mittleren Greenwich-Zeit (GMT) ein positives Vorzeichen und die Zonen östlich der GMT ein negatives Vorzeichen.

```
admin timezone category category zone zone
```

   Erläuterung:

   - *category* ist die Kategorie der Zeitzone
   - *zone* ist die Zeitzone

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 16.4
Ortszeit-Einstellungen konfigurieren

Über die Ortszeit-Einstellungen wird die Ortszeit auf dem Gerät als NTP-Zeitquelle konfiguriert.

Um die NTP-Ortszeit-Einstellungen zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Aktivieren und konfigurieren Sie die NTP-Ortszeit-Einstellungen, indem Sie Folgendes eingeben:

   ```
   services ntp local-clock enable stratum number
   ```

   Erläuterung:

   - *`number`* ist die Stratum-Nummer der Ortszeit
3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 16.5
Den NTP-Service aktivieren und konfigurieren

Um den NTP-Service zu aktivieren und zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***services » ntp*** und konfigurieren Sie je nach Bedarf die folgenden Parameter:

   HINWEIS
   RUGGEDCOM ROX II unterstützt sowohl IPv4- als auch IPv6-Adressen.

Parameter	Beschreibung
enabled	**Zusammenfassung:** { true, false } **Standard:** false Aktiviert NTP-Dienst.
bind-interface { bind-interface }	**Zusammenfassung:** Eine Zeichenkette Legt die IP-Adresse der ausgewählten Schnittstelle als IP-Quelladresse für ausgehende NTP-Nachrichten fest. Stellen Sie sicher, dass zuerst eine IP-Adresse der gewählten Schnittstelle zugewiesen wird. Die Schnittstelle "dummy0" sollte verwendet werden, sofern nichts anderes erforderlich ist.

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 16.6

Anzeigen des Status des NTP-Diensts

Um den Status des NTP-Dienst anzuzeigen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass der NTP-Dienst aktiviert ist. Weitere Informationen finden Sie unter Abschnitt 16.5, „Den NTP-Service aktivieren und konfigurieren“.
2. Zeigen Sie den Status des NTP-Diensts an, indem Sie Folgendes eingeben:

   ```
   services ntp ntp-status
   ```

   Eine Tabelle ähnlich dem folgenden Beispiel wird angezeigt:

   ```
   ruggedcom# services ntp ntp-status
    ntp-status
      remote           refid      st t when poll reach   delay   offset  jitter
    ==============================================================================
    *142.3.100.2     .GPS.          1 u  937 1024  377   38.104   -0.273   0.802
     172.30.149.45   .INIT.        16 u    - 1024    0    0.000    0.000   0.000
    +206.186.255.226 128.138.140.44   2 u  413 1024  377   58.578    0.143  27.963
    x206.186.255.227 CHU_AUDIO(1)     3 u  927 1024  377   58.034  10846.0  30.289
    +209.87.233.53   209.87.233.52    2 u  449 1024  377   27.060   -1.132   3.153
   ```

Diese Tabelle liefert die folgenden Informationen:

Parameter	Beschreibung
remote	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 40 Zeichen Dezentrale Adresse.
reference-id	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 40 Zeichen Die Kennung der Referenz-Uhr.
stratum	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 32 Zeichen Die Stratum-Nummer der Referenz-Uhr.
address-type	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 32 Zeichen Der Adresstyp der entfernten Maschine.
when	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 32 Zeichen Die Anzahl an Sekunden seit dem letzten Polling der Referenz-Uhr.
poll	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 32 Zeichen Das Polling-Intervall in Sekunden.
reach	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 32 Zeichen Ein linksdrehendes 8-Bit-Register. 1 Bit bedeutet immer, dass ein Zeit-Paket empfangen wurde.
delay	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 32 Zeichen Die Verzögerungszeit (in Millisekunden) für die Kommunikation mit der Referenz-Uhr.
offset	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 32 Zeichen Der Versatz (in Millisekunden) zwischen unserer Uhrzeit und der der Referenz-Uhr.
jitter	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 32 Zeichen Der beobachtete Jitter (in Millisekunden).

Ein Zeichen vor einer Adresse wird als Tally-Code bezeichnet. Tally-Codes geben das Verhalten des Peers im Uhrauswahlprozess an. Im Folgenden wird die Bedeutung aller Tally-Codes beschrieben:

Tally-Code	Beschreibung
leer	Ein leerer Tally-Code gibt an, dass der Peer verworfen wurde, da er entweder nicht erreichbar ist, über denselben Server (Sync Loop) synchronisiert wurde oder die Synchronisationsdistanz zu groß ist.
x	Dieser Tally-Code gibt an, dass der Peer verworfen wurde, da seine Uhr nicht korrekt ist. Dies wird als *Falseticker* bezeichnet.
.	Dieser Tally-Code gibt an, dass der Peer verworfen wurde, da seine Synchronisationsdistanz zu schlecht ist, um als Kandidat betrachtet zu werden.
-	Dieser Tally-Code gibt an, dass der Peer verworfen wurde, da sein Versatz im Vergleich zu den anderen Peers zu signifikant ist. Dies wird als *Outlier* bezeichnet.
+	Dieser Tally-Code gibt an, dass der Peer als Kandidat betrachtet wird.
#	Dieser Tally-Code gibt an, dass der Peer als Kandidat betrachtet wird, jedoch befindet er sich nicht unter den nach Synchronisationsdistanz sortierten obersten sechs. Wenn die Zuordnung kurzlebig ist, kann sie zum Einsparen von Ressourcen demobilisiert werden.
*	Dieser Tally-Code gibt an, dass der Peer der System-Peer ist.
o	Dieser Tally-Code gibt an, dass der Peer der System-Peer ist, seine Synchronisationsdistanz wird jedoch aus einem Pulse-Per-Second-(PPS)-Signal abgeleitet.

Abschnitt 16.7

Status der Referenzuhren anzeigen

Um den Status der Referenzuhren anzusehen, geben Sie Folgendes ein:

```
show services ntp status
```

Eine Tabelle ähnlich dem folgenden Beispiel wird angezeigt:

```
ruggedcom# show services ntp status reference-clock
                                  REFERENCE           ADDRESS
ADDRESS          STATE            ID         STRATUM  TYPE     WHEN  POLL  REACH  DELAY  OFFSET
 JITTER
-------------------------------------------------------------------------------------------------------
127.127.1.0      System peer      .LOCL.  10       l        2     64    377    0.000  0.000   0.000
206.186.255.227  Not synchronized .INIT.  16       -        -     1024  0      0.000  0.000   0.000
206.186.255.226  Not synchronized .INIT.  16       -        -     1024  0      0.000  0.000   0.000
142.3.100.2      Not synchronized .INIT.  16       -        -     1024  0      0.000  0.000   0.000
```

Diese Tabelle liefert die folgenden Informationen:

Parameter	Beschreibung
address	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 40 Zeichen IP-Adresse der Referenz-Uhr.
state	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 32 Zeichen Der Status der Uhr.
reference-id	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 40 Zeichen Die Kennung der Referenz-Uhr.
stratum	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 32 Zeichen Die Stratum-Nummer der Referenz-Uhr.
address-type	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 32 Zeichen

Parameter	Beschreibung
	Der Adresstyp der entfernten Maschine.
when	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 32 Zeichen Die Anzahl an Sekunden seit dem letzten Polling der Referenz-Uhr.
poll	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 32 Zeichen Das Polling-Intervall in Sekunden.
reach	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 32 Zeichen Ein linksdrehendes 8-Bit-Register. 1 Bit bedeutet immer, dass ein Zeit-Paket empfangen wurde.
delay	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 32 Zeichen Die Verzögerungszeit (in Millisekunden) für die Kommunikation mit der Referenz-Uhr.
offset	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 32 Zeichen Der Versatz (in Millisekunden) zwischen unserer Uhrzeit und der der Referenz-Uhr.
jitter	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 32 Zeichen Der beobachtete Jitter (in Millisekunden).

Abschnitt 16.8
NTP-Server verwalten

RUGGEDCOM ROX II kann regelmäßig die Verbindung zu einem entfernten NTP-Server aufbauen, um die entstandene Drift in der eingebauten Uhr zu korrigieren. RUGGEDCOM ROX II kann ferner über SNTP (Simple Network Time Protocol) Zeit für Hosts anbieten, die diese anfordern.

NTP-Server können mit oder ohne Authentifizierungsschlüssel hinzugefügt werden. Um einem NTP-Server einen Authentifizierungsschlüssel zuzuordnen, ist zuerst ein Serverschlüssel festzulegen. Informationen über das Hinzufügen von Serverschlüsseln finden Sie in Abschnitt 16.8.5.2, „Einen Server-Schlüssel hinzufügen“.

INHALT

- Abschnitt 16.8.1, „Eine Liste der NTP-Server anzeigen“
- Abschnitt 16.8.2, „Überwachen von Subscribern“
- Abschnitt 16.8.3, „Hinzufügen eines NTP-Servers“
- Abschnitt 16.8.4, „Einen NTP-Server löschen“
- Abschnitt 16.8.5, „Serverschlüssel verwalten“
- Abschnitt 16.8.6, „Server-Einschränkungen verwalten“

Abschnitt 16.8.1
Eine Liste der NTP-Server anzeigen

Um eine Liste der im Gerät konfigurierten NTP-Server anzusehen, geben Sie Folgendes ein:

```
show running-config services ntp server
```

Falls Server konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config services ntp server | tab
                                                                    NTP
NAME             ENABLED  PEER  MINPOLL  MAXPOLL  IBURST  VERSION  PREFER  KEY
-------------------------------------------------------------------------------
142.3.100.2      X        -     6        10       -       -        X       -
206.186.255.226  X        -     6        10       -       -        -       -
206.186.255.227  X        -     6        10       -       -        -       -

!
!
```

Falls keine Server konfiguriert wurden, fügen Sie je nach Bedarf Server hinzu. Weitere Informationen finden Sie unter Abschnitt 16.8.3, „Hinzufügen eines NTP-Servers“.

Abschnitt 16.8.2

Überwachen von Subscribern

Der RUGGEDCOM ROX II überwacht das Abonnement von bis zu 600 Hosts (z. B. Clients, Server und Peers), die mit dem NTP-Server verbunden sind.

Um die Liste der Subscriber-Hosts anzuzeigen, geben Sie Folgendes ein:

```
show services ntp status monitor-list
```

Wenn Hosts gefunden wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show services ntp status monitor-list | tab
                                                                    AVERAGE   LAST
 REMOTE         PORT  COUNT  MODE  VERSION  RESTRICT                 INTERVAL  INTERVAL
 ------------------------------------------------------------------------------------------
 192.168.0.1    123   2      3     4        [ nomodify nopeer noquery notrap ]  447       887
 192.168.0.2    123   1      3     4        [ nomodify nopeer noquery notrap ]  885       885
 192.168.0.3    123   1      3     4        [ nomodify nopeer noquery notrap ]  883       883
 192.168.0.4    123   1      3     4        [ nomodify nopeer noquery notrap ]  881       881
 192.168.1.1    123   1      3     4        [ nomodify nopeer noquery notrap ]  862       862
 192.168.1.3    123   1      3     4        [ nomodify nopeer noquery notrap ]  854       854
 192.168.1.8    123   1      3     4        [ nomodify nopeer noquery notrap ]  850       850
 192.168.2.1    123   1      4     4        [ nomodify nopeer noquery notrap ]  837       837
 192.168.2.4    123   1      4     4        [ nomodify nopeer noquery notrap ]  834       834
 192.168.2.10   123   1      4     4        [ nomodify nopeer noquery notrap ]  830       830
 192.168.3.3    123   1      1     4        [ nomodify nopeer noquery notrap ]  823       823
 192.168.3.7    123   1      1     4        [ nomodify nopeer noquery notrap ]  816       816
 192.168.3.9    123   1      1     4        [ nomodify nopeer noquery notrap ]  813       813
```

Die Tabelle/Liste enthält folgende Informationen:

Parameter	Beschreibung
remote	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 40 Zeichen Dezentrale Adresse.
port	**Zusammenfassung:** Eine vorzeichenbehaftete 16-Bit-Ganzzahl UDP-Portnummer.
count	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl Anzahl der empfangenen Pakete.
mode	**Zusammenfassung:** Eine vorzeichenbehaftete 8-Bit-Ganzzahl Modus des letzten Pakets.

Parameter	Beschreibung
version	**Zusammenfassung:** Eine vorzeichenbehaftete 8-Bit-Ganzzahl Version des letzten Pakets.
restrict	**Zusammenfassung:** { ignore, kod, limited, lowpriotrap, nomodify, nopeer, noquery, noserve, notrap, notrust, ntpport, version } Flags einschränken.
average-interval	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl Durchschnittliches Intervall (in Sekunden) zwischen Paketen von dieser Adresse.
last-interval	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl Intervall (in Sekunden) zwischen dem Empfang des letzten Pakets von dieser Adresse und dem Abschluss der Statusabfrage.

Abschnitt 16.8.3

Hinzufügen eines NTP-Servers

Um einen NTP-Server auf dem Gerät zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. [Optional] Wenn die Kommunikation mit dem Server authentifiziert werden soll, fügen Sie einen Server-Authentifizierungsschlüssel hinzu oder stellen sicher, dass der erforderliche Schlüssel konfiguriert wurde. Weitere Informationen finden Sie unter Abschnitt 16.8.5, „Serverschlüssel verwalten“.
3. Navigieren Sie zu ***services » ntp » server*** und konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

HINWEIS
RUGGEDCOM ROX II unterstützt sowohl IPv4- als auch IPv6-Adressen.

Parameter	Beschreibung
{ name }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 253 Zeichen Die zu überwachende Internetadresse des entfernten NTP-Servers.
enabled	Schaltet die NTP-Schnittstelle zu diesem Server ein.
peer	Ermöglicht Ihnen, Peers einzugeben und zu bearbeiten. Peers sind NTP-Server desselben Stratums wie der Router und sind nützlich, wenn der Kontakt zu den Hosts im NTP-Server-Menü verloren geht.
minpoll { minpoll }	**Zusammenfassung:** Eine vorzeichenlose 8-Bit-Ganzzahl zwischen 4 und 17 **Standard:** 6 Das kleinste Polling-Intervall für NTP-Nachrichten, in Sekunden als Zweierpotenz. **HINWEIS** *"minpoll" muss <= "maxpoll" sein*
maxpoll { maxpoll }	**Zusammenfassung:** Eine vorzeichenlose 8-Bit-Ganzzahl zwischen 4 und 17 **Standard:** 10 Das größte Polling-Intervall für NTP-Nachrichten, in Sekunden als Zweierpotenz.

Parameter	Beschreibung
	HINWEIS *"minpoll" muss <= "maxpoll" sein*
iburst	Wenn der Server nicht erreichbar ist und bei jedem Poll-Intervall wird ein Burst von acht Paketen anstelle von einem gesendet.
ntp-version { ntp-version }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 1 und 4 Die Version des NTP-Protokolls, das verwendet wird, um mit diesem Host zu kommunizieren. Ändern Sie diese nur, wenn bekannt ist, dass der Host eine andere Version als Version 4 erfordert.
prefer	Kennzeichnet diesen Server als bevorrechtigt.
key { key }	**Zusammenfassung:** Eine Zeichenkette Ein mit diesem Host verbundener Authentifizierungsschlüssel.

4. [Optional] Legen Sie Einschränkungen fest, um zu kontrollieren, auf welche NTP-Dienste auf dem Server zugegriffen werden kann. Weitere Informationen finden Sie unter Abschnitt 16.8.6.2, „Hinzufügen einer Servereinschränkung“.
5. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 16.8.4

Einen NTP-Server löschen

Um einen auf dem Gerät konfigurierten NTP-Server zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den NTP-Server, indem Sie Folgendes eingeben:

   ```
   no services ntp server IP Address
   ```

   Erläuterung:

   - *`IP Address`* ist die interne Adresse des entfernten NTP-Servers
3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 16.8.5

Serverschlüssel verwalten

Serverschlüssel dienen zur Authentifizierung von NTP-Kommunikation und zur Verhinderung der Verfälschung von NTP-Zeitstempeln. Wird die Authentifizierung verwendet, müssen die lokalen und entfernten Server den gleichen Schlüssel und die gleiche Schlüsselkennung besitzen. Pakete, die an den Server/Peer gesendet bzw. von diesem empfangen werden, enthalten Authentifizierungsfelder, die mit dem Schlüssel verschlüsselt sind.

INHALT

- Abschnitt 16.8.5.1, „Eine Liste der Serverschlüssel anzeigen“

- Abschnitt 16.8.5.2, „Einen Server-Schlüssel hinzufügen“
- Abschnitt 16.8.5.3, „Einen Server-Schlüssel löschen“

Abschnitt 16.8.5.1
Eine Liste der Serverschlüssel anzeigen

Um eine Liste der Serverschlüssel anzusehen, geben Sie Folgendes ein:

```
show running-config services ntp key
```

Falls Schlüssel konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config services ntp key
services
 ntp
  key 1
   value   $4$87sRT/Z+sxs9hYYI0d4IDw==
   trusted
  !
 !
!
```

Falls keine Serverschlüssel konfiguriert wurden, fügen Sie je nach Bedarf Schlüssel hinzu. Weitere Informationen finden Sie unter Abschnitt 16.8.5.2, „Einen Server-Schlüssel hinzufügen“.

Abschnitt 16.8.5.2
Einen Server-Schlüssel hinzufügen

Um einen Server-Schlüssel hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie den Schlüssel hinzu, indem Sie Folgendes eingeben:

   ```
   services ntp key id
   ```

   Erläuterung:

   - *id* ist die dem Schlüssel zugewiesene ID
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
value { value }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 1024 Zeichen Der Schlüssel. Dieser Parameter ist obligatorisch.
trusted	Diesen Schlüssel als vertrauenswürdig für die Authentifizierung von Peers mit symmetrischer Schlüsselkryptographie markieren. Das Authentifizierungsverfahren setzt voraus, dass sowohl die lokalen als auch die entfernten Server den gleichen Schlüssel und Schlüssel-Identifier besitzen.

4. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 16.8.5.3
Einen Server-Schlüssel löschen

Um einen Server-Schlüssel zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie den ausgewählten Schlüssel durch Eingabe von:

   ```
   no services ntp key id
   ```

   Erläuterung:

   - *id* ist die dem Schlüssel zugewiesene ID
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 16.8.6
Server-Einschränkungen verwalten

Mit Server-Einschränkungen wird der Zugang zu den NTP-Servern kontrolliert.

INHALT

- Abschnitt 16.8.6.1, „Eine Liste der Servereinschränkungen anzeigen“
- Abschnitt 16.8.6.2, „Hinzufügen einer Servereinschränkung“
- Abschnitt 16.8.6.3, „Eine Servereinschränkung löschen“

Abschnitt 16.8.6.1
Eine Liste der Servereinschränkungen anzeigen

Um eine Liste der NTP-Servereinschränkungen anzusehen, geben Sie Folgendes ein:

```
show running-config services ntp restrict
```

Falls Einschränkungen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config services ntp restrict | tab
NAME       MASK     FLAGS
---------------------------
127.0.0.1  default  -

 !
!
```

Falls keine Einschränkungen konfiguriert wurden, fügen Sie je nach Bedarf Einschränkungen hinzu. Weitere Informationen finden Sie unter Abschnitt 16.8.6.2, „Hinzufügen einer Servereinschränkung“.

Abschnitt 16.8.6.2
Hinzufügen einer Servereinschränkung

Um eine Einschränkung des NTP-Servers hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie die Einschränkung hinzu, indem Sie Folgendes eingeben:

```
services ntp restrict address mask
```

   Erläuterung:

   - *address* ist die passende IP-Adresse. Die Adresse kann ein Host, eine Netzwerk-IP-Adresse oder ein gültiger DNS-Name des Hosts sein.
   - *mask* ist die Maske, die verwendet wird, um die Adresse zuzuordnen. Ein Wert von 255.255.255.255 besagt, dass die Adresse als die Adresse eines einzelnen Hosts behandelt wird.

3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

   ACHTUNG!
   Sicherheitsgefahr – Risiko des unbefugten Zugriffs und/oder Missbrauchs. Es wird empfohlen, Anfragen über ntpdc und ntpq einzuschränken, sofern die Anfragen nicht von einem lokalen Host kommen, oder diese Funktion komplett zu deaktivieren, falls sie nicht benötigt wird. Dies verhindert DDoS-(Distributed Denial of Service)-Reflection/Amplification-Angriffe. Um diese Einschränkung einzustellen, konfigurieren Sie die folgenden Merker: kod, nomodify, nopeer, noquery und notrap.

Parameter	Beschreibung
flags { flags }	**Zusammenfassung:** { ignore, kod, limited, lowpriotrap, nomodify, nopeer, noquery, noserve, notrap, notrust, ntpport, version } Kennzeichnet eingeschränkten Zugang zu NTP-Diensten. Ein Eintrag ohne Flags gewährt freien Zugang zum NTP-Server. • Version: Weist Pakete ab, die nicht mit der aktuellen NTP-Version übereinstimmen. • ntpport: Ordnet nur dann zu, wenn der Quellport im Paket der Standard-NTP-UDP-Port (123) ist. • notrust: Verweigert Dienst, sofern das Paket nicht kryptografisch authentifiziert ist. • notrap: Lehnt es ab, für übereinstimmende Hosts den Trap-Dienst für Steuernachrichten im Modus 6 ("mode 6 control message trap service") zur Verfügung zu stellen. • noserve: Weist alle Pakete ab, außer ntpq(8)- und ntpdc(8)-Abfragen. • noquery: Weist ntpq(8)- und ntpdc(8)-Abfragen ab. • nopeer: Weist Pakete ab, die zur Entstehung einer neuen Zuordnung führen. • nomodify: Weist ntpq(8)- und ntpdc(8)-Abfragen ab und versucht, den Server-Status zu verändern; Abfragen, die Informationen liefern, sind zulässig. • lowpriotrap: Bestimmt, dass Traps, die von passenden Hosts gesetzt wurden, niedrige Priorität haben. • limited: Verweigert den Dienst, wenn der Paketabstand die in der NTP-Verwerfen-Einstellung angegebenen unteren Grenzwerte überschreitet. • kod: Sendet ein Kiss-o'-Death Packet (KoD), wenn ein Zugriff verletzt wird. • ignore: Weist alle Pakete ab.

4. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 16.8.6.3
Eine Servereinschränkung löschen

Um eine Einschränkung des NTP-Servers zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die Einschränkung, indem Sie Folgendes eingeben:

   ```
   no services ntp restrict address mask
   ```

   Erläuterung:

   - *address* ist die passende IP-Adresse. Die Adresse kann ein Host, eine Netzwerk-IP-Adresse oder ein gültiger DNS-Name des Hosts sein.
   - *mask* ist die Maske, die verwendet wird, um die Adresse zuzuordnen. Ein Wert von 255.255.255.255 besagt, dass die Adresse als die Adresse eines einzelnen Hosts behandelt wird.
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 16.9

NTP-Broadcast-/Multicast-Clients verwalten

Setzen Sie das Gerät in den NTP-Broadcast- oder Multicast-Client-Modus, wenn der NTP-Server regelmäßige Mitteilungen zu einer bestimmten Uhrzeit generiert.

INHALT

- Abschnitt 16.9.1, „NTP-Multicast-Clients aktivieren und konfigurieren“
- Abschnitt 16.9.2, „NTP-Broadcast-Clients aktivieren und konfigurieren“
- Abschnitt 16.9.3, „NTP-Broadcast-/Multicast-Adressen verwalten“

Abschnitt 16.9.1

NTP-Multicast-Clients aktivieren und konfigurieren

Der NTP-Multicast-Client ermöglicht es dem NTP-Server, Ankündigungen von anderen NTP-Servern zu empfangen.

Um den NTP-Multicast-Client zu aktivieren und zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***services » ntp » multicastclient*** und konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
enabled	Aktiviert den Multicast-Nachrichten-Modus.
address { address }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 253 Zeichen **Standard:** 224.0.1.1 Die Multicast-Adresse, an der der NTP-Client NTP-Nachrichten empfängt.

3. Fügen Sie eine Multicast-Adresse für einen bekannten NTP-Server hinzu. Für weitere Informationen siehe Abschnitt 16.9.3.2, „Eine Broadcast-/Multicast-Adresse hinzufügen“.
4. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 16.9.2
NTP-Broadcast-Clients aktivieren und konfigurieren

Der NTP-Broadcast-Client ermöglicht es dem NTP-Server, Ankündigungen von anderen NTP-Servern zu empfangen und eigene Ankündigungen zu versenden.

Um den NTP-Broadcast-Client zu aktivieren und zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Navigieren Sie zu ***services » time » ntp***.
3. Konfigurieren Sie je nach Bedarf die folgenden Parameter:

Parameter	Beschreibung
broadcastclient	Aktiviert/deaktiviert den Broadcast-Client.

4. Fügen Sie eine Broadcast-Adresse für einen bekannten NTP-Server hinzu. Für weitere Informationen siehe Abschnitt 16.9.3.2, „Eine Broadcast-/Multicast-Adresse hinzufügen“.
5. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 16.9.3
NTP-Broadcast-/Multicast-Adressen verwalten

Sind Broadcast- oder Multicast-Adressen für bekannte NTP-Server konfiguriert, überwacht der NTP-Daemon die Mitteilungen von jeder Adresse und wählt den Server mit dem niedrigsten Stratum als NTP-Host aus. Dies ist das Gegenstück zur manuellen Konfigurierung einer Server- oder Peer-Liste.

INHALT

- Abschnitt 16.9.3.1, „Eine Liste der Broadcast-/Multicast-Adressen anzeigen“
- Abschnitt 16.9.3.2, „Eine Broadcast-/Multicast-Adresse hinzufügen“
- Abschnitt 16.9.3.3, „Eine Broadcast-/Multicast-Adresse löschen“

Abschnitt 16.9.3.1
Eine Liste der Broadcast-/Multicast-Adressen anzeigen

Um eine Liste der Broadcast-/Multicast-Adressen anzusehen, geben Sie Folgendes ein:

```
show running-config services ntp broadcast
```

Falls Adressen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config services ntp broadcast
services
 ntp
  broadcast 224.0.0.1
   no enabled
   key 1
   no ntp-version
  !
 !
```

```
!
```

Falls keine Broadcast-/Multicast-Adressen konfiguriert wurden, fügen Sie je nach Bedarf Adressen hinzu. Weitere Informationen finden Sie unter Abschnitt 16.9.3.2, „Eine Broadcast-/Multicast-Adresse hinzufügen“.

Abschnitt 16.9.3.2
Eine Broadcast-/Multicast-Adresse hinzufügen

Um eine Broadcast-/Multicast-Adresse für einen NTP-Server hinzuzufügen, gehen Sie wie folgt vor:

WICHTIG!
Die Aktivierung der NTP-Authentifizierung wird dringend empfohlen, sofern nicht alle Hosts im Netzwerk vertrauenswürdig sind.

1. Stellen Sie sicher, dass ein Server-Schlüssel über die Broadcast-/Multicast-Einstellung konfiguriert wurde, um die NTP-Authentifizierung zu aktivieren. Weitere Informationen finden Sie unter Abschnitt 16.8.5.2, „Einen Server-Schlüssel hinzufügen“.
2. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
3. Fügen Sie die Adresse hinzu, indem Sie Folgendes eingeben:

   WICHTIG!
   Die Broadcast-/Multicast-Adresse muss mit der Adresse für den NTP-Multicast-Client übereinstimmen.

   ```
   services ntp broadcast address
   ```

   Erläuterung:

   - *address* ist die Broadcast- oder Multicast-Adresse
4. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
enabled	Aktiviert das Senden von Broadcast- oder Multicast-NTP-Nachrichten an diese Adresse.
key { key }	**Zusammenfassung:** Eine Zeichenkette Authentifizierungsschlüssel.
ntp-version { ntp-version }	**Zusammenfassung:** Eine vorzeichenbehaftete 32-Bit-Ganzzahl zwischen 1 und 4 Die Version des NTP-Protokolls, das verwendet wird, um mit diesem Host zu kommunizieren. Ändern Sie diese nur, wenn bekannt ist, dass der Host eine andere Version als Version 4 erfordert.
ttl { ttl }	**Zusammenfassung:** Eine vorzeichenlose 8-Bit-Ganzzahl zwischen 1 und 127 **Standard:** 1 Lebenszeit (TTL).

5. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 16.9.3.3
Eine Broadcast-/Multicast-Adresse löschen

Um eine Broadcast-/Multicast-Adresse für einen NTP-Server zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die Einschränkung, indem Sie Folgendes eingeben:

   ```
   no services ntp broadcast address
   ```

   Erläuterung:

   - *address* ist die Broadcast- oder Multicast-Adresse
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

17 Virtualisierung

RUGGEDCOM ROX II unterstützt Kernel-basierte Virtualisierungssysteme auf dem RUGGEDCOM RX1400.

Die Virtual Processing Engine (VPE) stellt eine Linux-basierte Plattform zur Verwendung von Anwendungen von Fremdanbietern bereit, ohne dass sich diese Verwendung auf die auf dem System laufenden RUGGEDCOM RX1400-Kerndienste auswirkt. Die Virtualisierung erlaubt es, ein vollständiges Linux-Image (mit eigenen Speichermedien und E/A-Ports) parallel zum RUGGEDCOM ROX II laufen zu lassen, wobei eine KVM-(Kernel Virtual Machine)-basierte Lösung zum Einsatz kommt.

Eine Frontend-Management-Schnittstelle wird zur Nutzung und Konfiguration virtueller Maschinen hinzugefügt. Nach der Installation und Konfiguration können Benutzer ein Linux-basiertes Gastbetriebssystem laden und Anwendungen von Drittanbietern zusätzlich zum Image installieren. Anwendungen von Fremdanbietern haben je nach Konfiguration Zugriff auf Netzwerk- und serielle Schnittstellen auf dem System.

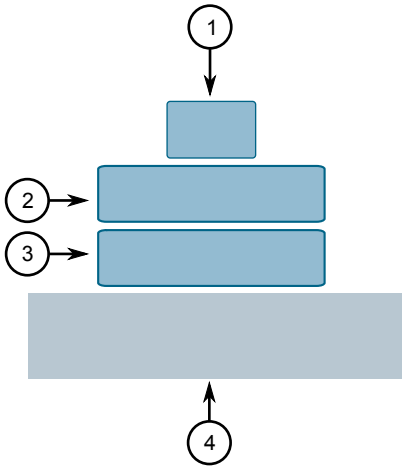


Abbildung 29: System-Blockschaltplan

1. Apps **2.** Gast-Linux-Kernel **3.** QEMU **4.** ROXII-Linux-Kernel-ARM

WICHTIG!
Images virtueller Maschinen müssen vom microSD/microSDHC-Speicher aus ausgeführt werden. Weitere Informationen finden Sie unter Abschnitt 1.1, „Produktmerkmale und Vorteile“.

HINWEIS
Es können mehrere virtuelle Maschinen installiert werden, jedoch kann jeweils nur eine virtuelle Maschine ausgeführt werden.

Als Unterstützung bei der Verwendung großer Images virtueller Maschinen, setzt das VPE-Setup voraus, dass Linux OS und Anwendungen in einer .tar.gz-Datei komprimiert werden. Diese Datei wird auf eine microSD-Karte übertragen, die anschließend im RUGGEDCOM RX1400 installiert wird. Der RUGGEDCOM ROX II-

Virtualisierungsdienst setzt die microSD-Karte ein, extrahiert die Image-Datei und verwendet diese als Dateisystem für das Linux-OS und Anwendungen.

INHALT

- Abschnitt 17.1, „Virtualisierung konfigurieren“
- Abschnitt 17.2, „Eine Imagedatei für eine virtuelle Maschine aufbauen/abrufen“
- Abschnitt 17.3, „Den Virtualisierungsdienst aktivieren oder deaktivieren“
- Abschnitt 17.4, „Die aktive virtuelle Maschine bestimmen“
- Abschnitt 17.5, „Globale Einstellungen konfigurieren“
- Abschnitt 17.6, „Eine Liste von Namen virtueller Maschinen anzeigen“
- Abschnitt 17.7, „Hinzufügen einer virtuellen Maschine“
- Abschnitt 17.8, „Ein Archiv der virtuellen Maschine extrahieren“
- Abschnitt 17.9, „Image einer vorhandenen virtuellen Maschine laden“
- Abschnitt 17.10, „Eine virtuelle Maschine löschen“
- Abschnitt 17.11, „Ein Archiv der virtuellen Maschine löschen“
- Abschnitt 17.12, „Eine virtuelle Maschine starten“
- Abschnitt 17.13, „Eine virtuelle Maschine stoppen“
- Abschnitt 17.14, „VM-Befehle absetzen“
- Abschnitt 17.15, „Zuweisen eines seriellen Ports“
- Abschnitt 17.16, „Zuordnung eines seriellen Ports löschen“
- Abschnitt 17.17, „Die VPE-Netzwerkschnittstelle aktivieren/deaktivieren“
- Abschnitt 17.18, „Eine virtuelle Schnittstelle hinzufügen“
- Abschnitt 17.19, „Eine virtuelle Schnittstelle löschen“
- Abschnitt 17.20, „Zuweisen einer Netzwerkschnittstelle“
- Abschnitt 17.21, „Auf die aktive virtuelle Maschine zugreifen“
- Abschnitt 17.22, „Abfragen der Seriennummer des Geräts“

Abschnitt 17.1

Virtualisierung konfigurieren

Um auf dem RUGGEDCOM RX1400 eine virtuelle Maschine zu konfigurieren, führen Sie die folgenden grundlegenden Schritte durch:

1. Aktivieren Sie den RUGGEDCOM ROX II Virtualisierungsservice.
2. Konfigurieren Sie die globalen Einstellungen für den Virtualisierungsservice.
3. Fügen Sie das Image der virtuellen Maschine hinzu und extrahieren Sie es.
4. Konfigurieren Sie die Netzwerkschnittstelle.
5. Starten Sie das Image der virtuellen Maschine.

Sobald die virtuelle Maschine gestartet ist, kann erstmals über die Konsole auf sie zugegriffen werden.

Abschnitt 17.2

Eine Imagedatei für eine virtuelle Maschine aufbauen/abrufen

Detaillierte Anweisungen zum Erstellen der Linux-Imagedatei .tar.gz sind in Building a Linux-Based Virtual Machine Image [https://support.industry.siemens.com/cs/ww/en/view/109482423] beschrieben.

Alternativ sind von Siemens Linux Debian 8 Imagedateien auf Wunsch über das Support-Portal mit Dateigrößen 1 GB und 3,5 GB erhältlich. Jede dieser Imagedateien lässt sich problemlos auf eine FAT32-formatierte SD Card extrahieren und dann über einen Windows PC übertragen. Wird eine größere Imagedatei erstellt und die extrahierte Dateigröße ist > 4 GB, sind eine EXT4-formatierte Karte sowie ein Linux-PC für die Formatierung und Übertragung erforderlich.

Abschnitt 17.3

Den Virtualisierungsdienst aktivieren oder deaktivieren

Um den Virtualisierungsdienst zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

HINWEIS
Ein vorkonfiguriertes Image einer virtuellen Maschine für Debian 8.0 (Jessie) ist auf Anfrage bei Siemens erhältlich. Für weitere Informationen wenden Sie sich bitte an den Siemens-Kundensupport.

1. Stecken Sie den microSD/microSDHC-Speicher mit dem Image der virtuellen Maschine in den microSD/microSDHC-Steckplatz. Ausführliche Informationen hierzu finden Sie im *RUGGEDCOM RX1400 Installationsleitfaden*.
2. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
3. Aktivieren oder deaktivieren Sie den Virtualisierungsdienst, indem Sie Folgendes eingeben:

   ```
   services virtualization enabled [ true | false ]
   ```

   Erläuterung:

   - *true* aktiviert den Virtualisierungsdienst
   - *false* deaktiviert den Virtualisierungsdienst
4. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 17.4

Die aktive virtuelle Maschine bestimmen

Um festzustellen, welche virtuelle Maschine aktiv ist, geben Sie Folgendes ein:

```
show services virtualization status
```

Wurde eine virtuelle Maschine aktiviert, erscheint eine Liste ähnlich dem folgenden Beispiel:

```
ruggedcom# show services virtualization status
status
 active-guest
  name   linux1
  pid    28579
  state  Started
  status Normal
```

HINWEIS
*Die aktive virtuelle Maschine wird als **active guest** bezeichnet.*

Diese Liste zeigt folgende Informationen:

Parameter	Beschreibung
name	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 64 Zeichen Der Name des aktiven Gasts. Dieser Parameter ist obligatorisch.
pid	**Zusammenfassung:** Eine Zeichenkette Die Prozess-ID des aktiven Gasts.
state	**Zusammenfassung:** Eine Zeichenkette Der Status des aktiven Gasts, wie z. B. "started", "stopped", "failed" oder "no reply". Dieser Parameter ist obligatorisch.
status	**Zusammenfassung:** Eine Zeichenkette Der Status des aktiven Gasts. Dieser Parameter ist obligatorisch.

Abschnitt 17.5

Globale Einstellungen konfigurieren

Um die globalen Einstellungen zu konfigurieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Konfigurieren Sie die globalen Einstellungen, indem Sie Folgendes eingeben:

   ```
   services virtualization virtual-machines basic-parameters cpu cpu machine machine memory memory
   auto-start auto-start
   ```

   Erläuterung:

   - *cpu* ist der zu emulierende CPU-Typ.
   - *machine* ist der zu emulierende Maschinentyp.
   - *memory* ist die Speicherzuordnung, in MB. Die Zuordnung kann jeden Wert zwischen 200 und 512 MB haben.
   - *auto-start* ist die Bezeichnung der virtuellen Maschine, die bei System-Neustart startet.
3. Weisen Sie einen oder mehrere serielle Ports dem Virtualisierungsdienst zu. Für weitere Informationen siehe Abschnitt 17.15, „Zuweisen eines seriellen Ports“.
4. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 17.6

Eine Liste von Namen virtueller Maschinen anzeigen

Um eine Liste der installierten virtuellen Maschinen anzusehen, geben Sie Folgendes ein:

```
show running-config services virtualization virtual-machines
```

Falls Gruppen konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config services virtualization virtual-machines linux-guests | tab
        LINUX                   LINUX
NAME    ARCHIVE       ARCHIVE   IMAGE      LINUX KERNEL                DEVICE TREE                INIT
 RAM DISK
-------------------------------------------------------------------------------------------------------------
linux1  demo2.tar.gz  tar.gz    linux.img  vmlinuz-3.16.0-4-armmp.knl  vexpress-v2p-ca15-tc1.dtb
 initrd.img.ird

 !
!
```

Falls keine virtuellen Maschinen konfiguriert wurden, fügen Sie je nach Bedarf Images hinzu. Weitere Informationen finden Sie unter Abschnitt 17.7, „Hinzufügen einer virtuellen Maschine“.

Abschnitt 17.7

Hinzufügen einer virtuellen Maschine

Benutzer können RUGGEDCOM ROX II eine virtuelle Maschine mithilfe einer microSD-Karte hinzufügen, auf der das Image der virtuellen Maschine gespeichert ist.

WICHTIG!
Beachten Sie beim Erstellen eines Images einer virtuellen Maschine folgende Voraussetzungen:

- *Es müssen mindestens ein Benutzerprofil und -passwort konfiguriert sein, um das Image der virtuellen Maschine zu erstellen. Dies wird für den Zugriff auf die virtuelle Maschine über den RUGGEDCOM ROX II vorausgesetzt. Weitere Informationen über das Zugreifen auf die virtuelle Maschine nach erfolgter Installation und Aktivierung finden Sie in Abschnitt 17.21, „Auf die aktive virtuelle Maschine zugreifen“.*
- *Jedes Image einer virtuellen Maschine muss in eine der folgenden TAR-Archiv-Dateiformate komprimiert werden: *.tar, *.tar.gz oder *.tar.bz2.*
- *Jedes Archiv der virtuellen Maschine muss folgende Dateien enthalten: die Initial-RAM-Disk-(initrd)-Datei (falls vom Image benötigt), eine Linux-Image-Datei (*.img), eine Linux-Kernel-Datei (*.knl), eine Device-Tree-Datei (*.dtb) und eine Manifestdatei (*vmconfig.txt).*

Um eine virtuelle Maschine hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass das Image der virtuellen Maschine auf dem Gerät installiert ist. Weitere Informationen finden Sie unter Abschnitt 4.12.1, „Installieren von Dateien“.
2. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
3. Fügen Sie die virtuelle Maschine hinzu, indem Sie Folgendes eingeben:

   ```
   services virtualization virtual-machines linux-guests name
   ```

Erläuterung:

- *name* ist die Bezeichnung der virtuellen Maschine, die hinzugefügt werden soll.

> **HINWEIS**
> *Wenn ein Image mit derselben Bezeichnung im Dateisystem bereits vorhanden ist, wird der Benutzer aufgefordert, das Image im Dateisystem entweder zu überschreiben oder das vorhandene Image zu laden. Für weitere Informationen siehe Abschnitt 17.8, „Ein Archiv der virtuellen Maschine extrahieren“ oder Abschnitt 17.9, „Image einer vorhandenen virtuellen Maschine laden“.*

4. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern.

Abschnitt 17.8

Ein Archiv der virtuellen Maschine extrahieren

> **HINWEIS**
> *Der Extraktionsvorgang kann mehrere Minuten dauern.*

> **WICHTIG!**
> *Extrahieren Sie kein Archiv für die aktive virtuelle Maschine.*

Um ein Archiv der virtuellen Maschine zu extrahieren, gehen Sie wie folgt vor.

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Stellen Sie fest, welche virtuelle Maschine aktiv ist. Weitere Informationen finden Sie unter Abschnitt 17.4, „Die aktive virtuelle Maschine bestimmen“.
3. Falls die virtuelle Maschine aktiv ist, stoppen Sie die Maschine. Weitere Informationen finden Sie unter Abschnitt 17.13, „Eine virtuelle Maschine stoppen“.
4. Extrahieren Sie ein Archiv der virtuellen Maschine, indem Sie Folgendes eingeben:

```
services virtualization vm-extract-archive vm-name name archive-name archive
```

Erläuterung:

- *name* ist die Bezeichnung der virtuellen Maschine
- *archive* ist die Bezeichnung der Archivdatei, die extrahiert werden soll

5. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 17.9

Image einer vorhandenen virtuellen Maschine laden

Ein Benutzer kann ein Image einer vorhandenen virtuellen Maschine aus dem Dateisystem laden.

Um ein Image einer vorhandenen virtuellen Maschine zu laden, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Laden Sie das Image einer virtuellen Maschine durch Eingabe von:

   ```
   services virtualization vm-load-image vm-name name
   ```

   Erläuterung:

   - *name* ist die Bezeichnung der virtuellen Maschine
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 17.10

Eine virtuelle Maschine löschen

Um eine virtuelle Maschine zu löschen, gehen Sie wie folgt vor:



WICHTIG!
Beim Löschen einer virtuellen Maschine wird das Image aus RUGGEDCOM ROX II und dem microSD/microSDHC-Laufwerk entfernt.

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Stellen Sie fest, welche virtuelle Maschine aktiv ist. Weitere Informationen finden Sie unter Abschnitt 17.4, „Die aktive virtuelle Maschine bestimmen“.
3. Falls die virtuelle Maschine aktiv ist, stoppen Sie die Maschine. Weitere Informationen finden Sie unter Abschnitt 17.13, „Eine virtuelle Maschine stoppen“.
4. Löschen Sie die virtuelle Maschine, indem Sie Folgendes eingeben:

   ```
   no services virtualization virtual-machines linux-guests name
   ```

   Erläuterung:

   - *name* ist die Bezeichnung der virtuellen Maschine, die gelöscht werden soll.
5. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 17.11

Ein Archiv der virtuellen Maschine löschen

Um ein Archiv der virtuellen Maschine zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie ein Archiv der virtuellen Maschine durch Eingabe von:

   ```
   services virtualization vm-delete-archive archive-name name
   ```

   Erläuterung:

   - *name* ist die Bezeichnung der Archivdatei, die gelöscht werden soll

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 17.12
Eine virtuelle Maschine starten

Um eine virtuelle Maschine zu starten, gehen Sie wie folgt vor:

1. Starten Sie die virtuelle Maschine durch Eingabe von:

   ```
   services virtualization vm-start name console-wait [ true | false ]
   ```

   Erläuterung:

   - *`name`* ist die Bezeichnung der virtuellen Maschine
   - *`console-wait`* ist ein optionaler Parameter. Ist er auf "True" gesetzt, wartet die virtuelle Maschine auf eine Konsolenverbindung, bevor sie startet. Der Standardwert ist "False".
2. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 17.13
Eine virtuelle Maschine stoppen

Um eine virtuelle Maschine zu stoppen, gehen Sie wie folgt vor:

1. Melden Sie sich an der aktiven virtuellen Maschine an. Weitere Informationen finden Sie unter Abschnitt 17.21, „Auf die aktive virtuelle Maschine zugreifen“.
2. Fahren Sie die aktive virtuelle Maschine durch Eingabe eines entsprechenden Linux-Befehls (z. B. *poweroff*) herunter.

Abschnitt 17.14
VM-Befehle absetzen

Um einen Befehl für eine virtuelle Maschine abzusetzen, gehen Sie wie folgt vor:

1. Um einen Befehl für eine virtuelle Maschine abzusetzen, geben Sie Folgendes ein:

   ```
   services virtualization vm-command cmd [ kill | quit | status | stop ]
   ```

   Erläuterung:

   - `kill` beendet den Prozess in der virtuellen Maschine zwangsweise
   - `quit` beendet den Prozess vom Host systematisch
   - `status` fragt den Status des Quick Emulator ab
   - `stop` versetzt die virtuelle Maschine in eine Pause
2. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 17.15
Zuweisen eines seriellen Ports

Die seriellen Ports werden innerhalb der virtuellen Maschine wie folgt zugeordnet:

- Port 1: /dev/ttyAMA1
- Port 2: /dev/ttyAMA2

Um einen seriellen Port zuzuweisen, gehen Sie wie folgt vor:

WICHTIG!
Wenn serielle Ports dem Dienst der virtuellen Maschine zugewiesen werden, dann sind sie dem Dienst fest zugeordnet und können vom RUGGEDCOM ROX II nicht zu anderen Zwecken verwendet werden.

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Legen Sie ein Protokoll für den gewünschten seriellen Port fest. Weitere Informationen finden Sie unter Abschnitt 9.2.3, „Hinzufügen eines Protokolls des seriellen Ports“.
3. Weisen Sie einen seriellen Port zu, indem Sie Folgendes eingeben:

   ```
   services virtualization virtual-machines basic-parameters serials serial-port
   ```

   Erläuterung:

   - *serial-port* der serielle Port der Host-Schnittstelle, umgeleitet zur virtuellen Maschine
4. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 17.16
Zuordnung eines seriellen Ports löschen

Um die Zuordnung eines seriellen Ports zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die Zuordnung des ausgewählten seriellen Ports durch Eingabe von:

   ```
   no services virtualization virtual-machines basic-parameters serials serial-port
   ```

   Erläuterung:

   - *serial-port* ist der serielle Schnittstellenport des Hosts für das ttyAMA-Gerät
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 17.17
Die VPE-Netzwerkschnittstelle aktivieren/deaktivieren

Die VPE-Netzwerkschnittstelle muss aktiviert sein, um den Netzwerkzugriff für virtuelle Maschinen zuzulassen.

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Aktivieren oder deaktivieren Sie die VPE-Netzwerkschnittstelle, indem Sie Folgendes eingeben:

   Aktivieren

   ```
   interface VPE name enabled
   ```

   Erläuterung:

   - *name* ist die Bezeichnung der emulierten Netzwerkschnittstelle

   Deaktivieren

   ```
   no interface VPE name enabled
   ```

   Erläuterung:

   - *name* ist die Bezeichnung der emulierten Netzwerkschnittstelle
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 17.18
Eine virtuelle Schnittstelle hinzufügen

Die Benutzer können bis zu drei Netzwerkschnittstellen hinzufügen, um den virtuellen Prozessor zu unterstützen.

Um eine virtuelle Schnittstelle hinzuzufügen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass das Image der virtuellen Maschine auf dem Gerät installiert ist. Für weitere Informationen siehe Abschnitt 4.12.1, „Installieren von Dateien“.
2. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
3. Fügen Sie die virtuelle Schnittstelle hinzu, indem Sie Folgendes eingeben:

   ```
   services virtualization virtual-machines basic-parameters network-interfaces name
   ```

   Erläuterung:

   - *name* ist die Bezeichnung der Schnittstelle, die hinzugefügt werden soll. Optionen sind u.a. vma.0001, vma.0002 und vma.0003.
4. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern.

Abschnitt 17.19
Eine virtuelle Schnittstelle löschen

Um eine virtuelle Schnittstelle zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Löschen Sie die virtuelle Schnittstelle durch Eingabe von:

   ```
   no services virtualization virtual-machines basic-parameters network-parameters name
   ```

   Erläuterung:

   - *name* ist die Bezeichnung der Schnittstelle, die gelöscht werden soll

3. Geben Sie **`commit`** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **`revert`** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 17.20

Zuweisen einer Netzwerkschnittstelle

Die Netzwerkkonfiguration ist in zwei Abschnitte unterteilt: die Netzwerkschnittstellen-Konfiguration auf der Gastseite und die Backend-Schnittstelle auf der Hostseite. Die verfügbaren Netzwerkschnittstellen auf der Gastseite sind *eth0*, *eth1* und *eth2*. Netzwerkschnittstellen werden über eine virtuelle Linux-Kernel-Bridge auf das externe Netzwerk überbrückt.

Um der virtuellen Maschine eine Netzwerkschnittstelle zuzuweisen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.

   HINWEIS
   Dem virtuellen Switch kann eine beliebige VLAN-Schnittstelle oder ein beliebiger dedizierter Port zugewiesen werden.

2. Fügen Sie eine virtuelle Maschine hinzu. Weitere Informationen finden Sie unter Abschnitt 17.7, „Hinzufügen einer virtuellen Maschine“.
3. Stellen Sie sicher, dass die VPE-Netzwerkschnittstelle für die virtuelle Maschine aktiviert ist. Weitere Informationen finden Sie unter Abschnitt 17.17, „Die VPE-Netzwerkschnittstelle aktivieren/deaktivieren“.

   HINWEIS
   Pro VPE sind bis zu drei Netzwerkschnittstellen möglich.

4. Fügen Sie eine oder mehrere Schnittstellen hinzu. Weitere Informationen finden Sie unter Abschnitt 17.18, „Eine virtuelle Schnittstelle hinzufügen“.
5. Konfigurieren Sie einen virtuellen Switch für den Virtualisierungsdienst. Weitere Informationen finden Sie unter Abschnitt 11.1.2, „Hinzufügen eines virtuellen Switch“.
6. Starten Sie die virtuelle Maschine. Weitere Informationen finden Sie unter Abschnitt 17.12, „Eine virtuelle Maschine starten“.
7. Rufen Sie das Konsolenfenster der virtuellen Maschine auf. Weitere Informationen finden Sie unter Abschnitt 17.21, „Auf die aktive virtuelle Maschine zugreifen“.
8. Loggen Sie sich auf der virtuellen Maschine ein.
9. Navigieren Sie zu ***etc » network » interfaces***.
10. Fügen Sie einen Eintrag für die gewünschte Schnittstelle hinzu, indem Sie einen geeigneten Linux-Befehl wie folgt eingeben:

    HINWEIS
    IP-Adressen können entweder manuell oder über DHCP zugewiesen werden. Im folgenden Beispiel wird DHCP verwendet.

    ```
    allow-hotplug interface
    iface interface inet dhcp
    ```

    Erläuterung:

    - *`interface`* ist die zu verwendende Schnittstelle. Optionen sind u.a. `eth0`, `eth1`, `eth2`.

11. Aktivieren Sie die Netzwerkschnittstelle, indem Sie Folgendes eingeben:

```
ifup interface
```

Erläuterung:

- *interface* ist die zu verwendende Schnittstelle. Optionen sind u.a. eth0, eth1, eth2.

Abschnitt 17.21

Auf die aktive virtuelle Maschine zugreifen

Die CLI enthält eine integrierte Befehlszeilenschnittstelle (Command Line Interface, CLI) für den Zugriff auf und die Arbeit mit der aktiven virtuellen Maschine. Für den Zugang zur aktiven virtuellen Maschine geben Sie Folgendes ein:

```
vm-console
```

Die Eingabeaufforderung für die virtuelle Maschine wird angezeigt. Beispiel:

```
ruggedcom# vm-console
Trying 127.0.0.1...
Connected to ruggedcom.localdomain.
Escape character is '^]'.

ruggedcom login:
```

Abschnitt 17.22

Abfragen der Seriennummer des Geräts

Um die Seriennummer des RUGGEDCOM RX1400 mit SNMP abzufragen, gehen Sie wie folgt vor:

1. Loggen Sie sich auf der aktiven virtuellen Maschine ein. Weitere Informationen finden Sie unter Abschnitt 17.21, „Auf die aktive virtuelle Maschine zugreifen“.
2. Stellen Sie sicher, dass das SNMP-Hilfsprogramm auf der virtuellen Maschine installiert ist. Falls nicht, installieren Sie das Hilfsprogramm, indem Sie Folgendes eingeben:

```
apt-get install snmp
```

> **WICHTIG!**
> *Die entsprechende Community-Zeichenkette bzw. das entsprechende Passwort, die/das für den RUGGEDCOM RX1400 konfiguriert wurde, muss verwendet werden.*

3. Fragen Sie die OID der Seriennummer ab, indem Sie Folgendes eingeben:

```
snmpget -v version -c id -u user address 1.3.6.1.4.1.15004.4.2.3.1.0
```

Erläuterung:

- *version* ist die zu verwendende SNMP-Version. Optionen sind u.a. 1, 2c, 3
- *id* ist die Bezeichnung der für das Gerät konfigurierten Community-Zeichenkette
- *user* ist die Bezeichnung des ROX-Benutzers
- *address* ist die IP-Adresse des RUGGEDCOM ROX II-Geräts

Beispiel: Folgender Index ist eine erfolgreiche Ausgabe einer Abfrage:

```
1.3.6.1.4.1.15004.4.2.3.1.0 = STRING: RUMED22080400
```

18 Anwendungen

Anwendungen sind spezielle Add-ons, die die Funktionalität von RUGGEDCOM ROX II erweitern, wie zum Beispiel eine erweiterte Unterstützung anderer RUGGEDCOM-Produkte (z. B. RUGGEDCOM CROSSBOW). Sie werden genau wie das RUGGEDCOM ROX II-Betriebssystem installiert und hochgerüstet, das heißt sie werden zuerst auf der inaktiven Partition installiert und erst nach einem Reboot aktiviert. Auf diese Weise kann die Installation abgelehnt oder rückgängig gemacht werden, wenn die Anwendung unerwünschte Ergebnisse bewirkt. Die jeweils aktive Partition wird durch die Installation oder das Hochrüsten einer Anwendung nicht beeinflusst.

Alle RUGGEDCOM ROX II-Anwendungen werden als Repositories herausgegeben und müssen auf einem Upgrade-Server gehostet werden. Weitere Informationen zum Einrichten eines Upgrade-Servers finden Sie in Abschnitt 4.15.2, „Einrichten eines Upgrade-Servers“.

INHALT

- Abschnitt 18.1, „Eine Liste der installierten Applikationen anzeigen“
- Abschnitt 18.2, „Eine Anwendung installieren“
- Abschnitt 18.3, „Ein Upgrade für eine Anwendung ausführen“
- Abschnitt 18.4, „Eine Anwendung deinstallieren“
- Abschnitt 18.5, „Applikations-Repositories verwalten“

Abschnitt 18.1

Eine Liste der installierten Applikationen anzeigen

Um eine Liste der auf dem Gerät installierten RUGGEDCOM ROX II-Applikationen anzusehen, geben Sie Folgendes ein:

```
show admin software-upgrade apps installed-apps
```

Falls Applikationen installiert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show admin software-upgrade apps installed-apps
APP NAME  VERSION
------------------
crossbow  4.1.2
elan      8.0.2
```

Falls keine Applikationen installiert wurden, installieren Sie Applikationen je nach Bedarf. Weitere Informationen finden Sie unter Abschnitt 18.2, „Eine Anwendung installieren“.

Abschnitt 18.2
Eine Anwendung installieren

Um eine Anwendung zu installieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Stellen Sie sicher, dass das Repository für die Anwendung vor dem Installieren der Anwendung konfiguriert wurde. Weitere Informationen finden Sie unter Abschnitt 18.5.3, „Ein Repository hinzufügen“.
3. Installieren Sie die Anwendung, indem Sie Folgendes eingeben:

   ```
   admin software-upgrade apps install-app app-name name
   ```

   Erläuterung:

   - *name* ist die Bezeichnung der Anwendung wie in der Repository-Konfiguration angezeigt. Um mehr als eine Anwendung zu installieren, verwenden Sie eine kommaseparierte Liste.

Abschnitt 18.3
Ein Upgrade für eine Anwendung ausführen

Um ein Upgrade einer Anwendung auszuführen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Deinstallieren Sie die Anwendung durch Eingabe von:

   ```
   admin software-upgrade apps upgrade-app app-name name
   ```

   Erläuterung:

   - *name* ist die Bezeichnung der Anwendung, für die ein Upgrade ausgeführt werden soll, wie in der Repository-Konfiguration angezeigt. Um Upgrades für mehr als eine Anwendung auszuführen, verwenden Sie eine kommaseparierte Liste.

Abschnitt 18.4
Eine Anwendung deinstallieren

Um eine Anwendung zu deinstallieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Deinstallieren Sie die Anwendung durch Eingabe von:

   ```
   admin software-upgrade apps uninstall-app app-name name
   ```

   Erläuterung:

   - *name* ist die Bezeichnung der Anwendung, die deinstalliert werden soll, wie in der Repository-Konfiguration angezeigt. Um mehr als eine Anwendung zu deinstallieren, verwenden Sie eine kommaseparierte Liste.

Abschnitt 18.5

Applikations-Repositories verwalten

Bevor eine RUGGEDCOM ROX II-Applikation installiert und hochgerüstet werden kann, muss eine Verbindung zu ihrem Repository auf dem Upgrade-Server konfiguriert werden.

INHALT

- Abschnitt 18.5.1, „Eine Liste der Repositories anzeigen“
- Abschnitt 18.5.2, „Die Repository-Verbindung überprüfen“
- Abschnitt 18.5.3, „Ein Repository hinzufügen“
- Abschnitt 18.5.4, „Ein Repository löschen“

Abschnitt 18.5.1

Eine Liste der Repositories anzeigen

Um eine Liste der RUGGEDCOM ROX II Applikations-Repositories anzusehen, geben Sie Folgendes ein:

```
show running-config admin software-upgrade apps repository
```

Falls Repositories konfiguriert wurden, wird eine Tabelle oder Liste ähnlich dem folgenden Beispiel angezeigt:

```
ruggedcom# show running-config admin software-upgrade apps repository | tab
APP NAME  URL                                              VERSION
-----------------------------------------------------------------
crossbow  http://10.200.20.231/crossbow-repo/debianppc  rs2

 !
!
```

Falls keine Repositories konfiguriert wurden, fügen Sie je nach Bedarf Repositories hinzu. Weitere Informationen finden Sie unter Abschnitt 18.5.3, „Ein Repository hinzufügen“.

Abschnitt 18.5.2

Die Repository-Verbindung überprüfen

Um die Verbindung mit einem Repository zu prüfen, geben Sie Folgendes ein:

```
admin software-upgrade apps check-repository-connection app-name name
```

Erläuterung:

- *name* ist die Bezeichnung des Repository wie in der Repository-Konfiguration angezeigt. Um die Verbindung mit mehr als einem Repository zu überprüfen, verwenden Sie eine kommaseparierte Liste.

Die Verbindungsergebnisse werden angezeigt.

Abschnitt 18.5.3
Ein Repository hinzufügen

Um ein Anwendungs-Repository hinzuzufügen, gehen Sie wie folgt vor:

HINWEIS
Ein Anwendungs-Repository ist zu konfigurieren, bevor eine Anwendung installiert oder ein Upgrade durchgeführt werden kann.

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie das Repository hinzu, indem Sie Folgendes eingeben:

   ```
   admin software-upgrade apps repository app-name name
   ```

   Erläuterung:

   - *name* ist die Bezeichnung des Repository wie in der Anwendungskonfiguration angezeigt. Beachten Sie die Freigabehinweise für die Anwendung.
3. Konfigurieren Sie je nach Bedarf den/die folgenden Parameter:

Parameter	Beschreibung
url { url }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 1024 Zeichen Die URL des Upgrade-Servers, der das Repository der Anwendung hostet (unterstützt werden http, https und ftp).
version { version }	**Zusammenfassung:** Eine Zeichenkette mit 1 bis 64 Zeichen Die Version der Anwendung, die Sie installieren oder aktualisieren.

4. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

Abschnitt 18.5.4
Ein Repository löschen

Um ein Anwendungs-Repository zu löschen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich die CLI im Konfigurationsmodus befindet.
2. Fügen Sie das Repository hinzu, indem Sie Folgendes eingeben:

   ```
   no admin software-upgrade apps repository app-name name
   ```

   Erläuterung:

   - *name* ist die Bezeichnung des Repository wie in der Anwendungskonfiguration angezeigt. Beachten Sie die Freigabehinweise für die Anwendung.
3. Geben Sie **commit** ein und drücken Sie auf **Enter**, um die Änderungen zu speichern, bzw. geben Sie **revert** ein und drücken Sie auf **Enter**, um abzubrechen.

19 Fehlersuche

Dieses Kapitel beschreibt die Fehlersuche für häufige Probleme, die bei der Arbeit mit RUGGEDCOM ROX II oder bei der Entwicklung eines Netzwerks auftreten können. Es beschreibt die folgenden Aufgaben:

WICHTIG!
Wenn Sie weitere Unterstützung benötigen, wenden Sie sich an den Siemens Kundensupport.

HINWEIS
Eine Beschreibung vorkonfigurierter Alarme finden Sie unter Abschnitt 5.6.1, „Vorkonfigurierte Alarme“.

INHALT

- Abschnitt 19.1, „Ethernet-Ports“
- Abschnitt 19.2, „Multicast-Filterung“
- Abschnitt 19.3, „Spanning Tree“
- Abschnitt 19.4, „VLANs“
- Abschnitt 19.5, „Fehlerbehebung bei Firmware-Updates“

Abschnitt 19.1

Ethernet-Ports

Im Folgenden werden häufig auftretende Probleme in Verbindung mit Ethernet-Ports beschrieben.

Problem	Lösung
Eine Verbindung scheint in Ordnung zu sein, wenn das Verkehrsniveau gering ist, fällt jedoch aus, sobald die Verkehrsraten zunehmen ODER eine Verbindung kann Ping-Anfragen erhalten und hat jedoch Probleme mit FTP/SQL/HTTP usw.	Eine mögliche Ursache des intermittierenden Betriebs ist die einer *Duplex-Nichtübereinstimmung*. Wenn ein Ende des Links fest auf Vollduplex-Modus eingestellt ist und für den Peer Auto-Negotiation eingestellt ist, fällt die Seite mit der Auto-Negotiationseinstellung auf Halbduplex-Betrieb zurück. Bei einem geringeren Verkehrsvolumen kann die Verbindung wenige bis keine Fehler aufweisen. Wenn das Verkehrsvolumen zunimmt, werden auf der Seite mit fester Negotiation Pakete verworfen, während auf der Seite mit der Auto-Negotiation Kollisionen auftreten. Wenn die Verkehrslast schließlich 100 % erreicht, wird die Verbindung völlig unbrauchbar. Der Ping-Befehl mit Flood-Optionen ist ein hilfreiches Mittel zum Testen in Betrieb genommener Verbindungen. Der Befehl **`ping`** `192.168.0.1 500 2` kann zum Ausgeben von 500 Ping-Anfragen, jeweils im Abstand von zwei Millisekunden, an den nächsten Switch verwendet werden. Wenn die verwendete Verbindung eine hohe Qualität aufweist, dann sollten keine Ping-Anfragen verloren gehen, und die mittlere Round-Trip-Zeit (RTT) sollte einen kleinen Wert aufweisen.

Problem	Lösung
Auf Verbindungen kann nicht zugegriffen werden, selbst wenn die Schutzfunktion Link Fault Indication (LFI) verwendet wird.	Stellen Sie sicher, dass die LFI-Funktion nicht am Peer aktiviert ist. Wenn LFI beidseitig an der Verbindung aktiviert ist, halten beide Seiten die Verbindungssignalgenerierung voneinander zurück.

Abschnitt 19.2

Multicast-Filterung

Im Folgenden werden häufig auftretende Probleme in Verbindung mit der Multicast-Filterung beschrieben.

Problem	Lösung
Beim Start wird ein Multicast-Traffic-Feed immer an alle Mitglieder des VLANs verteilt.	Ist IGMP für das VLAN aktiviert? Multicasts werden an alle Mitglieder des VLANs verteilt, sofern IGMP nicht aktiviert ist.
Mit dem Switch verbundene Computer empfangen Multicast-Datenverkehr, jedoch nicht, wenn sie mit einem Router verbunden sind.	Wird der Port zum Verbinden des in der Routerportliste aufgeführten Routers verwendet? Um zu ermitteln, ob der Multicast-Strom zum Router gesendet wird, ziehen Sie die für Switched-Ethernet-Ports erhobene Statistik hinzu. Weitere Informationen finden Sie unter Abschnitt 8.1.3, „Statistiken der Switched-Ethernet-Ports anzeigen“. Vergewissern Sie sich, dass der zum Router übertragene Traffic Count mit dem von der Multicast-Quelle empfangene Traffic Count identisch ist.
Der Videostrom an einer Endstation weist eine schlechte Qualität auf.	Die Videobereitstellung ist eine Ressourcen-intensive Anwendung. Da diese eine isochrone Belastung verwendet, müssen Daten mit einer vorgeschriebenen Geschwindigkeit übertragen werden, da Benutzer andernfalls Störungen im Video sehen. Netzwerke, die Daten vom Server zum Client transportieren, müssen so ausgelegt sein, dass sie dieser enormen, isochronen Belastung standhalten. Videodatenströme können enorme Mengen an Bandbreite verbrauchen. Die Funktionen und die Kapazität sowohl des Servers als auch des Netzwerks (einschließlich Router, Bridges, Switches und Schnittstellen) wirken sich auf die Datenströme aus. Überschreiten Sie 60 % der maximalen Schnittstellenbandbreite nicht. Wenn Sie beispielsweise ein 10 MBit/s schnelles Ethernet verwenden, betreiben Sie eine einzelne Multicast-Quelle mit nicht mehr als 6 MBit/s bzw. zwei Quellen zu je 3 MBit/s. Diese Ports müssen bei der Netzwerkplanung unbedingt berücksichtigt werden, da Routerports den Datenverkehr aller Multicast-Gruppen transportieren. **WICHTIG!** *Das Multicasting verursacht Latenz im gesamten Verkehr im Netzwerk. Gehen Sie bei der Netzwerkplanung mit Sorgfalt vor und berücksichtigen Sie Kapazitäts- und Latenzprobleme.*
Multicast-Datenströme bestimmter Gruppen werden nicht ordnungsgemäß weitergeleitet. Bestimmte Segmente ohne Subscriber empfangen Verkehr, andere Segmente mit Subscriber hingegen nicht.	Stellen Sie sicher, dass verschiedene Multicast-Gruppen keine Multicast-IP-Adressen haben, die auf dieselbe Multicast-MAC-Adresse verweisen. Die Switch-Weiterleitung arbeitet auf Basis von MAC-Adressen und funktioniert nicht korrekt, wenn verschiedene Gruppen auf dieselbe Multicast-MAC-Adresse verweisen.
Computer am Switch geben Join-Anfragen aus, empfangen jedoch keine Multicast-Ströme von einem Router.	Wird für die Multicast-Route IGMP in der Version 2 ausgeführt? Die IGMP-Version 2 muss ausgeführt werden, damit das IGMP Snooping ordnungsgemäß funktioniert.
Ein Verbinden oder Trennen bestimmter Switch-Ports ist nicht möglich, der Multicast-Verkehr wird überall hingeleitet. Ist IGMP ausgefallen?	IGMP ist nicht ausgefallen. Dies kann in der Tat ein ordnungsgemäßes Verhalten des Switch sein. Wenn der Switch eine Änderung in der Netzwerktopologie mittels RSTP erkennt, agiert er, um einen Verlust des Multicast-Verkehrs zu vermeiden. Wenn dieser so konfiguriert ist, leitet er den gesamten Multicast-Verkehr an alle Ports weiter, die keine RSTP-Edge-Ports sind (da sich diese eventuell mit Routern verbinden können). Dies kann ein unerwünschtes Flooding mit Multicast-Verkehr zur Folge haben, was nach wenigen Minuten aufhört. Dadurch wird

Problem	Lösung
	jedoch sichergestellt, dass alle an dem Verkehr interessierten Geräte den Verkehr weiterhin und ohne Unterbrechung empfangen. Dasselbe Verhalten kann beobachtet werden, wenn der Switch zurückgesetzt wird oder wenn das IGMP Snooping für das VLAN deaktiviert wird.

Abschnitt 19.3

Spanning Tree

Im Folgenden werden allgemeine Probleme im Zusammenhang mit dem Spanning Tree Protocol (STP) beschrieben.

Problem	Lösung
Das Netzwerk wird gesperrt, wenn ein neuer Port verbunden wird und die LEDs für den Portstatus in rascher Folge blinken.	Ist es möglich, dass bei einem der Switches im Netzwerk oder bei einem der Ports an einem Switch im Netzwerk STP deaktiviert ist und versehentlich die Verbindung mit einem anderen Switch hergestellt wird? Ist dieser Fall eingetreten, wurde eine Traffic-Schleife gebildet.
Gelegentlich scheinen an den Ports kurzzeitig erhebliche Überflutungen aufzutreten.	Scheint das Problem vorübergehend zu sein, ist es möglich, dass Ports, die Teil des Spanning Tree sind, als Edge-Ports konfiguriert wurden. Nachdem die Link-Layers auf Edge-Ports gestoßen sind, werden sie von STP (möglicherweise unangemessen) direkt an den Weiterleitungszustand weitergegeben. Wird dann eine RSTP-Konfigurationsnachricht empfangen, wird der Port wieder blockiert. Möglicherweise wurde für die Zeitdauer, die sich der Port im Weiterleitungszustand befand, eine Traffic-Schleife gebildet.
Ein Switch zeigt seltsames Verhalten, wo der Root-Port zwischen zwei Switch-Ports hin- und herwechselt und niemals zur Ruhe kommt.	Wenn einer der Switches den Root-Port von einem Port zu einem anderen zu wechseln scheint, kann das Problem in der Traffic-Priorisierung liegen. Weitere Informationen finden Sie unter The network becomes unstable when a specific application is started. Eine weitere mögliche Ursache für unregelmäßigen Betrieb kann die Nichtabstimmung von Auto-Negotiation sein. Wenn ein Ende des Links fest auf Vollduplex-Modus eingestellt ist und für den Peer Auto-Negotiation eingestellt ist, fällt die Seite mit der Auto-Negotiationseinstellung auf Halbduplex-Betrieb zurück. Bei geringerem Traffic-Volumen zeigt der Link, wenn überhaupt, dann wenige Fehler an. Bei ansteigendem Traffic-Volumen treten auf der Seite mit der festen Negotiation verworfene Pakete auf, während es auf der Seite mit der Auto-Negotiation zu Kollisionen kommt. Schließlich, sobald sich der Traffic einer Last von 100 % nähert, wird der Link komplett unbrauchbar. Zu diesem Zeitpunkt kann RSTP keine Konfigurationsnachrichten über den Link senden, und die Spanning-Tree-Topologie bricht zusammen. Ist ein alternativer Trunk vorhanden, aktiviert RSTP statt des blockierten Ports diesen Trunk. Da die Aktivierung des alternativen Ports dem blockierten Port häufig seinen Traffic abnimmt, wird der blockierte Port erneut zuverlässig. RSTP setzt ihn umgehend wieder ein, womit der Zyklus von vorn beginnt. Der Root-Port wechselt zwischen zwei Ports am Switch hin und her.
Ein Computer oder Gerät ist mit einem Switch verbunden. Nach dem Rücksetzen des Switch dauert der Wiederanlauf eine lange Zeit.	Ist es möglich, dass die RSTP-Edge-Einstellung für diesen Port auf False gesetzt ist? Wenn für Edge der Wert False eingestellt ist, veranlasst die Bridge, dass der Port zwei Weiterleitungsverzögerungszeiten durchlaufen muss, bevor der Port Frames senden oder empfangen kann. Wenn für Edge der Wert True eingestellt ist, gibt die Bridge den Port direkt an die Weiterleitung bei Link-up weiter. Eine weitere mögliche Erklärung ist, dass einige Links im Netzwerk im Halbduplex-Modus betrieben werden. RSTP verwendet ein Peer-to-Peer-Protokoll, das als Proposal-Agreement bezeichnet wird, und den Übergang bei Link-Ausfall sicherstellen soll. Für dieses Protokoll ist der Vollduplex-Betrieb erforderlich. Wenn RSTP einen Port erkennt, der nicht im Vollduplex-Modus ist, kann es sich nicht auf Proposal-Agreement verlassen und muss den Port-Übergang langsam (d.h. STP) gestalten. Konfigurieren Sie, wenn möglich, den Vollduplex-Betrieb für den Port. Andernfalls setzen Sie die Punkt-zu-Punkt-Einstellung des Ports auf True. Durch beide Verfahren erreichen Sie, dass das Proposal-Agreement-Protokoll verwendet wird.
Wenn der Switch getestet wird, indem ein Link absichtlich unterbrochen wird, dauert es	Ist es möglich, dass für einige Ports in der Topologie der STP-Modus konfiguriert wurde oder dass der Punkt-zu-Punkt-Parameter des Ports auf False gesetzt ist? STP- und Multipoint-Ports zeigen nach Auftreten von Fehlern nur sehr langsame Konvergenz.

Problem	Lösung
sehr lange, bis Geräte auf der anderen Seite des Switch abgefragt werden können.	Ist es möglich, dass der Port nach STP migriert ist? Wenn der Port über gemeinsame Medien an das LAN-Segment angeschlossen ist und STP-Bridges an diese Medien angeschlossen sind, dann ist die Konvergenz nach einem Link-Fehler sehr langsam. Verzögerungen in der Ordnung von zehntel oder hundertstel Millisekunden können zu Umständen führen, in denen der unterbrochene Link die einzige Verbindung zur Root-Bridge ist und die sekundäre Root-Bridge schlecht gewählt ist. Die schlimmste aller möglichen Strukturen tritt auf, wenn sich die sekundäre Root-Bridge am von der Root entferntesten Rand des Netzwerks befindet. In diesem Fall muss eine Konfigurationsnachricht bis zum Rand und zurück propagiert werden, um die Topologie neu aufzubauen.
Das Netzwerk besteht aus einem Ring aus Bridges, von denen zwei (miteinander verbundene) gemanagt sind, alle anderen sind unmanaged. Weshalb arbeitet das RSTP-Protokoll schnell, wenn zwischen den managed Bridges ein Link unterbrochen ist, jedoch nicht in dem Teil des Rings mit den unmanaged Bridges?	Eine einwandfrei arbeitende unmanaged Bridge ist gegenüber STP-Konfigurationsnachrichten transparent. Die managed Bridges tauschen in dem Teil des Rings mit den unmanaged Bridges Konfigurationsnachrichten so aus, als ob dieser Teil nicht existent wäre. Wenn jedoch ein Link im ungemanagten Teil des Rings ausfällt, können die managed Bridges den Ausfall nur durch Timeout von Hello-Nachrichten erkennen. Zur Wiederherstellung der vollständigen Konnektivität sind drei Hello-Nachrichten plus zwei Weiterleitungszeiten erforderlich.
Das Netzwerk wird instabil, wenn eine spezifische Anwendung gestartet wird. Das Netzwerk kehrt zum Normalzustand zurück, wenn die Anwendung gestoppt wird.	RSTP sendet seine Konfigurationsnachrichten mit der größtmöglichen Prioritätsstufe. Wenn CoS konfiguriert ist, um Datenverkehrsflüsse mit größtmöglicher Prioritätsstufe zuzulassen, und diese Datenverkehrsflüsse schwellen kontinuierlich auf 100 % der Leitungsbandbreite an, kann STP unterbrochen werden. Von daher ist es nicht ratsam, den höchsten CoS-Wert zu verwenden.
Wenn ein neuer Port eingebracht wird, wechselt der Root-Port zu diesem Port, statt zu dem Port, zu dem er wechseln oder auf dem er bleiben soll.	Ist es möglich, dass die Portkosten fehlerhaft programmiert sind oder dass die Auto-Negotiation einen unerwünschten Wert erlangt? Untersuchen Sie den Port und die Pfadkosten und aktivieren Sie dabei jeden Port als Root-Port.
Ein IED/Controller funktioniert mit dem Gerät nicht.	Es wurde festgestellt, dass sich bestimmte Controller mit niedriger CPU-Bandbreite weniger als perfekt verhalten, wenn sie unerwarteten Traffic empfangen. Versuchen Sie, STP für den Port zu deaktivieren. Wenn der Controller zum Zeitpunkt eines Link-Ausfalls ausfällt, besteht die entfernte Möglichkeit, dass Frame-Unordnung oder -Duplizierung die Ursache des Problems sein kann. Versuchen Sie, für den Root-Port der Bridge des ausfallenden Controllers STP einzustellen.
Abfragen an andere Geräte gehen gelegentlich verloren.	Überprüfen Sie die Netzwerkstatistik und ermitteln Sie, ob die Root-Bridge um den Zeitpunkt herum, zu dem Frame-Verlust beobachtet wird, TCNs empfängt. Es kann möglich sein, dass es Probleme mit zeitweise unterbrochenen Links im Netzwerk gibt.
Der Root empfängt eine Anzahl von TCNs. Woher kommen diese?	Untersuchen Sie die RSTP-Portstatistik und ermitteln Sie den Port, von dem die TCNs kommen. Melden Sie sich an dem Switch an, der sich am anderen Ende des Links dieses Ports befindet. Wiederholen Sie diesen Schritt, bis der Switch, der die TCNs erzeugt, gefunden ist (d.h. der Switch, der selbst keine große Anzahl von TCNs empfängt). Stellen Sie die Ursache für das Problem am Switch fest.

Abschnitt 19.4

VLANs

Im Folgenden werden allgemeine Probleme im Zusammenhang mit VLANs beschrieben.

Problem	Lösung
VLANs sind im Netzwerk nicht erforderlich. Können sie ausgeschaltet werden?	Ja. Lassen Sie einfach alle Ports auf *edge* und das systemeigene VLAN auf 1 eingestellt. Dies ist die Standardkonfiguration für den Switch.
Es wurden zwei VLANs erstellt und mehrere Ports sind deren Mitglieder geworden. Jetzt müssen einige der Geräte in einem VLAN	Wenn die Geräte auf der physikalischen Adressebene kommunizieren sollen, müssen sie Mitglieder desselben VLANs sein. Wenn sie auf Layer-3-Ebene kommunizieren können (z. B.

Problem	Lösung
Nachrichten an Geräte im anderen VLAN senden.	über ein Protokoll wie IP oder IPX), verwenden Sie einen Router. Der Router behandelt jedes VLAN als separate Schnittstelle, die über einen eigenen IP-Adressraum verfügt.

Abschnitt 19.5

Fehlerbehebung bei Firmware-Updates

Im Folgenden werden allgemeine Fehler und mögliche Lösungen im Zusammenhang mit Firmware-Updates beschrieben. Falls Sie weitere Unterstützung benötigen, wenden Sie sich an den Siemens-Kundensupport.

Fehlermeldung	Lösung
unknown firmware image file	Das Firmware-Image ist für das im Gerät installierte Modem nicht gültig bzw. der Firmware-Download wurde unbeabsichtigt unterbrochen. Überprüfen Sie die Verbindung zwischen dem Gerät und dem dezentralen Server. Stellen Sie sicher, dass die Verbindung zuverlässig ist.
mis-matched carrier	Die neue Firmware hat nicht das aktuell auf dem Gerät installierte Modem als Ziel. Überprüfen Sie den Firmware-Dateinamen in der Versionsinformationsdatei. Stellen Sie sicher, dass der Dateiname die PRI-ID des auf dem Gerät installierten Modems besitzt. Laden Sie die Firmware manuell in das Gerät und führen Sie anschließend den Befehl "qmi-firmware-update" aus, um den Zieldatenträger für die Firmware festzulegen. Siehe Befehl und Option in (*).
url connection/downloading failure	Das Gerät kann den dezentralen Hostserver mit der URL-Konfiguration nicht erreichen oder die Versionsinformationsdatei oder die Firmware-Datei kann auf dem dezentralen Server nicht gefunden werden. Überprüfen Sie die URL-Konfiguration und stellen Sie sicher, dass der dezentrale Server erreichbar ist. Überprüfen Sie den Pfad der URL-Konfiguration. Stellen Sie sicher, dass die neue Firmware-Datei sich am richtigen Speicherort auf dem dezentralen Server befindet.
invalid firmware information	Der Name der Versionsinformationsdatei oder der Name der Firmwaredatei existiert nicht auf dem Server. Überprüfen Sie, ob der Name der Versionsinformationsdatei oder der Name der Firmwaredatei auf dem dezentralen Server existiert.
Unspecified error.	Überprüfen Sie die Syslog-Datei auf ausführlichere Informationen.