comnet
Communication Networks

INSTALLATION AND OPERATION MANUAL



RELIANCE RLGE2FE16R

Substation-Rated, Enhanced Security Scada-Aware Ethernet Layer 2 Managed Switch/Layer 3 Router With Optional 2G/3G & 4G LTE Cellular Radio Link, Enhanced Network Security, Terminal Server, PoE+, and 100FX SFP Ports

ComNet product series RLGE2FE16R are substation-rated and industrially hardened layer 2 managed switches/layer 3 routers, with a unique and highly robust packet processing SCADA-aware security firewall for the most mission-critical and demanding cyber-security applications. The RLGE2FE16R is intended for deployment in environments where high levels of electromagnetic noise and interference (EMI) and severe voltage transients and surges are routinely encountered, such as electrical utility substations and switchyards, heavy manufacturing facilities, track-side electronic equipment, and other difficult out-of-plant installations. Layer 3 routing functionality allows for the participation and foundation of a core network infrastructure.

The RLGE2FE16R is an ideal platform for deploying a secure communications and networking gateway for remote electrical utility sites, and other critical infrastructure applications.

Contents

About This Guide 14
- Intended Audience 14
- Related Documentation 15
- About ComNet 15
- Website 15
- Support 15
- Safety 15

Overview 16
- Introduction 16
- Key Features 16

Hardware and Interfaces 19
- Graphic View of Hardware 22
- 22
- Distance kept for natural air flow 23
- Logical Structure 24
- Grounding 24
- Connecting to a Power Source 25
- Power Budget 26

Management over Console 26
- Connecting to Device 26
- Terminal 27
- SSH 28

Configuration Environment 29
- Command Line Interface 29
- Command Line navigation 30
- Dynamic Completion of Commands 31
- Help (?) 31
- Keyboard Shortcuts 32
- Supported Functionalities 33
- System Default state 36
- Root Commands 37
- Root Commands Description 38
- GCE Commands 39

GCE Commands Description 42
ACE Commands 46
Main Show Commands 47

System Version and Data Base 51
Configuration Database 51
OS VERSION 52
Running Configuration 53
Example upgrade the OS from USB 54
Example upgrade the OS from SFTP 55
Example export db and logs 56
Example handling DB files on flash 56
Example Import DB from TFTP 57
Safe Mode 58
SW Image upgrade and Recovery 59
Install OS image update from a USB 60
Installing First OS image from a USB 64
System Database Import/ Export 65

Port Interfaces 68
Port addressing 68
A Logical View Of Ports 68
Enabling Ports 69
ACE Ports 69
Default state 69
Vlan assignment 70
Ports FE 0/9-0/16 70
POE Ports 71
Power Management of POE 72
Mode of PoE 72
POE command Hierarchy 73
POE Commands Description 73

Controlling Ports 74
Storm Control 74
Rate Limit Output 74

Ports command Hierarchy 74

Port Commands Description 75
Port Configuration Example 77
Configuration Output Example 77
Login and Management 79
Login Authentication Hierarchy 79
Login Authentication Commands Description 80
Examples 81
Privilege level 82
Commands Description 82
Serial Console Port 83
Connecting to the Console Port 83
CLI Console Commands 84
Management 84
Commands Hierarchy 85
Commands Description 87
System Alias 89
CLI Pagination 90
MAC-Address Table (FDB) 91
Port Mac Learning and limit 91
Commands Hierarchy 91
Configuration Example, Static MAC entry 92
Example, exceeding MAC limit at a port 92
IP ARP Table 93
Commands Hierarchy 93
Commands Description 93
Configuration Example 94
VLAN 95
VLANs of System Usage 96
VLAN Range of NMS Usage 96
VLAN Configuration Guidelines 96
VLAN Default State 96
Vlan Ports 97
Enabling VLAN 97
Vlan command Hirarchy 98

IP Interfaces 101
GCE IP Interfaces 101
Commands Hierarchy 102
Commands Description 103
Default state 103
Static and Dynamic switch Default IP Address assignment 105
ACE IP Interfaces 106
ACE IP Interface Commands Hierarchy 107
ACE IP Interface Commands Description 107
Example for creating ACE IP Interface 108
Diagnostic 109
System Environment 109
RMON 110
System logs export 112
Commands Hierarchy 112
Capture Ethernet service traffic 113
Commands Hierarchy 113
Commands Description 114
Example 114
DDM 115
Debugging 119
Commands Hierarchy 119
Commands Description 120
Syslog 120
The Priority indicator 121
GCE Message Format 122
ACE Message Format 122
ACE Message severity 122
Firewall TCP SCADA Protocols 123
Firewall Serial SCADA Protocols 124
DM-VPN logs 127
Cellular logs 128
Alarm Relay logs 130
Commands Hierarchy 131
Commands Description 132

Configuration Example 133
Output example 134

Alarm Relay 135
ALARM Interface 135
Supported Alarms 138
Commands Hierarchy 139
Commands Description 140

Monitor Session 141
Commands Hierarchy 141
Commands Description 141
ACE Watchdog 141
Commands Hierarchy 142
Commands Description 142

SNMP 143
Supported traps 143
SNMP command Hierarchy 143
SNMP Command Description 144

Clock and Time 148

Local Clock 148
Commands Description 149
SNTP 150
SNTP Commands Descriptions 151

SSH 156
SSH Command Hierarchy 156
SSH Commands Descriptions 157
DHCP Client and Snooping Commands Hierarchy 158

DHCP Server 159
DHCP Server Commands Hierarchy 159
DHCP Relay Commands Description 160
Example 161
DHCP Client 162
DHCP Server show outputs 162

DHCP Relay 165
DHCP Relay GCE Command Hierarchy 165
DHCP Relay GCE Commands Description 166
DHCP Relay ACE Command Hierarchy 167
DHCP Relay ACE Commands Description 168
Example, GCE DHCP Relay 169
RADIUS Command Hierarchy 173
RADIUS Commands Descriptions 174
TACACS 176
Default Configurations 177
TACACS Command Hierarchy 177
TACACS Commands Descriptions 178
Configuration Example 179
802.1x 180
802.1x Commands Hierarchy 180
802.1x Commands Descriptions 181
Examples 183
IGMP Snooping 185
IGS Commands Hierarchy 185
IGS Commands Descriptions 186
Example 188
ACLs 190
ACL Flow validation at a port 190
ACL Commands Hierarchy 192
ACL Commands Descriptions 193
QOS 205
QOS Commands Hierarchy 205
QOS Commands Descriptions 207
Packet Queue Assignment 211
Set VPT or DSCP 213
Setting a Scheduling Algorithms 216
Traffic Filtering at Ingress 217
Setting a Shaper per Egress Port 217

Link Aggregation 218
LAG command Hierarchy 220
LAG Commands Descriptions 221
Example 222
STP 224
STP Description 225
Bridge ID and Switch Priority 226
Election of the Root Switch 227
STP Commands Hierarchy 228
STP Commands Descriptions 229
RSTP/MSTP 232
RSTP Description 232
Port States 232
Port Roles 232
Rapid Convergence 233
Proposal Agreement Sequence 233
Topology Change and Topology Change Detection 235
Default Configurations 235
Setting Spanning Tree Compatibility to STP 236
Configuring Spanning Tree Path Cost 238
Configuring Spanning Tree Port Priority 241
Configuring Spanning Tree Link type 244
Configuring Spanning Tree Portfast 245
Configuring Spanning Tree Timers 246
Enhanced RSTP 247
Method of operation 247
Commands Descriptions 249
LLDP 250
LLDP Commands Hierarchy 251
LLDP Commands Descriptions 252
Example 1 257
Show LLDP 260
Example 2 261
Show LLDP 262

1588v2 Precision Time Protocol 264
1588 Commands Hierarchy 264
1588 Commands Descriptions 265
Example 1 266
Configuration 266
Example 2 269
OAM CFM 272
CFM Command Hierarchy 272
CFM Commands Descriptions 273
ERPS 278
ERPS Commands Hierarchy 278
ERPS Commands Descriptions 280
Configuration validation 298
Verifying setup state 299
Discrete IO Channels 303
Discrete channel interfaces 303
Hardware 304
Modbus/TCP 304
Electric data 304
Discrete IO Channels Commands Hierarchy 305
Discrete Interfaces Commands 305
Example 306
NAT 308
Networking 308
NAT Commands Hierarchy 309
NAT Commands Description 309
Example, Fixed Network 310
Example, Cellular Network 313
OSPF 315
OSPF GCE Commands Hierarchy 315
OSPF GCE Commands Descriptions 318
OSPF ACE Commands Hierarchy 326
OSPF ACE Commands Descriptions 327

VRRP 334
VRRP Commands Hierarchy 334
VRRP Commands Descriptions 335
RIPv2 344
GCE RIP Commands Hierarchy 344
GCE RIP Commands Descriptions 345
ACE RIP Commands Hierarchy 346
ACE RIP Commands Descriptions 347
Example 348
Serial Ports and Services 351
Serial interfaces 352
Services configuration structure 352
Serial Commands Hierarchy 353
Serial Commands Description 355
Declaration of ports 358
Default State 358
System default VLAN 4093 358
Serial default VLAN 4092 359
RS-232 Port Pin Assignment 360
RS-232 Serial cable 361
LED Indicators 362
ACE QOS 362
ACE QOS Commands Hierarchy 362
ACE QOS Commands Descriptions 362
Example QOS for Serial Tunneling 363
Transparent Serial Tunneling 365
Concept of Operation 365
Supported Network topologies 366
Point to Point 366
Point to multipoint point 367
Multi Point to multipoint point 368
Modes of Operation 368
Bitstream 369
Service Buffer Mode 369
Service Connection Mode 370

Addressing Aware Modes 370
Reference drawing 371
Serial Traffic Direction 372
Allowed latency 372
Bus Idle Time 373
Bits for Sync 373
RS-232 Control lines 374
Modes of operation 374

Terminal Server 380
Terminal Server service 380
Service Buffer Mode 381
Terminal Server Commands Hierarchy 383
Terminal Server Commands 385
Example: Networking 390

Modbus Gateway 392
Implementation 392
Modbus Gateway Commands Hierarchy 393
Modbus Gateway Commands Description 394
Example 395

DNP3 Gateway 398
Example 398

Protocol Gateway IEC 101 to IEC 104 400
Modes of Operation 401
IEC101/104 Gateway properties IEC 101 402
IEC101/104 Gateway Configuration 403
Gateway 101/104 Configuration Flow 404
Gateway 101/104 Commands Hierarchy 406
Gateway 101/104 Commands 408

VPN 412
Background 412
Modes supported 412
Layer 2 VPN 412
DM-VPN 414

IPSec-VPN 416
L2-VPN Commands Hierarchy 418
L2-VPN Commands 419
DM-VPN Commands Hierarchy 419
IPSec-VPN Transport mode Commands Hierarchy 420
IPSec-VPN Transport mode Commands 421
IPSec 421
ISAKMP Phase 2 429
IPSec Commands Hierarchy 432
IPSec X.509 Commands Hierarchy 433
IPsec Commands 433
IPSec defaults 438

Cellular Modem 439

LTE Modem 439
GPRS/UMTS Modem 440
Hardware 440
Cellular modem as a USB device 441
Interface Name 441
Method of operation 442
L3 IPSec VPN 442
SIM card state 443
Backup and redundancy 445
Cellular Commands Hierarchy 448
Cellular Commands Description 449
Default State 450
LED Indicators 451
Example for retrieving the IMEI 451
Example: Sim Status 452
Example: Cellular Watch Dog 454

VPN Setup Examples 458

L2 VPN over Layer 3 cloud 458
Network drawing, part A 459
Configuration 459
Spoke 461
Network drawing, part B 464

Configuration 464
IPSec VPN over Layer 3 cloud 468
Configuration 469
L2 VPN over Cellular Setup 474
Adding Terminal server service 481
Adding an IEC 101/104 service 482
Adding serial tunneling service 483
DM-VPN over Cellular Setup 485
Network drawing 486
Configuration 487
Adding a terminal server service 491
Adding a transparent serial tunneling service 492

About This Guide

This user guide includes relevant information for utilizing the Reliance RLGE2FE16R line of switches.

The information in this document is subject to change without notice and describes only the product defined in the introduction of this document.

This document is intended for the use of customers of ComNet only for the purposes of the agreement under which the document is submitted, and no part of it may be reproduced or transmitted in any form or means without the prior written permission of ComNet.

The document is intended for use by professional and properly trained personnel, and the customer assumes full responsibility when using it.

If the Release Notes that are shipped with the device contain information that conflicts with the information in this document or supplements it, the customer should follow the Release Notes.

The information or statements given in this document concerning the suitability, capacity, or performance of the relevant hardware or software products are for general informational purposes only and are not considered binding. Only those statements and/or representations defined in the agreement executed between ComNet and the customer shall bind and obligate ComNet.

ComNet however has made all reasonable efforts to ensure that the instructions contained in this document are adequate and free of material errors. ComNet will, if necessary, explain issues which may not be covered by the document.

ComNet sole and exclusive liability for any errors in the document is limited to the documentary correction of errors. **ComNet is not and shall not be responsible in any event for errors in this document or for any damages or loss of whatsoever kind, whether direct, incidental, or consequential (including monetary losses),** that might arise from the use of this document or the information in it.

This document and the product it describes are the property of ComNet, which is the owner of all intellectual property rights therein, and are protected by copyright according to the applicable laws.

Other product and company names mentioned in this document reserve their copyrights, trademarks, and registrations; they are mentioned for identification purposes only.

Copyright © 2016 Communication Networks, LLC. All rights reserved.

Intended Audience

This user guide is intended for network administrators responsible for installing and configuring network equipment. Users must be familiar with the concepts and terminology of Ethernet and local area networking (LAN) to use this User Guide.

Related Documentation

The following documentation is also available:

» RLGE2FE16R Data sheet

» RLGE2FE16R Quick Start Guide

» RLGE2FE16R_ES Enhanced Security Software Options Manual

» SFP Modules Data sheet

About ComNet

ComNet develops and markets the next generation of video solutions for the CCTV, defense, and homeland security markets. At the core of ComNet's solutions are a variety of high-end video servers and the ComNet IVS software, which provide the industry with a standard platform for analytics and security management systems enabling leading performance, compact and cost effective solutions.

ComNet products are available in commercial and rugged form.

Website

For information on ComNet's entire product line, please visit the ComNet website at **http://www.comnet.net**

Support

For any questions or technical assistance, please contact your sales person (**sales@comnet.net**) or the customer service support center (**techsupport@comnet.net**)

Safety

» Only ComNet service personnel can service the equipment. Please contact ComNet Technical Support.

» The equipment should be installed in locations with controlled access, or other means of security, and controlled by persons of authority.

Overview

Introduction

The ComNet Service-aware Industrial Ethernet switches combine a ruggedized Ethernet platform with a unique application-aware processing engine.

As an Industrial Ethernet switch the Reliance RLGE2FE16R switches provide a strong Ethernet and IP feature-set with a special emphasis on the fit to the mission-critical industrial environment such as fit to the harsh environment, high reliability and network resiliency.

In addition, the ComNet switches have unique service-aware capabilities that enable an integrated handling of application-level requirements such as implementation of security measures.

Such an integrated solution results in simple network architecture with an optimized fit to the application requirements.



Figure 1 - Illustration of ComNet RLGE2FE16R

Key Features

The Reliance RLGE2FE16R devices offer the following features (subject to configuration options):

» Service aware security of industial control protocols
» Wire speed, non-blocking Layer 2 switching
» Dynamic and static layer 3 routing
» Compact systems with flexible ordering options of interfaces type /quantity
» Advanced Ethernet and IP feature-set
» Integrated Defense-in-Depth tool-set
» Ethernet and Serial interfaces
» Cellular mode
» Fit to harsh industrial environment
» Supported by a dedicated industrial service configuration tool (RLConfig)

Conventions	Description
commands	CLI and SNMP commands
`command example`	CLI and SNMP examples
<Variable>	user-defined variables
(numerical variable)	numerical variable
{mandatory command parameters}	CLI syntax
[Optional Command Parameters]	CLI syntax

Seamless & Reliable Connection to Any Network

The RLGE2FE16R provides connectivity to any copper, fiber optic, or cellular radio-based Ethernet network. Fiber optic networks are supported by the use of two 100/1000FX SFP uplink ports. The optional highly resilient 2G/3G/4G LTE cellular radio uplink with 2 SIM card slots for network redundancy, is ideal where fiber optic infrastructure is not available, and may be used as a back-up link for those applications where interruption of service is not tolerable. The 8 optional 100 Mbps SFP communications ports provide a simple to implement aggregation capability to the user's network.

Extremely Effective Network Security

The RLGE2FE16R is available with two different levels of network security software: Standard Security; or Enhanced Security, for the most mission-critical applications.

Standard Security Software Package Version:

Service Gateway – The RLGE2FE16R service gateway includes a highly robust application layer, and provides legacy support, an enterprise-class firewall, serial tunnelling, protocol gateway, and extremely effective encryption technologies. The service gateway offers a uniquely capable feature set which may serve as the hardware foundation to a secure industrial controls network, and includes Protocol Gateway, VPN, and IPsec features.

Protocol Gateway – Gateway functionality between a DNP3 TCP client (local) and a DNP3 Serial RTU, IED, PLC, or other compatible device is supported. This same functionality is supported across MODBUS TCP to MODBUS RTU, and IEC 61850 101/104 TCP to IEC 61850 101/104 RTU. This level of protocol conversion allows legacy protocols to be secured by enterprise and industry best practice level encryption across a TCP IP-based network.

VPN – VPN tunnels are included for secure inter-site connectivity with IPsec, DM-VPN, and VPN GRE tunnels with key management certificates. The supported VPN modes allow both layer-2 and layer-3 services, to best suit the user's application-specific cyber-protection needs.

IPSec – Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and/or encrypting each IP packet of a communication session. IPsec-VPN as well as IPsec encryption are supported over other VPN technologies. By implementing this level of industry-accepted encryption, data may traverse the network in a guaranteed delivery method, as well as providing a cohesive and secure methodology for network communication across legacy and modern networks.

Ease of Installation and Network Integration

High levels of cyber-security experience are not required to successfully deploy the RLGE2FE16R. It is fully supported by ComNet's Reliance Product Configuration Utility and CLI, allowing the secure switch/router to be easily configured, and to diagnose network and security functions.

Configuration of the secure firewall is also simple. Once connected to the user's network, the RLGE2FE16R immediately begins to collect and analyse information across the network, including from other connected devices, traffic behavior, etc. Recommended firewall rules are then suggested to the user; the implementation of these rules is optional, and they can be easily edited using the Configuration Utility.

OAM (IEEE 802.3-2005 & IEEE 802.1ag) and QoS are also supported. Strict priority, Weighted Round Robin (WRR), ingress policing, and egress traffic shaping are included for traffic management.

Product Options

Enhanced Security Software Option – Includes all of the security features of the Standard Security version, plus: Identity management and authentication proxy access (APA), event logger, IPsec authentication with certificates, cyber-physical Integration, enhanced SCADA-aware firewall, and DPI (Deep Packet Inspection) SCADA protocols firewall. This manual does not cover Enhanced Security Software Options.

Cellular Radio Option – An internal 2G/3G/4G LTE GPRS/UMTS cellular radio modem, with 2 SIM card slots for maximum network reliability and availability. All world-wide cellular radio frequency bands are supported.

Serial Data Interface Option – The 4-port serial interface is available for applications including terminal server with protocol gateway and serial tunnelling functionality, and provides direct connectivity to legacy RS-232 serial data IEDs, RTUs, and other devices.

PoE (Power over Ethernet) Option – 30 watts per port is available for 8 of the RJ-45 Ethernet communications ports, and is compliant with the IEEE 802.3at specification.
The maximum PoE load per switch is dependant on the voltage type ordered and is shared across ports 1-8 only. Please refer to the PoE Power Management section for further details.

100 Mbps SFP Option – Includes (8) 100 Mbps SFP ports for network aggregation applications. Provides (8) 10/100 Mbps copper/RJ-45 communications ports; (8) 100 Mbps SFP ports; and (2) 100/1000 Mbps SFP uplink ports. Note: This option deletes the cellular radio option, as well as the serial interfaces option.

Hardware and Interfaces

Depending on the RLGE2FE16R hardware variant ordered your switch will hold physical Ethernet and Serial ports.

» Serial, RJ45 ports, support RS-232. Max 4 ports
» Ethernet RJ45 copper ports are 10/100 FE. Max 16 ports
» Ethernet SFP based ports are 10/100 FE. Max 8 ports.
» Ethernet SFP based ports are 100/1000 GE. Max 2 ports.

Ordering options of Hardware

RLGE2FE16R/S variants do not support the following features:
- APA
- IPSEC X.509
- Event Logger
- Application Aware Firewall
These features are only supported in RLGE2FE16R/E models

RLGE2FE16R Standard Security Models

Part Number	Description
RLGE2FE16R/S/XX/28[3]	RLGE2FE16R with 2 × 100/1000 FX SFP, 8 × 10/100 TX
RLGE2FE16R/S/XX/28/S22[3]	RLGE2FE16R with 2 × 100/1000 FX SFP, 8 × 10/100 TX, 4 × RS-232
RLGE2FE16R/S/XX/28/CGU[3]	RLGE2FE16R with 2 × 100/1000 FX SFP, 8 × 10/100 TX, 2G/3G GPRS/UMTS Cellular Modem
RLGE2FE16R/S/XX/28/CH+[3]	RLGE2FE16R with 2 × 100/1000 FX SFP, 8 × 10/100 TX, 2G/3G HSPA+ Cellular Modem
RLGE2FE16R/S/XX/28/CNA[3]	RLGE2FE16R with 2 × 100/1000 FX SFP, 8 × 10/100 TX, 4G LTE Cellular Modem (NA Bands)
RLGE2FE16R/S/XX/28/CNA[3]	RLGE2FE16R with 2 × 100/1000 FX SFP, 8 × 10/100 TX, 4G LTE Cellular Modem (NA Bands)
RLGE2FE16R/S/XX/28/CEU[3]	RLGE2FE16R with 2 × 100/1000 FX SFP, 8 × 10/100 TX, 4G LTE Cellular Modem (EU Bands)
RLGE2FE16R/S/XX/28/S22/CGU[3]	RLGE2FE16R with 2 × 100/1000 FX SFP, 8 × 10/100 TX, 4 × RS-232, 2G/3G GPRS/UMTS Cellular Modem
RLGE2FE16R/S/XX/28/S22/CH+[3]	RLGE2FE16R with 2 × 100/1000 FX SFP, 8 × 10/100 TX, 4 × RS-232, 2G/3G HSPA+ Cellular Modem
RLGE2FE16R/S/XX/28/S22/CNA[3]	RLGE2FE16R with 2 × 100/1000 FX SFP, 8 × 10/100 TX, 4 × RS-232, 4G LTE Cellular Modem (NA Bands)
RLGE2FE16R/S/XX/28/S22/CEU[3]	RLGE2FE16R with 2 × 100/1000 FX SFP, 8 × 10/100 TX, 4 × RS-232, 4G LTE Cellular Modem (EU Bands)
RLGE2FE16R/S/XX/28P[3]	RLGE2FE16R with 2 × 100/1000 FX SFP, 8 × 10/100 TX PoE+
RLGE2FE16R/S/XX/28P/S22[3]	RLGE2FE16R with 2 × 100/1000 FX SFP, 8 × 10/100 TX PoE+, 4 × RS-232
RLGE2FE16R/S/XX/28P/CGU[3]	RLGE2FE16R with 2 × 100/1000 FX SFP, 8 × 10/100 TX PoE+, 2G/3G GPRS/UMTS Cellular Modem
RLGE2FE16R/S/XX/28P/CH+[3]	RLGE2FE16R with 2 × 100/1000 FX SFP, 8 × 10/100 TX PoE+, 2G/3G HSPA+ Cellular Modem

Part Number	Description
RLGE2FE16R/S/XX/28P/CNA[3]	RLGE2FE16R with 2 × 100/1000 FX SFP, 8 × 10/100 TX PoE+, 4G LTE Cellular Modem (NA Bands)
RLGE2FE16R/S/XX/28P/CEU[3]	RLGE2FE16R with 2 × 100/1000 FX SFP, 8 × 10/100 TX PoE+, 4G LTE Cellular Modem (EU Bands)
RLGE2FE16R/S/XX/28P/S22/CGU[3]	RLGE2FE16R with 2 × 100/1000 FX SFP, 8 × 10/100 TX PoE+, 4 × RS-232, 2G/3G GPRS/ UMTS Cellular Modem
RLGE2FE16R/S/XX/28P/S22/CH+[3]	RLGE2FE16R with 2 × 100/1000 FX SFP, 8 × 10/100 TX PoE+, 4 × RS-232, 2G/3G HSPA+ Cellular Modem
RLGE2FE16R/S/XX/28P/S22/CNA[3]	RLGE2FE16R with 2 × 100/1000 FX SFP, 8 × 10/100 TX PoE+, 4 × RS-232, 4G LTE Cellular Modem (NA Bands)
RLGE2FE16R/S/XX/28P/S22/CEU[3]	RLGE2FE16R with 2 × 100/1000 FX SFP, 8 × 10/100 TX PoE+, 4 × RS-232, 4G LTE Cellular Modem (EU Bands)
RLGE2FE16R/S/XX/216[3]	RLGE2FE16R with 2 × 100/1000 FX SFP, 16 × 10/100 TX
RLGE2FE16R/S/XX/216P[3]	RLGE2FE16R with 2 × 100/1000 FX SFP, 8 × 10/100 TX PoE+, 8 × 10/100 TX
RLGE2FE16R/S/XX/288[3]	RLGE2FE16R with 2 × 100/1000 FX SFP, 8 × 10/100 TX, 8 × 100 FX SFP
RLGE2FE16R/S/XX/288P[3]	RLGE2FE16R with 2 × 100/1000 FX SFP, 8 × 10/100 TX PoE+, 8 × 100 FX SFP

[3] XX in above part codes is a placeholder for one of the options from the following power input table

Power Input Option Code	Description
12	Dual Redundant 9 to 18 VDC Inputs
24	Dual Redundant 18 to 32 VDC Inputs
48	Dual Redundant 36 to 60 VDC Inputs
11	Dual Redundant 85 to 165 VDC Inputs
AC	Single 90 to 250 VAC Input

RLGE2FE16R Standard Security Models 220 VDC

Part Number	Description
RLGE2FE16R/S/22/28	RLGE2FE16R with 2 × 100/1000 FX SFP, 8 × 10/100 TX, 220 VDC
RLGE2FE16R/S/22/28P	RLGE2FE16R with 2 × 100/1000 FX SFP, 8 × 10/100 TX PoE+, 220 VDC
RLGE2FE16R/S/22/216	RLGE2FE16R with 2 × 100/1000 FX SFP, 16 × 10/100 TX, 220 VDC
RLGE2FE16R/S/22/216P	RLGE2FE16R with 2 × 100/1000 FX SFP, 8 × 10/100 TX PoE+, 8 × 10/100 TX, 220 VDC
RLGE2FE16R/S/22/288	RLGE2FE16R with 2 × 100/1000 FX SFP, 8 × 10/100 TX, 8 × 100 FX SFP, 220 VDC
RLGE2FE16R/S/22/288P	RLGE2FE16R with 2 × 100/1000 FX SFP, 8 × 10/100 TX PoE+, 8 × 100 FX SFP, 220 VDC

RLGE2FE16R Enhanced Security Models

Part Number	Description
RLGE2FE16R/E	Replace /S with /E in part code for Enhanced Security software package (refer to the Enhanced Security Manual)

Options

Optional Part No	Description
ANT3G-2M	2G/3G External Grade Cellular Antenna with 2M cable (1 required per switch)
ANT3G-5M	2G/3G External Grade Cellular Antenna with 5M cable (1 required per switch)
ANT4G-2M	4G LTE External Grade Cellular Antenna with 2M cable (2 required per switch)

Optional Part No	Description
ANT4G-5M	4G LTE External Grade Cellular Antenna with 5M cable (2 required per switch)
Power Supply	12 V, 24 V or 48 VDC DIN Rail power supply
Conformal Coat	Add suffix '/C' for Conformally Coated Circuit Boards to extend to condensation conditions
SFP Modules[1]	User selection of ComNet SFP (See SFP Modules data sheet for product numbers and compatibility)
DINBKT3	19-inch rack mount panel adapter

If using an RLGE2FE16R unit with cellular modem, please make sure to select the correct configuration of active USB device for your purposes. Refer to the **Cellular modem as a USB device** section.

Graphic View of Hardware

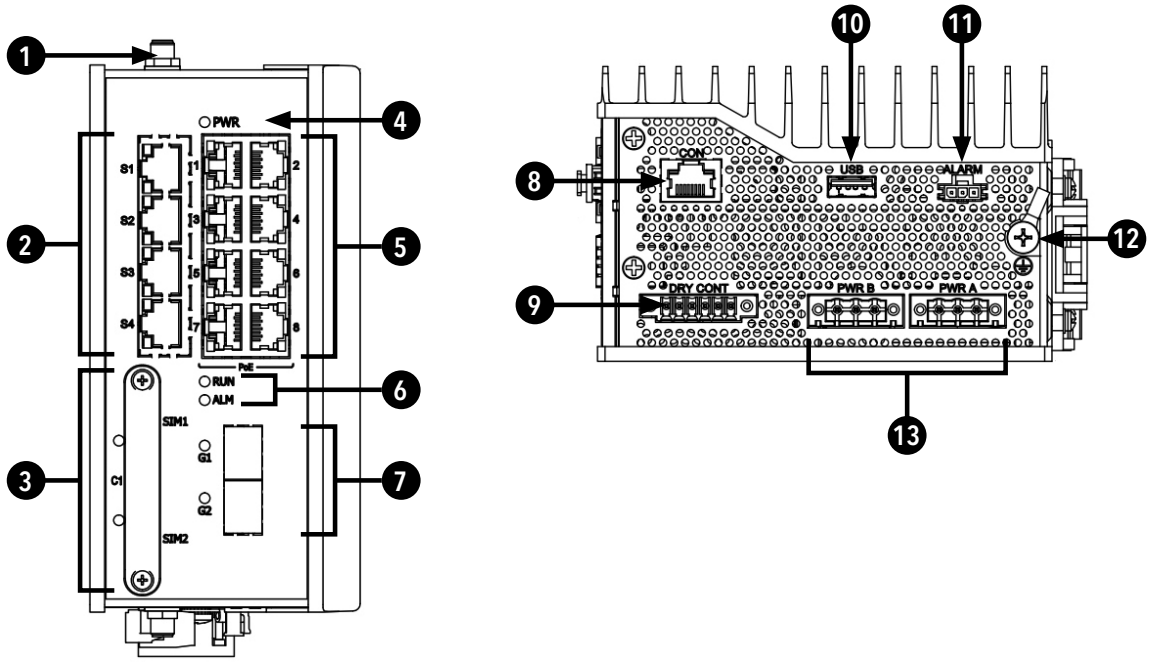
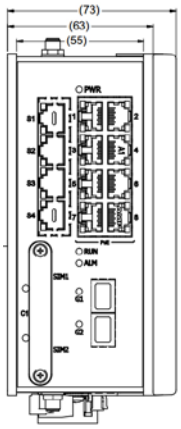


Figure 2 – R/S/22/28 Variant

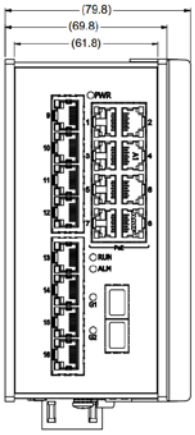
Table 1 – RLGE2FE16R Physical Feature Descriptions

Call-out	Description
1	Antenna Female Connection
2	RS-232 Ports 1 - 4, Link/Activity (L/A) LED Indicators
3	SIM Card Ports 1 - 2
4	Power LED Indicator
5	10/100 TX Ports 1 - 8 with Optional PoE, Link/Activity (L/A) and Speed LED Indicators
6	RUN and ALM LED Indicators
7	1000 FX SFP Ports 1- 2 (Fiber Type and Quantity are dependent on installed SFP) SFP Port Link Status and SFP Port Link Speed LED Indicators
8	Console Interface
9	Dry Contact DI/DO Interface
10	USB Interface
11	Alarm Interface
12	Chassis GND Lug
13	Redundant Power Interfaces

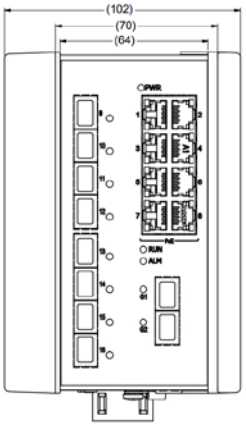
There are several physical varations of this product series dependent on the options selected.



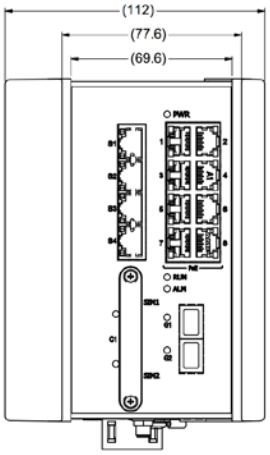
DC Models
8TX Ports



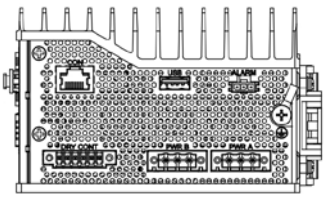
DC Models
16TX Ports



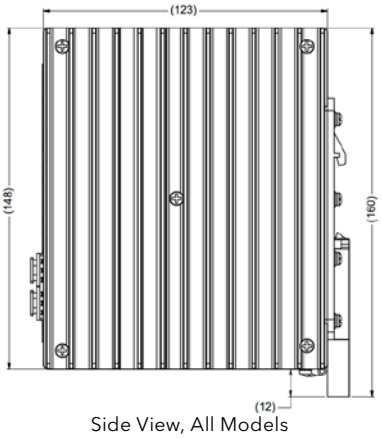
DC Models
8TX + 8SFP Ports



AC Models



Bottom View
(DC 8TX Model Shown)



Side View, All Models

Distance kept for natural air flow

Proper installation depends on natural air flow for cooling. You must maintain a 10cm distance above and below the ComNet switch for proper air flow.

Logical Structure

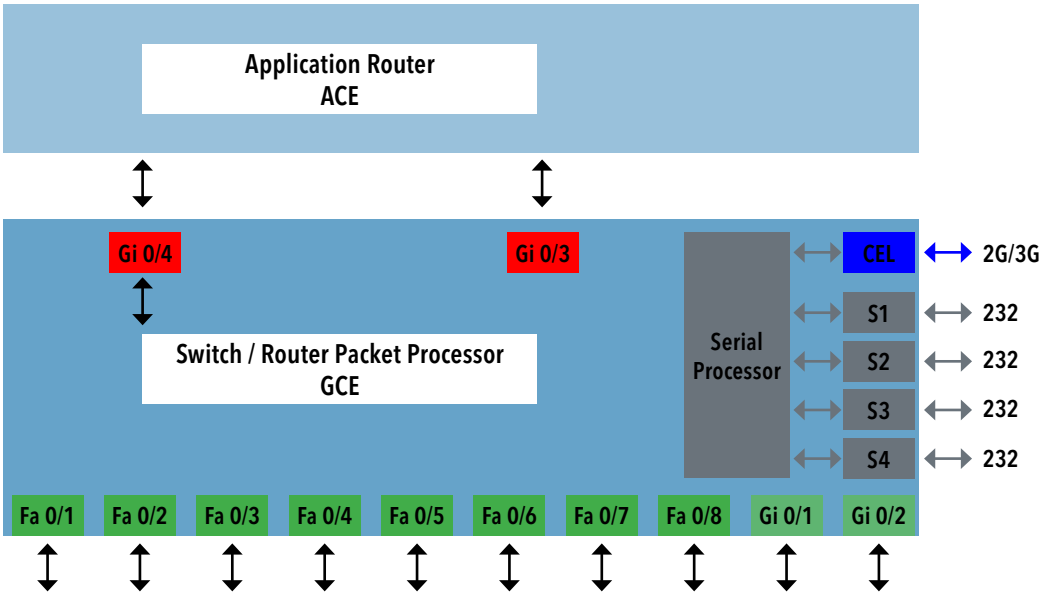


Figure 4 - Logical system view, illustration

Grounding

To install the grounding wire:

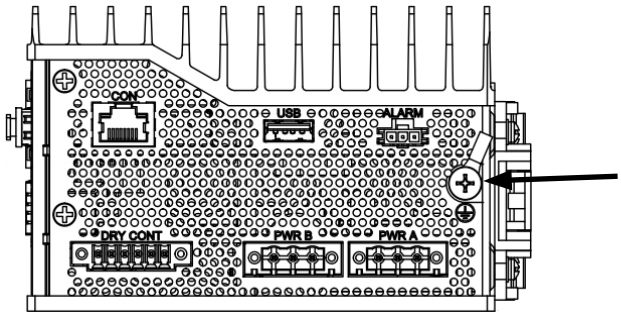
» Prepare a minimum 10 American Wire Gauge (AWG) grounding wire terminated by a crimped two-hole lug. Use a suitable crimping tool to fasten the lug securely to the wire. Adhere to your company's policy as to the wire gauge and the number of crimps on the lug.

» Apply some anti-oxidant onto the metal surface.

» Mount the lug on the grounding posts, replace the spring-washers and fasten the bolts. Avoid using excessive torque.

CAUTION – Do not remove the earth connection unless all power supply connections are disconnected.

DANGER – Before connecting power to the platform, make sure that the grounding posts are firmly connected to a reliable ground, as described below.



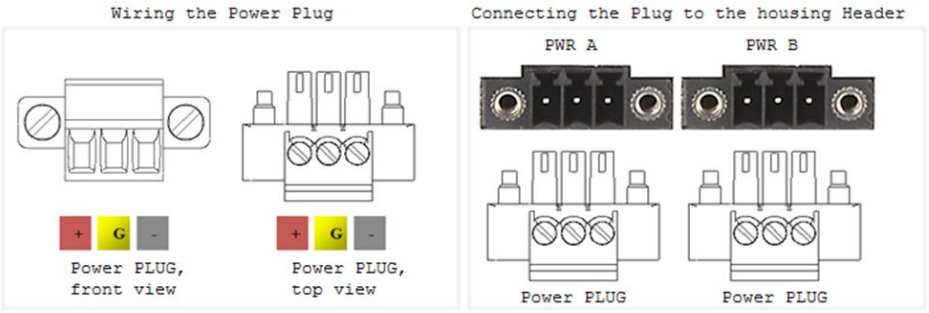
Connecting to a Power Source

Wiring DC Input voltage feed

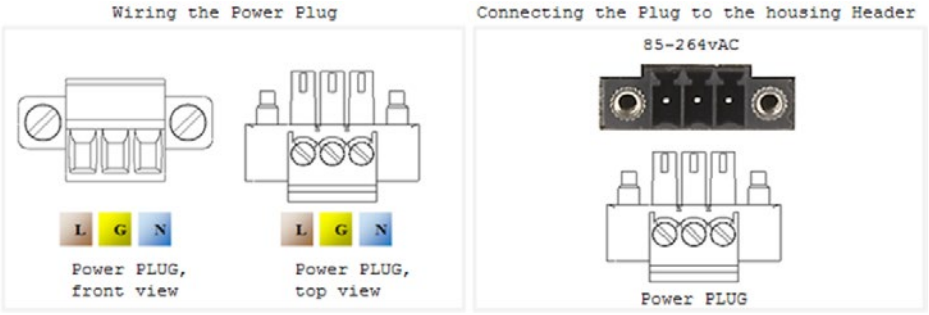
Input voltage can be either AC or DC depending on the specific module you purchased. Please take care to notice the label on the back of the module.

For the DC version there are 2 connection inputs, marked as “PWR A” and “PWR B”. For proper operation it is only necessary to connect one power source, either to “PWR A” or to “PWR B”. However, for redundancy purposes you may connect 2 different power sources one at “PWR A” and the second to “PWR B”.

For wiring the voltage an opposite plug connector (2 pcs) is supplied.



Wiring AC Input voltage connector



For an AC product variant there is a single input connector.

Use a Brown wire for the Line (Phase) conductor, a Green/Yellow for the grounding and a Blue wire for the Neutral conductor. use 18AWG (1mm2) wire, with insulated ferrules.

Power Budget

The following table details power consumption of the Hardware variants with cellular and serial interfaces.

Unit Power feed	Max Power [Watt] Version without POE ports	Max Power [Watt] Version with POE ports
12vDC	18.5	80
24vDC	18.5	100
48vDC	18.5	140
110vDC	18.5	120
220vDC	18.5	120
110vAC	20.35	141
220vAC	20.35	141

Management over Console

Connecting to Device

- Device is capable of being first set up via either the console port, or via an SSH connection
- Default Username and Password
  - Username: su
  - Password: 1234
- Default all ports act as a flat switch, with all ports as members of VLAN 1
- VLAN 1 set to hold an IP interface by default
- Default Management IP:
  - 10.0.0.1/8

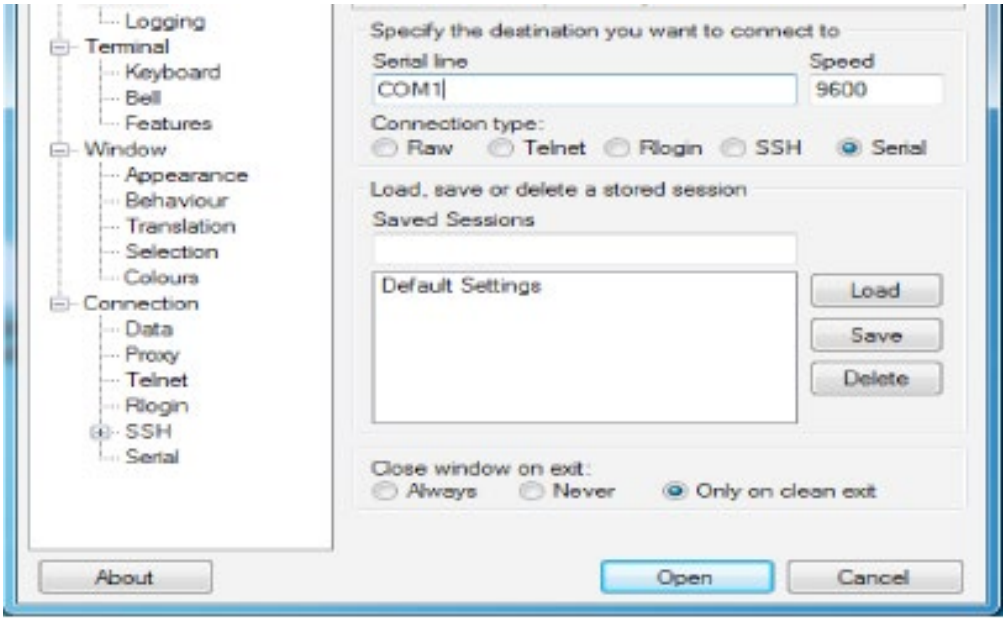
Terminal

» Power on device (Boot may take up to 3 minutes). PWR light should be green

» Console into Device

- Connect to CON port using the white ComNet Console Cable. Other console cables will not work as they have a different pinout.
- Connect to to serial port of PC, or use Serial to USB cable. (Drivers may need to be installed)
- Terminal Serial Connection

1. Install and open terminal software
2. Setup terminal for serial session
3. Determine correct COM port on PC (Device manager)
4. Enter correct COM port, enter correct baud rate speed (Default 9600)
5. Click Open to start session with device



- Press enter if screen is blank
- Default login username su, password 1234 (password will be invisible)

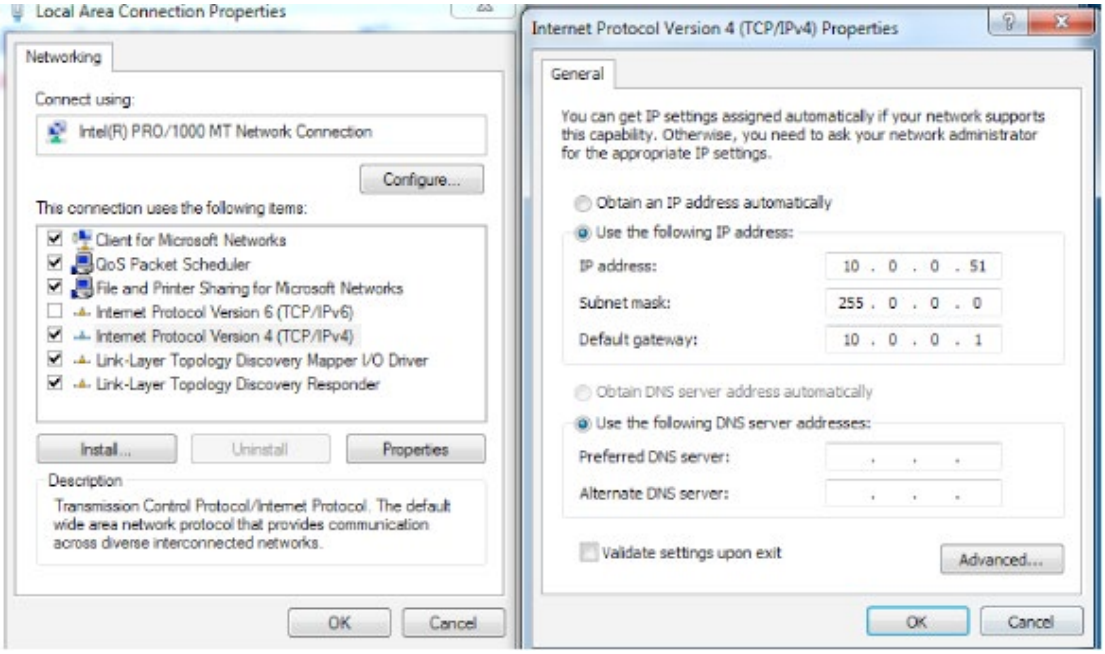
SSH

» SSH Connection to Device

› Setup PC network to be on the same as the default management network

· Example PC Setup:

- IP Address of PC: 10.0.0.51
- Subnet mask: 255.0.0.0
- Gateway: 10.0.0.1 (Optional)



» Ping management VLAN IP: 10.0.0.1

» From any terminal session type: ssh su@10.0.0.1

» Default login username su, password 1234 (password will be invisible)

Configuration Environment

Two CLI based configuration environments are available for the user, these are:

» Global Configuration Environment (GCE)

» Application Configuration Environment (ACE)

These two environments are complementing each other and allowing each a set of supported interfaces, network tools and management. At the RLGE2FE16R infrastructure, the GCE and ACE are representing two different software processing areas. The physical and logical communication between these areas are done by internal switching /routing using the Ethernet gigabit ports Gi 0/3 and Gi 0/4. These are known as the ACE ports.

For additional information about the ACE ports see chapter ACE ports.

Command Line Interface

The CLI (Command Line Interface) is used to configure the RLGE2FE16R from a console attached to the serial port of the switch or from a remote terminal using Telnet or SSH. The following table lists the CLI environments and modes.

Table 3-1: Command Line Interface

Command Mode	Access Method	Prompt	Exit Method
Root	Following user log in this mode is available to the user.	RLGE2FE16R#	To exit this mode would mean the user to log out from the system. Use the command **logout**
Global Configuration Environment (GCE)	Use the command config to enter the Global Configuration mode.	RLGE2FE16R(config)#	To exit to the Root mode, the commands **exit** and **end** are used.
Global Hierarchy Configuration	From the Global Configuration mode command you may drill down to specific feature sub tree. Example is shown here for interface configuration sub tree.	RLGE2FE16R(config-if)#	To exit to the Global Configuration mode, the exit command is used and to **exit** to the Root mode, the **end** command is used.
Application Configuration Environment (ACE)	Use the "**application connect**" from the Privileged mode to enter the application configuration area	[/]	To exit to the Global Configuration mode, the **exit** command is used
Application Hierarchy Configuration	From the application root you may drill down to specific feature sub tree. example is shown here for router configuration sub tree using the command "**router**"	[router/]	To exit to the application root use '..' (two dots). The commands **exit** and **end** are not applicable at this sub tree mode.

Command Line navigation

Minimum Abbreviation

The CLI accepts a minimum number of characters that uniquely identify a command. Therefore, you can abbreviate commands and parameters as long as they contain enough letters to differentiate them from any other available commands or parameters on the specific CLI mode.

GREP

The 'GREP' and 'GREP –V' allows filtering long show outputs.

'GREP <text>'- filter to output lines which includes the given text.

'GREP –v <text>'- filter to output lines which do not include the given text.

Example

1. Show running-config vlan without filtering

```
RLGE2FE16R# show running-config vlan
#Building configuration...
vlan 4091
 ports gigabitethernet 0/1-4

!
!
vlan 1
 ports fastethernet 0/1-8 gigabitethernet 0/1-4 untagged fastethernet 0/1-8 giga
bitethernet 0/1-2

!
!
vlan 4092
 ports gigabitethernet 0/3 fastethernet 0/10-11 untagged fastethernet 0/10-11

!
!
vlan 4093
 ports gigabitethernet 0/3

!
!
```

```
vlan 10
 ports fastethernet 0/1 gigabitethernet 0/3
!
!
mac-address-table static unicast 02:20:d2:fc:1c:78 vlan 4092 interface gigabitet
hernet 0/3
mac-address-table static unicast 02:20:d2:fc:1c:79 vlan 4092 interface fastether
net 0/10
mac-address-table static unicast 02:20:d2:fc:1c:7a vlan 4092 interface fastether
net 0/11
```

2. Show running-config vlan with grep filtering

```
RLGE2FE16R# show running-config vlan | grep vlan
vlan 4091
vlan 1
vlan 4092
vlan 4093
vlan 10
mac-address-table static unicast 02:20:d2:fc:1c:78 vlan 4092 interface gigabitet…
mac-address-table static unicast 02:20:d2:fc:1c:79 vlan 4092 interface fastether…
mac-address-table static unicast 02:20:d2:fc:1c:7a vlan 4092 interface fastether…
```

Dynamic Completion of Commands

In addition to the Minimum Abbreviation functionality, the CLI can display the commands' possible completions. To display possible command completions, type the partial command followed immediately by <Tab>.

In case the partial command uniquely identifies a command, the CLI displays the full command. Otherwise the CLI displays a list of possible completions.

Help (?)

Use **?** to retrieve completion options and help for a command.

Keyboard Shortcuts

Following keyboard shortcuts are supported.

1. 'CTRL D'
    a. At the GCE: moves one CLI mode back.
    b. At the ACE: exits to GCE Root.
2. 'CTRL Z'
    a. At the GCE: moves to the ROOT.

Supported Functionalities

The RLGE2FE16R is a feature rich industrial unit supporting:

» L2 Ethernet switching
» L3 dynamic and static Routing
» SCADA services
» Firewall
» Secure networking

The below table gives a high level view of the supported feature sets and their corresponding configuration environment.

Global Configuration Environment GCE		**Application Configuration Environment ACE**	
L2 Ethernet switching	Ethernet ports	Serial ports	Cellular modem
OSPF	Vlan tagging	IPSec	VPN
Management	Authentication	SCADA Gateway	SCADA Firewall
L2-L4 Firewall	QOS	Serial services	Terminal services
ERP	MSTP	OSPF	RIP
FTP	SNMP	NAT	

The below table details the RLGE2FE16R supported feature and its corresponding configuration environment.

Group	**Feature**	**GCE**	**ACE**
Interfaces	Cellular modem with 2 SIM cards		X
	FE RJ45 Ports	X	
	Fiber Optic ports	X	
	Gigabit ports	X	
	POE ports	X	
	RS 232 ports ,with control lines		X
	SFP Ports	X	
	USB	X	

Group	Feature	GCE	ACE
Switching Management	802.1	X	
	Auto Crossing	X	
	Auto Negotiation IEEE 802.3ab	X	
	Mac list	X	
	Storm Control	X	
	VLAN segregation Tagging IEEE 802.1q	X	
	IGMP Snooping	X	
	IGMP v1,v2,v3	X	
	Backup / Restore running config	X	
	Conditioned/ scheduled system reboot	X	
	Console serial port	X	
	FTP client	X	
	Inband Management	X	
	Outband Management	X	
	Remote Upgrade	X	
	Safe Mode	X	
	SFTP Client	X	
	SNMP Trap	X	
	SNMP	X	
	SSH Client	X	X
	Syslog	X	X
	Telnet Client	X	X
	Telnet server	X	X
	TFTP Client	X	
	Web management interface	X	
Networking	LLDP	X	
	OAM CFM ITU-T Y.1731	X	
	QOS	X	
Protection	Conditioned/ scheduled system reboot		X
	ITU-T G.8032v2 Ethernet ring	X	
	Link Aggregation with LACP	X	
	MSTP IEEE 802.1s	X	
	Protection between Cellular ISP (SIM cards backup)	X	
	Spanning Tree	X	

Group	Feature	GCE	ACE
Routing	DHCP Client	X	
	DHCP Relay	X	
	DHCP Server	X	
	IPv4	X	X
	OSPF v2	X	X
	RIPv2		X
	Static Routing	X	X
	VRRP	X	
	NAT		X
Security	ACLs , L2-L4	X	
	Application aware IPS Firewall for SCADA protocols	X	
	IEEE 802.1X Port Based Network Access Control.	X	
	IPSec		X
	Local Authentication	X	
	MAC limit	X	
	Port shutdown	X	
	RADIUS Accounting and Authentication	X	
	TACACS	X	
Time	Local Time settings	X	
	NTP	X	
Diagnostics	Counters & statistics per Port	X	
	Led diagnostics	X	
	Ping	X	X
	Port mirroring	X	
	Relay Alarm Contact	X	
	RMON	X	
	Trace Route	X	
Serial Gateway	IEC 101/104 gateway		X
	IEC 104 Firewall		X
	Serial Transparent Tunneling		X
	Terminal Server		X
VPN	L2 GRE VPN		X
	L3 IPSec VPN		X
	L3 mGRE DM-VPN		X

System Default state

The following table details the default state of features and interfaces.

Feature	Default state
Ethernet Ports	All ports are enabled
Serial interfaces	Disabled
Cellular modem	Disabled
Vlan 1	Enabled. All ports are members
Ports PVID	All Ethernet ports have pvid 1
POE	POE is enabled for supporting hardware
Layer 3 interface	Interface vlan 1 is set to : 10.0.0.1/8
Spanning Tree	Mst is enabled. Application ports gigabit 0/3-0/4 are edge ports. Depending on hardware type ports fast 0/9-0/16 may be edge ports as well (/216 and /288 model variants)
ERP	Disabled
LLDP	Disabled
SSH	Enabled
Telnet	Disabled
Http	Disabled
Syslog	Disabled
Snmp	Disabled
Tacacs	Disabled
Radius	Disabled
ACLs	Disabled
SNTP	Disabled
Firewall	Disabled
VPN	Disabled

Root Commands

The Root Configuration Environment list of main CLI commands is shown below

+ root
  - help
  - clear screen
  - enable
  - disable
  - configure terminal / configure
  - run script
  - listuser
  - lock
  - username
  - enable password
  - line
  - access-list provision mode
  - access-list commit
  - exec-timeout
  - logout
  - end
  - exit
  - show privilege
  - show line
  - show aliases
  - show users
  - show history

Root Commands Description

Command	Description
Help [command]	Displays a brief description for the given command. To display help description for commands with more than one word, do not provide any space between the words
clear screen	Clears all the contents from the screen.
Enable [<0-15> Enable Level]	Enters into default level privileged mode. If required, the user can specify the privilege level by enabling level with a password (login password) protection to avoid unauthorized user.
Disable [<0-15> Enable Level]	Turns off privileged commands. The privilege level varies between 0 and 15. This value should be lesser than the privilege level value given in the enable command.
configure [terminal]	Enters configuration mode.
run script	Runs CLI commands from the specified script file.
listuser	Lists all the default and newly created users, along with their permissible mode.
Lock	Locks the CLI console. It allows the user/system administrator to lock the console to prevent unauthorized users from gaining access to the CLI command shell. Enter the login password to release the console lock and access the CLI command shell.
username	Creates a user and sets the enable password for that user with the privilege level.
alias - replacement string	Replaces the given token by the given string and the no form of the command removes the alias created for the given string.
access-list commit	Triggers provisioning of active filter rules to hardware based on configured priority. This command is applicable only when provision mode is consolidated. Traffic flow would be impacted when filter-rules are reprogrammed to hardware.
logout	Exits the user from the console session. In case of a telnet session, this command terminates the session.
end	Exits the configuration mode
exit	Exits the current config location to one step up in the root
show privilege	Shows the current user privilege level
show line	Displays TTY line information such as EXEC timeout
show aliases	Displays all the aliases
show users	Displays the information about the current user.
show history	Displays a list of recently executed commands

GCE Commands

The Global Configuration Environment list of main CLI commands is shown below

+ root

+ config terminal

default vlan id

default ip address

ip address

default ip address allocation protocol

ip address - dhcp

login authentication

login authentication-default

authorized-manager ip-source

ip http port

set ip http

archive download-sw

interface-configuration and deletion

mtu frame size

system mtu

loopback local

mac-addr

snmp trap link-status

write

copy

clock set

cli console

flowcontrol

shutdown - physical/VLAN/port-channel/tunnel Interface

debug interface

debug-logging

incremental-save

rollback

shutdown ospf

start ospf

set switch maximum – threshold

set switch temperature – threshold

set switch power – threshold

mac-learn-rate

system contact

system location

clear interfaces – counters

clear counters

show ip interface

show authorized-managers

show interfaces

show interfaces – counters

show system-specific port-id

show interface mtu

show interface bridge port-type

show nvram

show env

show system information

show flow-control

show debug-logging

show debugging

show clock

show running-config

show http server status

show mac-learn-rate

show config log

management vlan-list <port_list>

show iftype protocol deny table

clear line vty

audit-logging logsize-threshold

feature telnet

show telnet server

show audit

set http authentication-scheme

set http redirection enable

http redirect

show http authentication-scheme

show http redirection

GCE Commands Description

Command	Description
default mode	Configures the mode by which the default interface gets its IP address.
default vlan id	
default ip address	Configures the IP address and subnet mask for the default interface.
ip address	Sets the IP address for an interface. The no form of the command resets the IP address of the interface to its default value.
default ip address allocation protocol	Configures the protocol used by the default interface for acquiring its IP address.
ip address - dhcp	Configures the current VLAN interface to dynamically acquire an IP address from a DHCP server.
login authentication	Configures the authentication method for user logins for accessing the GUI to manage the switch.
login authentication-default	Configures the authentication method for user logins for accessing the GUI to manage the switch.
authorized-manager ip-source	Configures an IP authorized manager and the no form of the command removes manager from authorized managers list.
ip http port	Sets the HTTP port. This port is used to configure the router using the Web interface. The value ranges between 1 and 65535. The no form of the command resets the HTTP port to its default value.
set ip http	Enables/disables HTTP in the switch.
mtu frame size	Configures the maximum transmission unit frame size for all the frames transmitted and received on all the interfaces in a switch.
snmp trap link-status	Enables trap generation on the interface. The no form of this command disables trap generation on the interface.
clock set	Manages the system clock.
Delete startup-cfg	Clears the contents of the startup configuration
cli console	Enables the console CLI through a serial port. The no form of the command disables console CLI.
flowcontrol	Set the send or receive flow-control value for an interface
[no] shutdown - physical/VLAN/port interface	Disables/enables a physical interface / VLAN interface / port-channel interface
debug interface	Sets the debug traces for all the interfaces. The no form of the command resets the configured debug traces.
debug-logging	Configures the displays of debug logs. Debug logs are directed to the console screen or to a buffer file, which can later be uploaded, based on the input.
incremental-save	Enables/disables the incremental save feature
auto-save trigger	Enables / disables the auto save trigger function.
Rollback { enable | disable }	Enables/disables the rollback function.
set switch maximum – threshold	Sets the switch maximum threshold values of RAM, CPU, and Flash
set switch temperature – threshold	Sets the maximum and minimum temperature threshold values of the switch in Celsius.
mac-learn-rate	Configures the maximum number of unicast dynamic MAC (L2) MAC entries hardware can learn on the system
system contact	
system location	

Command	Description
clear interfaces – counters	
clear counters	
show ip interface	
show authorized-managers	
show interfaces	
show interfaces – counters	
show interface mtu	
show interface bridge port-type	
show nvram	Displays the current information stored in the NVRAM.
show env	Displays the status of the all the resources like CPU, Flash and RAM usage, and also displays the current, power and temperature of the switch.
show system information	Displays system information.
show flow-control	
show debug-logging	
show debugging	
show clock	
show running-config	
show http server status	
show mac-learn-rate	
port-isolation in_vlan_ID	
show port-isolation	
audit-logging reset	
show config log	
memtrace	
show memtrace status	
management vlan-list <port_list>	
show iftype protocol deny table	
clear line vty	
login block-for	
audit-logging logsize-threshold	
feature telnet	
show telnet server	
show audit	
set http authentication-scheme	
set http redirection enable	
http redirect	
show http authentication-scheme	
show http redirection	
audit-logging reset	
show config log	
clear line vty	
tunnel hop-limit	

Command	Description
tunnel hop-limit	
login block-for	
audit-logging logsize-threshold	
feature telnet	
show telnet server	
show audit	
set http authentication-scheme	
set http redirection enable	
http redirect	
show http authentication-scheme	
show http redirection	
audit-logging reset	
default rm-interface	
show config log	
show memtrace status	
management vlan-list <port_list>	
show iftype protocol deny table	
clear line vty	
audit-logging logsize-threshold	
feature telnet	
show telnet server	
show audit	
set http authentication-scheme	
set http redirection enable	
http redirect	
show http authentication-scheme	
show http redirection	
audit-logging reset	
show config log	
management vlan-list <port_list>	
internal-lan	
show iftype protocol deny table	
clear line vty	
login block-for	
audit-logging logsize-threshold	
feature telnet	
show telnet server	
show audit	
set http authentication-scheme	
set http redirection enable	
http redirect	

Command	Description
show http authentication-scheme	
show http redirection	
audit-logging reset	
show config log	
show iftype protocol deny table	
clear line vty	
login block-for	

ACE Commands

The Application Configuration Environment list of main CLI commands is shown below.

+ Application connect
    + Router {interface | route |static |ospf |ip |rip| NAT}
    + cellular { connection | continuous-echo| disable |enable| modem| network| refresh| settings| show| wan}
    + capture {delete |export |help |show |start |stop}
    + date
    + discrete {service| show}
    + dm-vpn {multipoint-gre| nhrp}
    + dns {host| resolver}
    + exit
    + firewall {log| profile| tcp| serial}
    + idle-timeout
    + iec101-gw {cnt| operation| config iec-101| config iec-104| config gw| show}
    + ipsec {enable| disable| isakmp update| policy| preshared| log-show| show| show-sa proto}
    + ipsec-vpn tunnel {show | create | remove}
    + l2-vpn {fdb| tunnel| nhrp}
    + ping
    + reload {cancel| schedule| show}
    + schedule {add |show |remove}
    + serial {card |port| local-end-point| remote-end-point}
    + ssh
    + ssh-server user {create| remove| show}
    + syslog show
    + telnet
    + terminal-server {admin-status| counters| settings| connections| serial-tunnel| telnet-service}
    + trace
    + version

Main Show Commands

GCE

[System Information]

- os-image show-list
- show system information
- show env all

[Vlan & Ports]

- show vlan
- show running-config interface fastethernet 0/<1-8>
- show running-config interface gigabitethernet 0/<1-2>
- show vlan port config
- show interfaces status

[ACLs]

- show running-config acl

[FDB]

- show mac-address-table
- show ip arp
- show logging
- show interfaces storm-control

[GCE Routing]

- show ip interface
- show ip route
- show ip ospf
- show ip ospf neighbor
- show running-config ospf
- show ip rip database
- show ip rip statistics
- show running-config rip

[SNMP]

- show running-config snmp

[STP]

- show spanning-tree detail
- show spanning-tree summary

[ERP]

- show running-config ecfm
- show ethernet cfm domain
- show ethernet cfm service
- show ethernet cfm maintenance-point local
- show ethernet cfm maintenance-points remote
- show ethernet cfm global information
- show aps ring
- show aps ring global info

ACE

[ACE Routing]

- router interface show
- router route show
- router static

  enable

  show running-config

  show ip route

  exit
- router ospf

  enable

  show running-config

  show ip ospf route

show ip ospf neighbor

show ip ospf interface

exit

- router rip

enable

show running-config

show ip rip

exit

[Cellular]

- cellular wan show
- cellular settings show
- cellular network show
- cellular connection show

[VPN & IPSec]

- application connect
- dm-vpn multipoint-gre
- dm-vpn nhrp map
- dm-vpn nhrp map
- dm-vpn nhrp route-show
- l2-vpn tunnel show
- l2-vpn fdb show
- l2-vpn nhrp spoke show
- l2-vpn nhrp hub show
- ipsec-vpn tunnel show
- ipsec show global-defs
- ipsec show preshared
- ipsec show sa
- ipsec show log

[Serial]

- serial card show
- serial port show
- serial local-end-point show
- serial port show slot <4-9> port <1-4>
- serial remote-end-point show
- iec101-gw show all
- terminal-server settings show
- terminal-server connections show

[Firewall]

- show running-config acl
- show access-lists
- firewall log show
- firewall profile show
- firewall tcp show

System Version and Data Base

Configuration Database

By default, User configuration is saved in a file called **RLGE2FE16R.conf**. Configuration saved in this file will be available at system startup. If this file is deleted, the system will boot with the **RLGE2FE16Rnvram.txt** file holding factory configuration.

User Configuration is taking effect immediately upon entering. No specific COMMIT command is required.

The user can as well save his running configuration in a file with a chosen name for backup and boot the system with this file when needed.

Multiple running configuration files can be saved with different names locally on the flash or at an TFTP /SFTP server.

However, configuration which will not be saved as below example will not be available following system reboot.

User configuration is saved (to the RLGE2FE16R.conf) using the following command

```
RLGE2FE16R# write startup-cfg
Building configuration...
[OK]
```

Removing all user configuration and setting the switch to its factory defaults is done by erasing the RLGE2FE16R.conf with the following command

```
RLGE2FE16R# delete startup-cfg
RLGE2FE16R# reload
```

NOTE – RLGE2FE16R.conf and RLGE2FE16Rnvram.txt files are not accessible for the user to do file operations on (copy, rename and such)

OS VERSION

Updating of system version is available by TFTP/SFTP server and via the USB port.

Available OS files on the switch can be seen with the command shown below.

Running OS file is marked with “active”.

Upgrading system OS from a USB drive can be done under safe mode interface or under a running system assuming the USB drive was in place when the system booted.

NOTE – The OS image file is a tar file type. When upgrading the system from the USB the file should be placed at the root directory of the USB drive. The file should not be unzipped.

NOTE – The USB drive must be FAT32

NOTE – The RLGE2FE16R can hold a maximum of two OS image files. Before downloading a new OS file to the switch make sure the RLGE2FE16R has on it only one (the active) file. If needed, delete the unused file before attempting to download the new version.

Running Configuration

The user can save his running configuration to a file with a chosen name for backup and boot the system with this file when needed.

Multiple running configuration files can be saved with different names locally on the flash or at a TFTP /SFTP server.

It is also possible to import/export a running configuration file to a USB drive from the safe mode.

Commands Hierarchy

+ Root

- write startup-cfg

- delete startup-cfg

- os-image show-list

- os-image activate flash:<file_name>

- os-image delete flash: <file_name>

- os-image download-sw flash:<file_name>

- os-image download-sw sftp://user:password@aa.bb.cc.dd/file_name

- os-image download-sw tftp://aa.bb.cc.dd/file_name

- startup-config {import | export}
  [flash: <file_name> |
  sftp://user:password@aa.bb.cc.dd/<file_name> |
  tftp://aa.bb.cc.dd/<file_name>]

- logs-export [flash: <file_name> |
  sftp://user:password@aa.bb.cc.dd/<file_name> |
  tftp://aa.bb.cc.dd/<file_name>]

- startup-config show files
- reload

NOTE – System must be rebooted following activation of a new OS image file

Example upgrade the OS from USB

The following flow will demonstrate how to upgrade the OS image file from a USB.

Connect to the switch via console and establish CLI management.

Have a USB stick, formatted to FAT32, holding the OS version at its root directory.

1. Display available OS files

```
RLGE2FE16R# os-image show-list
Versions list:
RF _ RLGE2FE16R _ 3.5.03.11 (active)
RF _ RLGE2FE16R _ 3.1.00.25.tar
```

2. Deleting unneeded OS files

```
RLGE2FE16R# os-image delete flash:RF _ 3.1.00.25.tar
RLGE2FE16R# os-image show-list
Versions list:
RF _ RLGE2FE16R _ 3.5.03.11 (active)
RLGE2FE16R#
```

3. Downloading OS file from USB

```
Command syntax:
RLGE2FE16R# os-image download-sw flash:<file _ name>
Example:
RLGE2FE16R# os-image download-sw flash:RF _ RLGE2FE16R _ 3.5.04.15.tar
RLGE2FE16R# os-image show-list
Versions list:
RF _ RLGE2FE16R _ 3.5.03.11 (active)
RF _ RLGE2FE16R _ 3.5.04.15.tar
RLGE2FE16R#
```

4. Activating desired OS file (will automatically reboot the device)

```
RLGE2FE16R# os-image activate flash:RF _ RLGE2FE16R _ 3.5.04.15.tar
RLGE2FE16R# os-image show-list
Versions list:
RF _ RLGE2FE16R _ 3.5.03.11
RF _ RLGE2FE16R _ 3.5.04.15.tar (active)
```

Example upgrade the OS from SFTP

The following flow will show how to upgrade the OS image file from a SFTP server.

1. Display available OS files

```
RLGE2FE16R# os-image show-list
Versions list:
RF _ RLGE2FE16R _ 3.5.03.11 (active)
RF _ RLGE2FE16R _ 3.1.00.25.tar
```

2. Deleting unneeded OS files

```
RLGE2FE16R# os-image delete flash:RF _ 3.1.00.25.tar
RLGE2FE16R# os-image show-list
Versions list:
RF _ RLGE2FE16R _ 3.5.03.11 (active)
RLGE2FE16R#
```

3. Downloading OS file from sftp

```
Command syntax:
RLGE2FE16R# os-image download-sw sftp://user:password@aa.bb.cc.dd/file _ name
Example:
RLGE2FE16R# os-image download-sw sftp://user:user@172.17.203.100/RF _ RLGE2FE16R _ 3.5.04.15.tar
----25%-------50%-------75%------100%

RLGE2FE16R# os-image show-list
Versions list:
RF _ RLGE2FE16R _ 3.5.03.11 (active)
RF _ RLGE2FE16R _ 3.5.04.15.tar
RLGE2FE16R#
```

4. Activating desired OS file (will automatically reboot the device)

```
RLGE2FE16R# os-image activate flash:RF _ RLGE2FE16R _ 3.5.04.15.tar
Switch booting…

RLGE2FE16R# os-image show-list
Versions list:
RF _ RLGE2FE16R _ 3.5.03.11
RF _ RLGE2FE16R _ 3.5.04.15.tar (active)
```

5. Exporting configuration data base to SFTP server

```
Command syntax:
RLGE2FE16R# startup-config export sftp://user:password@aa.bb.cc.dd/file _ name.
Example:
RLGE2FE16R# startup-config export sftp://rad:rad@172.18.212.230/config _ january13
```

Example export db and logs

The following flow will show how to export configuration and logs to a TFTP server

1. Exporting configuration data base to SFTP server

```
Command syntax:
RLGE2FE16R# startup-config export sftp://user:password@aa.bb.cc.dd/file _ name.
Example:
RLGE2FE16R# startup-config export sftp://rad:rad@172.18.212.230/config _ january13
```

2. Exporting logs base to SFTP server

```
Command syntax:
RLGE2FE16R# logs-export sftp://<user-name>:<pass-word>@ip-address/filename
Example:
RLGE2FE16R# logs-export sftp://rad:rad@172.18.212.230/logs _ january13
```

Example handling DB files on flash

The following flow will show how to export configuration as a file to the local flash drive

1. Exporting configuration data

```
RLGE2FE16R# startup-config export flash:db _ march

RLGE2FE16R# startup-config show files
db _ february
db _ test
db _ march
```

2. Activating DB file from flash

```
RLGE2FE16R# startup-config import flash: db _ february
 startup-config import Successful
 Reload to use new db
RLGE2FE16R# reload
```

Example Import DB from TFTP

The following flow will show how to import configuration from a TFTP server

1. Establish connectivity between the switch and the TFTP server

2. Start importing the target file

```
RLGE2FE16R# startup-config import tftp://172.18.212.231/RF1 _ ospf.cfg

downloaded size:2408448 Bytes
 startup-config import Successful
 Reload to use new db
```

3. Reload the switch for the data base to take effect

```
RLGE2FE16R# reload
..
..
RF1 login: su
Password:
<129>Mar 10 09:06:28 RF1 CLI Attempt to login as su via console Succeeded
RF1#
```

Safe Mode

The system has two safe mode menus available. To access safe mode, connect to the switch via console cable, reboot the unit and interrupt the boot process at the safe mode prompt.

The first Safe mode is used for approved technician only and should not be used unless specified by ComNet. This safe mode state is available at the prompt

"For first safe mode Press 's'..."

The second safe mode is accessible at the following prompt:

##########################

For safe mode Press 's'...

##########################

Below screenshot details the 2 safe mode menus and their options for:

1. system reset

2. Load the factory-default configuration for the device

3. Write to EEPROM (should be used only after consulting with ComNet)

4. Recover the device's images from a package file

5. Export / Import DB (running configuration)

```
For first safe mode Press 's'...
s
Safe mode requested from boot...
--------------------------------------------------------------------------------
|safe mode menu:
|
|      reset               | 1 :  Reset the device
|
|      format              | 2 :  Format flash
|
|      activate           | 3 :  Activate sw version on flash
|
|      install             | 4 :  Install first sw version from USB
|
|      other               | o :  write other type field
|
|      continue           | c :  Continue with start up process
|
|      help                | H :  Display help about this utility
|
```

```
--------------------------------------------------------------------------------------------c
Extracting software
|s
OK
01/01/70 00:25:34 Running applications
##########################
For safe mode Press 's'...
##########################
-------------------------------------------------------------------------------------------
|safe mode menu:
|      reset               | 1 :  Reset the device
|      defcfg              | 2 :  Load the factory-default configuration for the device
|      eeprom              | 3 :  Write to EEPROM
|      recover             | 4 :  Recover the device's images from a package file
|      db                  | 5 :  Export / Import DB
|      continue            | c :  Continue in start up process
|      refresh             | r :  Refresh menu
|      help                | H :  Display help about this utility
-------------------------------------------------------------------------------------------|
```

SW Image upgrade and Recovery

From the second safe mode, select option 4 "Recover the device's images from a package file".

At this sub menu the user can handle system version update ,activatation or restore.

```
-------------------------------------------------------------------------------------------
|safe mode menu:
|      reset               | 1 :  Reset the device
|      defcfg              | 2 :  Load the factory-default configuration for the device
|      eeprom              | 3 :  Write to EEPROM
|      recover             | 4 :  Recover the device's images from a package file
|      db                  | 5 :  Export / Import DB
|      continue            | c :  Continue in start up process
|      refresh             | r :  Refresh menu
|      help                | H :  Display help about this utility
-------------------------------------------------------------------------------------------
4

#############################################################################
```

```
###   Device Image Recovery   ########################################
#####################################################################
 usb             | 1 :  Download the package file from USB
 ls              | 2 :  List the available application files
 active          | 3 :  Change the active working application
 show            | 4 :  Display the active working application
 remove          | 5 :  Delete an application
 free            | 6 :  Display the free space in the application file system
 main            | X :  Return to the main menu
 help            | H :  Display help about this menu
```

Install OS image update from a USB

Follow below steps as an example of uploading a desired OS image stored on a local USB key and activating it.

1. Access second safe mode, use option 4 “recover” and list the current OS images available at the switch.

```
-------------------------------------------------------------------------------------
|safe mode menu:
|      reset              | 1 :  Reset the device
|      defcfg             | 2 :  Load the factory-default configuration for the device
|      eeprom             | 3 :  Write to EEPROM
|      recover            | 4 :  Recover the device’s images from a package file
|      db                 | 5 :  Export / Import DB
|      continue           | c :  Continue in start up process
|      refresh            | r :  Refresh menu
|      help               | H :  Display help about this utility
-------------------------------------------------------------------------------------
4


#####################################################################
###   Device Image Recovery   ########################################
#####################################################################
 usb             | 1 :  Download the package file from USB
 ls              | 2 :  List the available application files
 active          | 3 :  Change the active working application
 show            | 4 :  Display the active working application
 remove          | 5 :  Delete an application
 free            | 6 :  Display the free space in the application file system
```

```
 main             | X :  Return to the main menu
 help             | H :  Display help about this menu

2
List of sw versions:
3.5.04.32 (active)
3.5.04.15
```

2. Delete the unused OS-Image file

```
-------------------------------------------------------------------------------------
|safe mode menu:
|      reset               | 1 :  Reset the device
|      defcfg              | 2 :  Load the factory-default configuration for the device
|      eeprom              | 3 :  Write to EEPROM
|      recover             | 4 :  Recover the device's images from a package file
|      db                  | 5 :  Export / Import DB
|      continue            | c :  Continue in start up process
|      refresh             | r :  Refresh menu
|      help                | H :  Display help about this utility
-------------------------------------------------------------------------------------
4

#########################################################################
###   Device Image Recovery   ###########################################
#########################################################################
 usb              | 1 :  Download the package file from USB
 ls               | 2 :  List the available application files
 active           | 3 :  Change the active working application
 show             | 4 :  Display the active working application
 remove           | 5 :  Delete an application
 free             | 6 :  Display the free space in the application file system
 main             | X :  Return to the main menu
 help             | H :  Display help about this menu

5
List of sw versions:
3.5.04.32 (active)
3.5.04.15
Enter version name
```

```
For main menu press X
3.5.04.15
Removing version 3.5.04.15
Version was deleted successfully
```

3. Download a new OS Image file from the usb. A list of available files at the usb will be displayed. Copy the complete file name and path. Below examples relates to version 4.0.02.10.tar

```
-------------------------------------------------------------------------------
|safe mode menu:
|      reset               | 1 :  Reset the device
|      defcfg              | 2 :  Load the factory-default configuration for the device
|      eeprom              | 3 :  Write to EEPROM
|      recover             | 4 :  Recover the device's images from a package file
|      db                  | 5 :  Export / Import DB
|      continue            | c :  Continue in start up process
|      refresh             | r :  Refresh menu
|      help                | H :  Display help about this utility
-------------------------------------------------------------------------------
4
#########################################################################
###   Device Image Recovery   #########################################
#########################################################################
 usb              | 1 :  Download the package file from USB
 ls               | 2 :  List the available application files
 active           | 3 :  Change the active working application
 show             | 4 :  Display the active working application
 remove           | 5 :  Delete an application
 free             | 6 :  Display the free space in the application file system
 main             | X :  Return to the main menu
 help             | H :  Display help about this menu

1
-rw-rw-rw-    1 root     root      58112000 Jan 21  2014 /mnt/usb/RF _ RLGE2FE16R _ 3.5.04.15.
tar
-rw-rw-rw-    1 root     root      59494400 Apr  7  2014 /mnt/usb/RF _ RLGE2FE16R _ 3.5.04.31.
tar
-rw-rw-rw-    1 root     root      59555840 Jun  5  2014 /mnt/usb/RF _ RLGE2FE16R _ 3.6.04.24.
tar
-rw-rw-rw-    1 root     root      59842560 Jun  2  2014 /mnt/usb/RF _ RLGE2FE16R _ 4.0.02.10.
tar
Enter version number on usb.
```

```
For main menu press X
/mnt/usb/RF _ RLGE2FE16R _ 4.0.02.10.tar
Version was installed successfully
```

4. Activate the new version. The system will boot

```
-------------------------------------------------------------------------------------
|safe mode menu:
|      reset               | 1 :  Reset the device
|      defcfg              | 2 :  Load the factory-default configuration for the device
|      eeprom              | 3 :  Write to EEPROM
|      recover             | 4 :  Recover the device's images from a package file
|      db                   | 5 :  Export / Import DB
|      continue            | c :  Continue in start up process
|      refresh             | r :  Refresh menu
|      help                | H :  Display help about this utility
-------------------------------------------------------------------------------------
4
#######################################################################
###   Device Image Recovery   ########################################
#######################################################################
 usb              | 1 :  Download the package file from USB
 ls               | 2 :  List the available application files
 active           | 3 :  Change the active working application
 show             | 4 :  Display the active working application
 remove           | 5 :  Delete an application
 free             | 6 :  Display the free space in the application file system
 main             | X :  Return to the main menu
 help             | H :  Display help about this menu

3
List of sw versions:
3.5.04.32 (active)
4.0.02.10
Enter version to activate
For main menu press X
4.0.02.10
Updating bank1 with vmlinux.UBoot file, please wait ...
```

Installing First OS image from a USB

Follow below steps as an example of installing a first version from a usb. Local database and any active OS image will be deleted. The system will boot with manufacturing defaults using the new OS imported file.

1. Access first safe mode, use option 4 “install”. Select the version to be used. the system will boot automatically to activate the new OS.

```
-------------------------------------------------------------------------------------------
Safe mode requested from boot...
-------------------------------------------------------------------------------------------
|safe mode menu:
|
|      reset               | 1 :  Reset the device
|
|      format              | 2 :  Format flash
|
|      activate            | 3 :  Activate sw version on flash
|
|      install             | 4 :  Install first sw version from USB
|
|      other               | o :  write other type field
|
|      continue            | c :  Continue with start up process
|
|      help                | H :  Display help about this utility
|
-------------------------------------------------------------------------------------------
4


!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!! This choice will delete data from flash !!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!               Continue [y/n]                !!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!


y
-rw-rw-rw-     1 root      root      58112000 Jan 21   2014 /mnt/usb/RF _ RLGE2FE16R _ 3.5.04.15.
tar
-rw-rw-rw-     1 root      root      59842560 Jun  2   2014 /mnt/usb/RF _ RLGE2FE16R _ 4.0.02.10.
tar
Enter version number on usb.
For main menu press X
/mnt/usb/RF _ RLGE2FE16R _ 3.5.04.15.tar
```

```
Veryfing sw version RF _ RLGE2FE16R _ 3.5.04.15.tar
bcm _ sdk _ iss _ app.tar.gz: OK
SW version was verified successfuly
vmlinux.tar
vmlinux.UBoot: OK
Updating bank1 with vmlinux.UBoot file, please wait ...OK
```

System Database Import/ Export

To import/ export system configuration database, access the second safe mode.

1. Access second safe mode, use option 4 “recover” and list the current OS images available at the switch.

```
-------------------------------------------------------------------------------
|safe mode menu:
|      reset               | 1 :  Reset the device
|      defcfg              | 2 :  Load the factory-default configuration for the device
|      eeprom              | 3 :  Write to EEPROM
|      recover             | 4 :  Recover the device’s images from a package file
|      db                  | 5 :  Export / Import DB
|      continue            | c :  Continue in start up process
|      refresh             | r :  Refresh menu
|      help                | H :  Display help about this utility
-------------------------------------------------------------------------------
4


-------------------------------------------------------------------------------
|safe mode menu:
|      reset               | 1 :  Reset the device
|      defcfg              | 2 :  Load the factory-default configuration for the device
|      eeprom              | 3 :  Write to EEPROM
|      recover             | 4 :  Recover the device’s images from a package file
|      db                  | 5 :  Export / Import DB
|      continue            | c :  Continue in start up process
|      refresh             | r :  Refresh menu
|      help                | H :  Display help about this utility
-------------------------------------------------------------------------------
```

2. At the sub menu, select option 5 “db”. Use option 3 to view available db files at the usb (for import). Below example demonstrate importing a db file named “ss_spoke1” from the usb and booting the system with it.

```
3
List of db files on usb:
-rwxr-xr-x    1 root     root       2503168 Jan  1  1980 ss _ spoke1

-------------------------------------------------------------------------------
|safe mode menu:
|     reset              | 1 :  Reset the device
|     defcfg             | 2 :  Load the factory-default configuration for the device
|     eeprom             | 3 :  Write to EEPROM
|     recover            | 4 :  Recover the device’s images from a package file
|     db                 | 5 :  Export / Import DB
|     continue           | c :  Continue in start up process
|     help               | H :  Display help about this utility
5

#########################################################
###   Export / Import DB  ###############################
#########################################################
export          | 1 :  Export DB to usb
import          | 2 :  Import DB from usb
list            | 3 :  Show list of db files on usb
main            | X :  Return to the main menu
help            | H :  Display help about this menu

2
Import Db from usb
Enter file name
ss _ spoke1

-------------------------------------------------------------------------------
|safe mode menu:
|     reset              | 1 :  Reset the device
|     defcfg             | 2 :  Load the factory-default configuration for the device
|     eeprom             | 3 :  Write to EEPROM
|     recover            | 4 :  Recover the device’s images from a package file
|     db                 | 5 :  Export / Import DB
|     continue           | c :  Continue in start up process
```

```
|      help                | H :  Display help about this utility
-------------------------------------------------------------------------------------------
C
…….
```

Port Interfaces

Port addressing

The ports are configured as <interface-type> <port id>

Command	Description
interface-type <>	Specify the interface type Fastethernet gigabitethernet
Port id <>	Specify the port id in a slot number/port format Slot number is: 0 for Ethernet ports, 1 for Serial ports Port number is in the range of 0-16 (depending on hardware configuration)

A Logical View Of Ports

Below screenshots show available typical ports of a RLGE2FE16R with 8 Ethernet ports.

```
RLGE2FE16R# show vlan

Switch default

Vlan database
---------------
Vlan ID     : 1
Member Ports      : Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5, Fa0/6
                    Fa0/7, Fa0/8, Gi0/1, Gi0/2, Gi0/3, Gi0/4
Untagged Ports    : Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5, Fa0/6
                    Fa0/7, Fa0/8, Gi0/1, Gi0/2
Forbidden Ports   : None
Name              :
Status            : Permanent
-------------------------------------------------
Vlan ID           : 4092
Member Ports      : Gi0/3, Fa0/10, Fa0/11
Untagged Ports    : Fa0/10, Fa0/11
Forbidden Ports   : None
Name              :
Status            : Permanent
-------------------------------------------------
```

NOTE – The RS232 ports are configured and identified within the ACE CLI mode and are not seen at "show vlan". See chapter Serial Interfaces for more information.

NOTE – The RLGE2FE16R has several hardware ordering options of interfaces. The Ethernet interfaces which are applicable to the hardware will be available for configuration.

Enabling Ports

In order to be accessible, the required interfaces must be activated. This is done using the no shutdown command.

1. Example of enabling port interface number 5

```
RLGE2FE16R(config)# interface fastethernet 0/5
RLGE2FE16R(config-if)# no shutdown
RLGE2FE16R(config-if)# end
RLGE2FE16R# write startup-cfg
```

NOTE – System Default has all ports as enabled

The show interfaces command displays the complete information of all available interfaces.

ACE Ports

Ports Gigabitethernet 0/3 and Gi 0/4 are unique ports. These are internal system ports used for directing access and network traffic handled at the GCE to the Application services.

The use of these ports should be made in accordance to configuration instructions given in relevant chapters of this manual.

Default state

Vlan id / port	Gi 0/3	Gi 0/4
Vlan 4092	Tagged	
Vlan 4093	Tagged	
Vlan 1	Tagged (pvid)	Tagged

NOTE – The ACE ports properties should not be changed from their default settings of auto-negotiation and hybrid state.

Vlan assignment

The assignment of the ACE ports to a VLAN is always as a tagged member.

Following table summarizes the ports VLAN membership depending on the network planning.

Networking / port	Gi 0/3	Gi 0/4
Serial tunneling	Service VLANs	
Terminal Server	Service VLANs	
Gateway	Service VLANs	
L2 VPN	NNI Vlan	UNI Vlan
L3 VPN	NNI Vlan	
IPsec	NNI Vlan	
Cellular		
Firewall		Service VLANs

Ports FE 0/9-0/16

The usage of ports FE 0/9 - 0/16 is dependent on the hardware type.

With hardware versions of /216 and /288 these ports are standard user ports to be addressed and configured for all application purposes.

With hardware versions of /28 these ports are not physically available for the user but are still mapped in the CLI. At this case these ports are designated for internal system functions and should not be addressed by the user unless specifically mentioned in a configuration setup of feature in this manual.

NOTE – With hardware versions of /28 these ports properties should not be changed from their default settings of auto-negotiation and hybrid state.

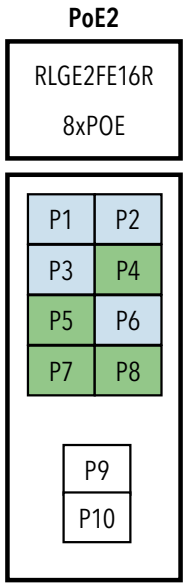
POE Ports

Depending on your hardware variant POE ports might be applicable.

PoE is supported at the RJ-45 ports only.

Hardware supporting POE is named:

RLGE2FE16R/X/XX/28P, RLGE2FE16R/X/XX/216P and RLGE2FE16R/X/XX/288P - hardware includes 8 POE support on the FE Ethernet ports 1-8. All POE ports are wired as Alternative-A (PoE runs on the FE twisted pairs). Each port supports up to 30w PoE. Notice the total PoE power allowed per the unit and per port group.



Power Management of POE

1. The 8 POE ports supports in total maximum power output of:
    a. For 12Vdc powered units (RLGE2FE16R/X/12) : 60 W
    b. For 24Vdc powered units (RLGE2FE16R/X/24) : 80 W
    c. For 48Vdc powered units (RLGE2FE16R/X/48) : 120 W
    d. For 110Vdc powered units (RLGE2FE16R/X/11) : 100 W
    e. For 220Vdc powered units (RLGE2FE16R/X/22) : 100 W
    f. For AC powered units (RLGE2FE16R/X/AC) : 120 W
2. The 8 POE ports divided to 2 groups , each group supports maximum power output of:
    1. For 12Vdc powered units (RLGE2FE16R/X/12) : 30 W
    2. For 24Vdc powered units (RLGE2FE16R/X/24) : 40 W
    3. For 48Vdc powered units (RLGE2FE16R/X/48) : 60 W
    4. For 110Vdc powered units (RLGE2FE16R/X/11) : 50 W
    5. For 220Vdc powered units (RLGE2FE16R/X/22) : 50 W
    6. For AC powered units (RLGE2FE16R/X/AC) : 60 W
    7. The group division is as follows:
        a. Group 1: p1,p2,p3,p6
        b. Group 2: p4,p5,p7,p8

Mode of PoE

All PoE models are provided with “Alternative A” wired ports and will supply POE power by IEEE 802.3at negotiation on demand. Non-POE equipment connected to such port is protected as it will not receive power over the Fast Ethernet communication lines.

POE command Hierarchy

+ Root

+ config terminal

    + interface <type> <port id>

        - poe-power { detect | manual }

        - poe { shutdown | no shutdown }

- show poe-status port <1-8>

POE Commands Description

Command	Description
Config terminal	
Interface <type> <port id>	Enter the specific Interface. only fastethernet ports are applicable. Permissible values : Fastethernet <1-8>
Poe	No shutdown: port is POE enabled. Shutdown: port is POE disabled. (default)
poe-power	Detect: POE will be available only upon negotiation with a POE connected load device. (default) Manual: POE will be available constantly. Caution: connect only POE capable load devices to ports which are in Manual mode.
show poe-status port <>	Show the POE state of the port. Port number is in the range 1-8, relating to fastethernet 1-8.

Controlling Ports

Storm Control

Sets the storm control rate for broadcast, multicast

Rate Limit Output

Enables the rate limiting and burst size rate limiting by configuring the egress packet rate of an interface and the no form of the command disables the rate limiting and burst size rate limiting on an egress port

Ports command Hierarchy

+ Root

+ config terminal

  + interface [range] <type> {<port id>| <iface_list>}

    - [no] alias DESCRIPTION

    - [no] speed (10 | 100 | 1000 | auto)

    - [no] duplex (auto | full | half)

    - [no] switchport pvid <vlan ID>

    - [no] switchport mode {access | trunk | hybrid}

    - [no] switchport acceptable-frame-type {all | tagged | untaggedAndPrioritytagged}

    - [no] system-specific port-id <id>

    - [no] snmp trap link-status

    - [no] negotiation

    - flowcontrol (receive | send) (desired | on | off)

    - mtu <mtu-value>

    - [no] shutdown

    - [no] storm-control { broadcast |multicast | dlf } level <pps (1-250,000>

    - [no] rate-limit output [rate-limit] [burst-limit]

- switchport unicast-mac learning limit <limit value(0-32767)>

- switchport unicast-mac learning { enable | disable }

clear interfaces [<interface-type> <interface-id>] counters

clear counters [<interface-type> <interface-id>]

- Show interfaces [<interface-type> <interface-id>] [vlan <vlan-id>]

- Show interfaces <type> <port id>

- show interface mtu

- show interfaces status

- show interfaces counters

- show interfaces capabilities

- show vlan port config [port <type> <port id>]

- show running-config interface <type> <port id>

Port Commands Description

Command	Description
Config terminal	
Interface <type> <port id>	
Alias	Set a description name for the port.
Speed	Set manual speed to the port. Requires first disabling 'negotiation' at the port.
Default: negotiation enabled.	
Duplex	Set port duplex as full | half | auto.
Default: full	
switchport mode	Configures the mode of operation for a switch port. This mode defines the way of handling of traffic for VLANs. **Access**: accepts and sends only untagged. This kind of port is added as a member to specific VLAN only and carries traffic only for the VLAN to which the port is assigned. This mode is allowed only if the port is not a tagged member at any vlan. The port property of "switchport acceptable-frame-type" must be set to untagged AND priority Tagged". **Trunk**: accepts and sends only tagged frames. This kind of port is added as member of all existing VLANs and for any new VLAN created, and carries traffic for all VLANs. The trunk port accepts untagged frames too, if the "switchport acceptable-frame-type" is set as "all". The port can be set as trunk port, only if the port is not a member of untagged ports for any VLAN in the switch. **Hybrid**: Configures the port as hybrid port that accepts and sends both tagged and untagged frames. Default: Hybrid

Command	Description
switchport pvid	The PVID represents the VLAN ID that is to be assigned to untagged frames. The packets are processed against PVID, if the packets accepted at ingress is not having a tag. Permissible range: 1-4000. default: 1.
switchport acceptable-frame-type	
negotiation	Enables port auto negotiation of speed. default: enabled
mtu frame size	This command configures the maximum transmission unit frame size for all the frames transmitted and received on all the interfaces in a switch. The size of the MTU frame size can be increased using this command. The value ranges between 90 and 9216. This value defines the largest PDU that can be passed by the interface without any need for fragmentation. This value is shown to the higher interface sub-layer and should not include size of the encapsulation or header added by the interface. This value represents the IP MTU over the interface, if IP is operating over the interface. Note: Any messages larger than the MTU are divided into smaller packets before transmission Default : 1500
system-specific port-id <>	This command configures the system specific index for the port. It provides a different numbering space other than the IfIndex to identify ports. The value ranges between 1 and 16384. Default : 0.
[no] snmp trap link-status	This command enables trap generation on the interface. The no form of this command disables trap generation on the interface. The interface generated linkUp or linkDown trap. The linkUp trap denotes that the communication link is available and ready for traffic flow. The linkDown trap denotes that the communication link failed and isnot ready for traffic flow. Default : enable
flowcontrol	
{ send | receive}	**Send** : Sets the interface to send flow control packets to a remote device **Receive** : Sets the interface to receive flow control packets from a remote device
{ on | off |desired}	**On** : If used with receive allows an interface to operate with the attached device to send flow control packets .If used with send the interface sends flowcontrol packets to a remote device if the device supports it **Off** : Turns-off the attached devices (when used with receive) or the local ports (when used with send) ability to send flow-control packets to an interface or to a remote device respectively **Desired** : Allows a local port to operate with an attached device that is required to send flow control packets or that may send the control packets, when used with receive option. Allows the local port to send administrative status to a remote device if the remote device supports it, when used with send option.
storm-control	sets the storm control rate for broadcast, multicast and DLF packets **broadcast** - Broadcast packets **multicast** - Multicast packets **dlf** - Unicast packets **level** - Storm-control suppression level as a total number of packets per second. Permissible values : 1-250,000
rate-limit output	rate-value - Line rate in kbps burst-value- Burst size value in kbps
clear interfaces [<interface-type> <interface-id>] counters	clears all the current interface counters from the interface

Port Configuration Example

1. Set a port speed to 100 Mbps

```
RLGE2FE16R# config terminal
RLGE2FE16R(config)# interface fastethernet 0/2
RLGE2FE16R(config-if)# no negotiation
RLGE2FE16R(config-if)# speed 100
```

2. Set a port as Trunk. Make sure to remove it from any vlan at which it is set as untagged member.

```
RLGE2FE16R(config)# Vlan 1
RLGE2FE16R(config-vlan)# no ports fastethernet 0/1 untagged fastethernet 0/1
RLGE2FE16R(config-vlan)# exit
RLGE2FE16R(config)# interface fastethernet 0/1
RLGE2FE16R(config-if)# switchport mode trunk
RLGE2FE16R(config-if)# switchport acceptable-frame-type all
```

3. Set a port PVID

```
RLGE2FE16R(config)# interface fastethernet 0/5
RLGE2FE16R(config-if)# switchport pvid 5
```

4. Set a Port Alias

```
RLGE2FE16R(config)# interface fastethernet 0/2
RLGE2FE16R(config-if)# alias Office-network
```

Configuration Output Example

```
RLGE2FE16R# show interfaces fastethernet 0/2

Fa0/2 up, line protocol is up (connected)
Bridge Port Type: Customer Bridge Port

Interface SubType: fastEthernet
Interface Alias: Office-network

Hardware Address is 00:20:d2:fc:c1:f1
MTU  1500 bytes, Full duplex, 100 Mbps,  No-Negotiation
HOL Block Prevention disabled.
```

```
CPU Controlled Learning disabled.
Auto-MDIX on
Input flow-control is off,output flow-control is off

Link Up/Down Trap is enabled

RLGE2FE16R# show interfaces status

Port         Status            Duplex    Speed       Negotiation     Capability
----         ------            ------    -----       -----------     ----------
Fa0/1        not connected     Half      -           Auto             Auto-MDIX on
Fa0/2        connected         Full      100 Mbps    No-Negotiation  Auto-MDIX on
Fa0/3        not connected     Half      -           Auto             Auto-MDIX on
…
RLGE2FE16R# show vlan port config port fastethernet 0/1
Vlan Port configuration table
------------------------------
Port Fa0/1
 Bridge Port Type                     : Customer Bridge Port
 Port Vlan ID                         : 1
 Port Acceptable Frame Type           : Admit All
 Port Mac Learning Status             : Enabled
 Port Mac Learning Limit              : Default
 Port Ingress Filtering               : Disabled
 Port Mode                             : Trunk
…
RLGE2FE16R# show vlan port config port fastethernet 0/5
Vlan Port configuration table
------------------------------
Port Fa0/5
 Bridge Port Type                     : Customer Bridge Port
 Port Vlan ID                         : 5
 Port Acceptable Frame Type           : Admit All
 Port Mac Learning Status             : Enabled
…
```

Login and Management

Configuring the Login Authentication Method sets the authentication method for user logins.

Setting up specific authorized personal for the switch management is possible using filtering conditions as: IP address (mandatory), vlan-id and service type (SSH, Telnet, SNMP...)

Once an authorized personal is configured in the system, no other entity can have management to the switch over IP. Serial console management remains available and not influenced by the authorized manager conditions.

If no authorized managers are configured (default state), then switch management is possible on all configured VLANs and associated ports via the respective IP interfaces assigned.

Login Authentication Hierarchy

+ root

- lock

- logout

    + config terminal

        -[no] authorized-manager ip-source <IP> {<subnet> | <prefix-length>, interface <type> ,vlan <id> ,service <type> }

        - login authentication [{ radius [local]| tacacs [local]}] [local]

        - login authentication default

        - login block-for <seconds(30-600)> attempts <tries(1-10)>

        - username <user-name> password [8-20 char] privilege <1-15>

        - username <user-name> status [enable | disable]

        - no username <user-name>

- show authorized-manager [ip-source < ip-address >]

- show system information

- show logging

- show users

- show line

- listuser

- show privilege

Login Authentication Commands Description

Command	Description
Config terminal	
authorized-manager ip-source	Configures an IP authorized manager and the no form of the command removes manager from authorized managers list.
<ip-address>	Sets the network or host address from which the switch is managed. An address 0.0.0.0 indicates 'Any Manager'."
<subnet-mask>	Sets the subnet mask for the configured IP address. The configured subnet mask should be in the same subnet of the network in which the switch is placed.
<prefixlength(1-32)>	Configures the number of high-order bits in the IP address. These bits are common among all hosts within a network. The value ranges between 1 and 32.
interface	
vlan <>	Sets the list of VLANs or a single specific VLAN in which the IP authorized manager can reside.
Service	Configures the type of service to be used by the IP authorized manager. The values can be: SSH | SNMP | HTTP | HTTPS
login authentication [{radius | tacacs }] [local]	**radius**: Sets the RADIUS server to be used as an authentication server. Enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. **tacacs**: Sets the TACACS server to be used as an authentication server. Communicates with the authentication server commonly used in networks. **local**: Sets locals authentication. The user identification, authentication, and authorization method is chosen by the local system administration and does not necessarily comply with any other profiles. Default : local
[no] login authentication default	**default**: Sets the default authentication method for User Logins.
[no] username	Set a new user. **Username**: should be 1-20 characters' length. - Allowed lowercase and uppercase letters, numbers: 0-9, hyphen (-) and underscore (_) **Password**: should be 4-20 characters' length. - Must include small letters. - Must include capitol letter. - Must include number - Must include special symbol. - allowed symbols: @#$%^&*()-+./<\` Privilege: 1-15.
show alias	Displays the aliases

Examples

1. Changing the password of the su user

```
RLGE2FE16R(config)# username su password Eb12#$asd privilege 15
```

2. configure user

```
RLGE2FE16R(config)# username company-ceo password User#123 privilege 15
```

3. example for assignment of authorized manager

```
RLGE2FE16R(config)# authorized-manager ip-source 10.10.20.20 / 32 interface fastethernet 0/1
vlan 1 service ssh snmp telnet
RLGE2FE16R(config)# authorized-manager ip-source 10.10.10.10
RLGE2FE16R# show authorized-managers
Ip Authorized Manager Table
---------------------------
Ip Address        : 10.10.10.10
Ip Mask           : 255.255.255.255
Services allowed : SSH
Ports allowed     : Fa0/1, Fa0/2, Fa0/3, Fa0/4
                    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                    Gi0/1, Gi0/2, Gi0/3, Gi0/4
                    Fa0/9, Fa0/10, Fa0/11, Fa0/12
                    Fa0/13
On cpu0          : Deny
Vlans allowed     : All Available Vlans
Ip Address        : 10.10.20.20
Ip Mask           : 255.255.255.255
Services allowed : SNMP, TELNET, SSH
Ports allowed     : Fa0/1
On cpu0          : Deny
Vlans allowed     : 1
```

4. example for blocking management to VLAN 1

```
config terminal
authorized-manager ip-source 0.0.0.1 / 32 vlan 1
```

Privilege level

Privilege Levels can be determined in order to best allocate system accessibility to different users.

Total of 16 levels, numbered 0-15 can be configured.

By default, the root user holds privilege level 15, allowing complete system availability.

Privilege Level 0 is the lowest level, restricting the user to minimum system access.

Users with Privilege Level 0 can access only the following commands:

- **Enable**
- **Disable**
- **Exit**
- **Help**
- **logout**

Users with Privilege Level 1 can access all user-level commands with RLGE2FE16R> prompt.

System allows to configure additional privilege levels (from level 2 to 14) to meet the needs of the users while protecting the system from unauthorized access.

Users with Privilege Level 15 can access all commands. It is the least restricted level.

Commands Description

Command	Description
VLAN Module status	Enable
Config	
Username <user-name>	Specifies the login user name to be created
Password <passwd>	Specifies the password to be entered by the user to login to the system. Password must contain 8-20 characters and should include at least one of each character type: special character (Supports !@#$%^&*(){}[]/\`~+=) numerical character uppercase alphabetic character lowercase alphabetic character
privilege <1-15>	Applies restriction to the user for accessing the CLI commands. This values ranges between 1 and 15. For example, a user ID configured with privilege level as four can access only the commands having privilege ID lesser than or equal to four

Serial Console Port

Management over the serial console port is enabled by default but can be blocked with the following command.

For the change in state to take effect the system must be rebooted.

Keep in mind to maintain management over IP interface prior to disabling the console port.

Connecting to the Console Port

The console port is an EIA232 VT-100 compatible port to enable the definition of the device's basic operational parameters.

Connecting the device to a PC using the Console Port:

Connect the RJ-45 connector of the console cable to the device's Console Port (CON).

Connect the other side of the cable to the PC.

Configure the PC port to 9600-N-8-1 (9600 bps, no parity,8 data bits, 1 stop bit, no flow control)

Below table details the console cable pin-out.

	RJ45 Male	DB9 Female
	1	-
Rx	2	3
Tx	3	2
GND	4	5
GND	5	5
	6	-
	7	-
	8	-

CLI Console Commands

This command enables the console CLI through a serial port. The no form of the command disables the console CLI.

+ root

    - lock

    - logout

    - [no] Cli console

        + config

            + line {vty |console}

                - exec-timeout <timeout sec>

- Show nvram

NOTE: The "cli console" takes effect only after system restart.

Management

The switch can be managed via the following methods:

» IP and VLAN based
» Serial console port
» RLConfig Software Utility

For Restrictions of users, privileges and authentications please see related chapters in this manual.

Default state

Feature	Default state
Vlan 1	Active. All ports are members
Layer 3 interface	Interface vlan 1 is set to : 10.0.0.1/8
SSH	Enabled
Telnet	Disabled
Http	Disabled (HTTP interface is not currently supported and should not be enabled. This feature is reserved for a future firmware release)
Console	Enabled
User	User name: su Password: 1234 Privilege : admin (15)

Commands Hierarchy

+ root

- set host-name <[default | <name>]
- set switch-host-name { default | <string(15)> }
- set welcome-banner [default | <"banner name">]
- set ssh-client { enable | disable }
- set telnet-client { enable | disable }
- ssh {<user>@<remote IP>}
- show iss memory all
- show iss-memory-leak modules
- telnet [user]@{remote IP}
- lock
- logout
- show running-config system

+ config terminal

+ line {vty |console}

- exec-timeout <timeout sec>

-[no] cli console

- set cli pagination {on| off}
- set cli terminal-line-count <integer (10-40)>
- set cli terminal-line-lenght <integer (40-132)>

-[no] feature telnet

- set ip http [enable | disable]
- ip http port <port-number(1-65535)>

+ interface <type> <port id>

- [no] switchport pvid <vlan ID>
- [no] shutdown

+ [no] interface vlan <vlan id>

- [no] shutdown

+ ip address [dhcp | <ip-address> <subnet-mask>]

- [no] ip http port <port>

- set ip http

+ Application connect

+ reload

- schedule date-and-time YYYY-MM-DD,HH:MM:SS

- schedule every <180 – 604800 seconds >

- schedule time HH:MM:SS

- schedule in <0 – 604800 seconds >

- cancel

- show

- show ip interface

- show http server status

- show running-config interface vlan <vlan id>

- Show interfaces

- Show interfaces <type> <port id>

- show telnet server

- show vlan port config [port <type> <port id>]

- show running-config interface <type> <port id>

- show telnet-client

- show ssh-client

Commands Description

Command	Description
set host-name	Set the switch name as shown in the root prompt. Default name is "RLGE2FE16R". Spaces are not supported.
set switch-host-name	Set the system host name and the SNMP name. configurable 15-character string. Special characters are supported except the symbol !.
set welcome-banner	Set the welcome banner as shown at log in screen. default is "Welcome ComNet customer". If spaces are required, place the complete title in double brackets.
ssh	The switch supports ssh client allowing It to open ssh session to a remote partner. User: user name to be logged in at the remote partner. Remote-ip : IP address of remote partner.
Config terminal	
line vty	Set idle time out for telnet / ssh to the switch. exec-timeout : given in seconds . default : 300 seconds
[no] cli	This command enables the console CLI through a serial port. The no form of the command disables console CLI. This command takes effect only on system restart.
[no] ip http port <port>	This command sets the HTTP port. This port is used to configure the router using the Web interface. port number: 1-65535. Default : 80
set ip http {enable | disable}	Enable: Enables HTTP in the switch. Disable: Disables HTTP in the switch Default : enable
[no] feature telnet	This command enables the telnet service in the system.
Application Connect	
reload schedule date-and-time	Set specific date and time for switch reload. Time format : YYYY-MM-DD,HH:MM:SS configuration which was not committed will not be available after reload!
reload schedule every	Set time interval for cyclic automatic system reload. Permissible range in seconds is 180 – 604800. configuration which was not committed will not be available after reload!
reload schedule time	Set specific time for switch reload. Time format : HH:MM:SS configuration which was not committed will not be available after reload!
reload schedule in	Set specific timer for next switch reload. Permissible range in seconds is 180 – 604800. configuration which was not committed will not be available after reload!
reload cancel	Cancels all scheduled automatic reloads
reload show	Shows user set scheduled reloads

Example

Follow below configuration example for establishing management on a certain port/s using designated VLAN and IP.

1. Create your vlan and assign ports. Port 0/1 is configured as untagged,0/2 as tagged

```
Config terminal
vlan 10
 ports fastethernet 0/1-2 untagged fastethernet 0/1
exit
```

2. Enable the required ports

```
interface fastethernet 0/1
 no shutdown
switchport pvid 10
map switch default
exit
interface fastethernet 0/2
 no shutdown
switchport pvid 10
map switch default
exit
```

3. Create the IP interface to the vlan

```
interface vlan 10
shutdown
ip address 192.168.0.100 255.255.255.0
 no shutdown
end
```

4. Create static route

```
Config terminal
ip route 0.0.0.0 0.0.0.0 192.168.0.1 1
end
write startup-cfg
```

System Alias

This command replaces the given token by the given string and the no form of the command removes the alias created for the given string. This is to allow easier names to be used for perhaps long cli command.

+ Root

    + Config terminal

        - alias <replacement string> <token to be replaced>

        - show alias

Command	Description
Config terminal	
Alias	
<replacement string>	Represents the string for which a replacement is needed.
<token to be replaced>	Specifies an abbreviated/ short form of the replacement string
show alias	Displays the aliases

CLI Pagination

Some show commands for example might produce a long output. By default, the output will be interrupted after every screen length pending with the notice "–more–" to continue.

Options:

- » Pressing the ENTER key will progress the output by a single line.
- » Pressing the SPACE key will progress the output by a screen length.
- » Pressing the Q key will interrupt the output entirely.
- » Turning CLI pagination on/off iss available with following command:

```
RLGE2FE16R(config)# set cli pagination on
RLGE2FE16R(config)# set cli pagination off
```

An output example of a show command with pagination set to on:

```
RLGE2FE16R# show running-config
#Building configuration...
snmp trap syslog-server-status
!
no smtp authentication
!
!
queue 1 interface fastethernet 0/1 qtype 1 scheduler 1 weight 1 queue-type unicast
!
queue 3 interface fastethernet 0/1 qtype 1 scheduler 1 weight 1 priority 2 queue
-type unicast
!
--More–
```

MAC-Address Table (FDB)

Port Mac Learning and limit

The Administrator configures the Mac Learning Status of each port as enabled or disabled. By default, each port in the bridge is allocated a limit on the number of Mac address that is learnt on that port. The Mac Learning Limit on each port is also configurable. The Port Mac Learning Limit is applicable only for the dynamic learnt entries.

Commands Hierarchy

+ root

    + config terminal

        - set mac-learning { enable | disable }

        - unicast-mac learning limit <100-16000>

        - mac-address-table aging-time <sec (300,10-1000000)>

        - mac-address-table static unicast <MAC> vlan <vlan id> interface <type> <id>

        - no mac-address-table static unicast <MAC> vlan <vlan id>

        + interface <type> <port id>

            - switchport unicast-mac learning [enable | disable]

            - switchport unicast-mac learning limit <limit value(0-100)>

            - switchport unicast-mac learning { enable | disable }

            - switchport ingress-filter

            - multicast-mac limit <limit>

- clear fdb

- show mac-address-table

- show vlan port config

- show multicast-mac limit

NOTE: For MAC traffic to be learned with the proper VLAN tag ,ingress-filtering must be enabled on the interface. Otherwise will be learned at VLAN 1.
IP traffic will be learned with the VLAN tag by default.

Configuration Example, Static MAC entry

1. place a static entry

```
RLGE2FE16R(config)# mac-address-table static unicast 00-22-3B-0E-09-95 vlan 1 interface
fastethernet 0/4
RLGE2FE16R# show mac-address-table

Switch default

Vlan  Mac Address       Type        ConnectionId      Ports
----  -----------       ----        ------------      -----
1     00-22-3B-0E-09-95  Static                       Fa0/4
4092  00-22-3B-0E-09-78  Static                       Gi0/3
4092  00-22-3B-0E-09-79  Static                       Fa0/10
4092  00-22-3B-0E-09-7a  Static                       Fa0/11

Total Mac Addresses displayed: 4
```

2. remove a static entry

```
RLGE2FE16R(config)# no mac-address-table static unicast 00-22-3B-0E-09-95 vlan 1
```

Example, exceeding MAC limit at a port

1. set limit to MAC learning at an interface

```
config
interface fastethernet 0/1
switchport unicast-mac learning limit value 5
end
```

Station MAC which is exceeding the allowed limit will not be learned at the fdb table and syslog message will indicate this as a warning.

```
RLGE2FE16R# show logging

<129>May 11 11:38:12 RLGE2FE16R CFA Mac learning limit exceeded on Port Fa 0/1 SRC MAC
54:53:ED:2B:19:86
```

IP ARP Table

The ARP (Address Resolution Protocol) cache timeout can be set in the system. Static entries are as well allowed to be entered

Commands Hierarchy

+ root

    + config terminal

        - arp timeout <seconds (7200,30-86400)>

        - arp <ip address> <hardware address> Vlan <vlan-id(1-4094)>

        - no arp <ip address>

- show ip arp [{ Vlan <vlan-id(1-4094)> | <interface-type> <interface-id> |<ip-address> | <mac-address> |summary | information }]

Commands Description

Command	Description
Config terminal	
Arp timeout <>	sets the ARP (Address Resolution Protocol) cache timeout. The timeout defines the period an ARP entry remains in the cache. When a new timeout value is assigned, it only affects the new ARP entries. All the older entries retain their old timeout values. The timeout values can be assigned to dynamic ARP entries only. static ARP entries remain unaltered by timeout value. timeout <seconds (30-86400)> default : 7200
arp <ip address> <MAC> vlan <>	<ip address> : Defines the IP address or IP alias to map to the specified MAC address. <hardware address> : Defines the MAC address to map to the specified IP address or IP alias. Vlan <vlan-id(1-4094)>

Configuration Example

1. Set timeout

```
RLGE2FE16R# config terminal
RLGE2FE16R(config)# arp timeout 50
```

2. set static entry

```
RLGE2FE16R(config)# arp 172.18.212.100 00:11:22:33:44:55 Vlan 1

Output example
RLGE2FE16R# show ip arp

VRF Id  : 0
VRF Name: default
Address           Hardware Address    Type   Interface   Mapping
-------           ----------------    ----   ---------   -------
172.18.212.100    00:11:22:33:44:55   ARPA   vlan1       Static

RLGE2FE16R# show ip arp information

ARP Configurations:
-------------------
VRF Name:  default

 Maximum number of ARP request retries is 3
 ARP cache timeout is 50 seconds
```

VLAN

VLAN technology, defined under the IEEE 802.1q specifications, allows enterprises to extend the reach of their corporate networks across WAN. VLANs enable partitioning of a LAN based on functional requirements, while maintaining connectivity across all devices on the network. VLAN groups network devices and enable them to behave as if, they are in one single network. Data security is ensured by keeping the data exchanged between the devices of a particular VLAN within the same network. VLAN offers a number of advantages over traditional LAN. They are:

1. Performance

In networks with traffic consisting of a high percentage of broadcasts and multicasts, VLAN minimizes the possibility of sending the broadcast and multicast traffic to unnecessary destinations.

2. Formation of Virtual Workgroups

VLAN helps in forming virtual workgroups. During this period, communication between the members of the workgroup will be high. Broadcasts and multicasts can be restricted within the workgroup.

3. Simplified Administration

Most of the network costs are a result of adds, moves, and changes of users in the network. Every time a user is moved in a LAN, re-cabling, new station addressing, and reconfiguration of hubs and routers becomes necessary. Some of these tasks can be simplified with the use of VLANs.

4. Reduced Cost

VLANs can be used to create broadcast domains, which eliminate the need for expensive routers.

5. Security

Sensitive data may be periodically broadcasted on a network. Placing only users who are allowed to access such sensitive data on a VLAN can reduce the chances of an outsider gaining access to the data. VLAN can also be used to control broadcast domains, set up firewalls, restrict access, and inform the network manager of an intrusion.

VLANs of System Usage

The VLAN range of 4000-4093 is reserved for system internal usage and is not to be used or manipulated by the user unless explicitly indicated in this manual.

VLAN Range of NMS Usage

NMS software may use a configurable range of VLANs for the creation and management of services.

The user should take notice to avoid manipulating NMS created VLANs.

VLAN Configuration Guidelines

- VLAN is enabled in the switch by default.
- The default VLAN 1 cannot be deleted in the switch, but the ports can be removed from it.
- Mapping of forwarding database identifier (FID) to VLANs is successful only when VLAN learning mode is hybrid.
- To configure a static unicast/multicast MAC address in the forwarding database, VLAN and member ports must have been configured for the specified VLAN.
- It is not possible to configure a port as trunk, if the port is an untagged member of a VLAN.
- Up to 1k VLANs may be configured simultaneously.

VLAN logically segments the shared media LAN, forming virtual workgroups. It redefines and optimizes the basic Transparent Bridging functionalities such as learning, forwarding, filtering and flooding.

VLAN Default State

Command	Description
VLAN Module status	Enable
Default VLAN Id configured in the switch	1
Mac address table aging time	300 seconds
Acceptable frame types	All (Accepts untagged frames or priority-tagged frames or tagged frames received on the port)
Ingress filtering	Disabled

Vlan Ports

Member ports represent the set of ports permanently assigned to the VLAN egress list. Frames belonging to the specified VLAN are forwarded to the ports in the egress list.

The untagged setting allows the port to transmit the frames without a VLAN tag. This setting is used to configure a port connected to an end user device.

NOTE: If the port type is not explicitly specified as untagged, then all the ports are configured to be of tagged port type allowing transmission of frames with the specified VLAN tag.

NOTE: If PVID value has not been explicitly configured for a port, then PVID assumes a default value of 1

NOTE: Adding port to a VLAN using the command "ports <type>.." will remove all ports from the VLAN and associate only the detailed ports to the VLAN. Adding port to a VLAN using the command "ports add <type>.." will add this port to the VLAN without affecting other port members of the VLAN.

Enabling VLAN

A VLAN can be activated in two ways:

» By adding a member port to a VLAN (refer to section Configuring Static)

» By using the VLAN active command.

Vlan command Hirarchy

+ root

+ config terminal

+ [no] vlan <vlan id>

  - [no] ports <port type> <port IDs> [untagged <port type> <port IDs>]

  - ports add <port type> <port IDs> [untagged <port type> <port IDs>]

  - set unicast-mac learning { enable | disable | default}

  - vlan active

  - vlan unicast-mac learning limit <0-4294967295>

+ interface <type> <port id>

  - [no] switchport pvid <vlan ID>

  - port mac-VLAN

  - mac-address-table static [unicast | multicast] <MAC> Vlan <id> recv port <type> <port id> interface <type> <port id>

  - switchport unicast-mac learning { enable | disable }

  - switchport unicast-mac learning limit <0-4294967295>

+ interface vlan <vlan id>

  - [no] shutdown

  - ip address [dhcp | <ip-address> <subnet-mask>]

- Show vlan [brief | id <vlan-range> | summary]

- show vlan device info

- show vlan port config [port <type> <port id>]

- show running-config vlan [<vlan id>]

- show mac-address table static [unicast | multicast]

Configuration Example

1. Setting all ports of the RLGE2FE16R to VLAN 1 as untagged members

```
config terminal
vlan 1
ports fastethernet 0/1-8 untagged fastethernet 0/1-8
ports add gigabitethernet 0/1-2 untagged gigabitethernet 0/1-2
exit
interface fastethernet 0/1
no shutdown
switchport pvid 1
exit
interface fastethernet 0/2
no shutdown
switchport pvid 1
exit
interface fastethernet 0/3
no shutdown
switchport pvid 1
exit
interface fastethernet 0/4
no shutdown
switchport pvid 1
exit
interface fastethernet 0/5
no shutdown
switchport pvid 1
exit
interface fastethernet 0/6
no shutdown
switchport pvid 1
exit
interface fastethernet 0/7
no shutdown
switchport pvid 1
exit
interface fastethernet 0/8
no shutdown
switchport pvid 1
exit
```

```
interface gigabitethernet 0/1
no shutdown
switchport pvid 1
exit
interface gigabitethernet 0/2
no shutdown
switchport pvid 1
exit
end
write startup-cfg
```

2. VLAN configuration example

```
RLGE2FE16R# config terminal
RLGE2FE16R(config)# vlan 55
RLGE2FE16R(config-vlan)# ports fastethernet 0/1-4,0/7 untagged fastethernet 0/2,0/7
RLGE2FE16R(config-vlan)# end
```

3. VLAN configuration example

```
RLGE2FE16R# config terminal
RLGE2FE16R(config)# vlan 32
RLGE2FE16R(config-vlan)# vlan active
RLGE2FE16R(config-vlan)# ports fastethernet 0/1-8 untagged all
RLGE2FE16R(config-vlan)# end
```

4. Configuration example for static Unicast entry configuring a Static Unicast Entry requires the VLAN to be configured and the member ports for that specified VLAN must also be configured.

```
RLGE2FE16R(config)# mac-address-table static unicast 22:22:22:22:22:22 VLAN 2 recv-port
gigabitethernet 0/1 interface gigabitethernet 0/2
```

IP Interfaces

The RLGE2FE16R supports multiple layer 3 interfaces to be set for the purposes of:

» Routing.

» Management.

» Serial services.

An IP interface is always assigned to a VLAN. Depending on its purpose an interface will be set either at the Global Configuration Environment or at the Application Configuration Environment.

GCE IP Interfaces

The GCE interfaces are usually used for:

1. IP Management to the switch (SSH, Telnet ,HTTP, SNMP, FTP)

2. Routing of access traffic using static entries or OSPF

- Different Interfaces must be in different subnets.

- Each interface can be assigned, and must be assigned, to a single VLAN.

- A VLAN can only be assigned a single IP interface.

- Static routing of GCE IP interfaces is immediate and requires no special configuration.

- Dynamic routing of GCE IP interfaces is supported with OSPF.

NOTE: Total limit of 64 subnets are supported at the routing table. Customer static and dynamic entries in total should not exceed a total of 60 entries.

Commands Hierarchy

+ root

+ config terminal

+ interface vlan <vlan id>

- [no] shutdown

- ip address [dhcp | <ip-address> <subnet-mask>]

[no] ip route <destination ip address> <destination subnet mask>

<next hope ip> <distance>

- debug ip dhcp client all

- release dhcp vlan <>

- renew dhcp vlan <>

- show interfaces

- show ip interface [vlan <vlan id>] [loopback <loopback id>]

- show running-config interface vlan <vlan id>

- show ip route [{<ip-address> [<mask>] | connected |ospf | rip | static | summary}]

- show debugging

- show ip dhcp client stats

- show ip dhcp server binding

- show running-config ip

NOTE: Configuring the IP address for an Interface requires the interface to be shutdown prior to the configuration.

Commands Description

Command	Description
Config terminal	
Interface vlan <>	
ip address	This command sets the IP address for an interface. The no form of the command resets the IP address of the interface to its default value.
<ip address>	Sets the IP address for an interface. Default : 172.18.212.150
<subnet mask>	Sets the subnet mask for the configured IP address. The configured subnet mask should be in the same subnet of the network in which the switch is placed. Default : 255.255.255.0
[no] shutdown	Disable / enable the interface. Prior to any configuration changes to the interface it must first be disabled.
[no] ip route	This command adds a static route. The Route defines the IP address or interface through which the destination can be reached. The no form of this command deletes a static route.
<destination ip address>	A.B.C.D
<destination mask>	Format 255.255.255.255
<next hop ip address>	Defines the IP address or IP alias of the next hop that can be used to reach that network. A.B.C.D
<distance>	(1-254)

Default state

```
RLGE2FE16R# show ip interface
vlan1 is up, line protocol is up
Internet Address is 10.0.0.1/8
Broadcast Address  255.255.255.255
vlan4093 is up, line protocol is up
Internet Address is 7.7.7.4/29
Broadcast Address  7.7.7.7
```

NOTE: Interface VLAN 1 is available by default for In-band management.

NOTE: Interface VLAN 4093 is used for internal purposes and should not be deleted /changed.

Configuration Examples

1. Example for interface configuration

```
RLGE2FE16R#config terminal
interface vlan 10
ip address 192.168.0.100 255.255.255.0
no shutdown
end
write startup-cfg
```

2. Static route configuration

```
Config terminal
ip route 0.0.0.0 0.0.0.0 192.168.0.10 1
end
write startup-cfg
```

3. Dhcp configuration

```
config terminal
interface vlan 1
ip address dhcp
end
```

```
RLGE2FE16R# show ip interface
vlan1 is up, line protocol is up
Internet Address is 172.17.203.39/24
Broadcast Address  172.17.203.255
IP address allocation method is dynamic
IP address allocation protocol is dhcp
```

Static and Dynamic switch Default IP Address assignment

+ root

    + config terminal

    + default mode [dynamic | manual]

    + default ip address <ip-address> [subnet-mask<subnet mask>] [interface <interface-type><interface-id>]

    + default ip allocation protocol dhcp

show nvram

Command	Description
Config terminal	
default mode	
manual|dynamic	**manual** - Assigns static IP address to the default interface. The IP address and IP mask configured by user are assigned to the default interface. **dynamic** - Assigns dynamic IP address to the default interface. IP address provided by the server in the network is assigned to the default interface on switch reboot. The IP address is fetched through the dynamic IP address configuration protocols such as DHCP client. Default : manual
Default ip address	
<ip address>	Sets the IP address for the default interface / specified interface. If the network in which the switch is implemented contains a server such as DHCP server, dynamically allocating IP address, the configured IP address should not be within the range of the addresses that will be allocated by the server to the other switches. This precaution avoids creation of IP address conflicts between the switches. Default : 10.0.0.1
subnet-mask <subnet mask>	Sets the subnet mask for the configured IP address. The configured subnet mask should be in the same subnet of the network in which the switch is placed Default : 255.0.0.0
<interface-type>	fastethernet | gigabitethernet
<interface-id>	ID : <slot number>/<port number> Slot number is fixed as 0.
default ip allocation protocol	
dhcp	Allows the client device to obtain configuration parameters such as network address, from the DHCP server. Default : dhcp

ACE IP Interfaces

The following services require assignment of an IP interface and possibly routes at the Application Configuration Environment.

Multiple IP interfaces are optional.

The Application IP interfaces are supported on top of the layer 3 interfaces configured at the GCE and may be routed with them.

Application IP interfaces are required for the following:

- Serial tunneling
- Terminal server
- Protocol gateway
- L2-VPN
- L3-DMVPN
- IPSec
  - Each IP interface must be associated with a user predefined VLAN (set at the GCE).
  - Each interface must be associated with a “purpose”.
  - One (and only one) of the interfaces must be set to purpose application-host
  - All other interfaces must be set to purpose general
  - At each such purpose VLAN, the ACE port Gi 0/3 must be set as a tagged member.
  - Each interface must be in a unique subnet.
  - The IP interfaces are given an automatic name indicating the VLAN tag they are created with. The name format is: ETH1.<vlan id>

ACE IP Interface Commands Hierarchy

+ root

    + application connect

        + router

            - interface {create | remove} address-prefix <IP address>/<netmask> vlan [vlan id] purpose {application-host |general}

            - static {enable | dissable}

                + configure terminal

                    - ip route static <dest network> /<subnet> <Gateway>

            - interface show

            - route show

ACE IP Interface Commands Description

Command	Description
Application connect	Enter the industrial application menu
Router	Enter the application router configuration mode
interface create | remove	Add or Remove an IP interface for the application engine. The configuration should include: Address-prefix : IP address in the format aa.bb.cc.dd/xx vlan : VLAN ID that the application engine will use for this IP interface The interface will be name eth1.<vlan id>
Static	
	Managing static route entries Enable Disable
Configure terminal	
ip route static	dest network: target network address in the format aa.bb.cc.dd/xx Gateway : IP address in the format aa.bb.cc.dd
Show	Show ACE IP interfaces
Route show	Show ACE static route entries

Example for creating ACE IP Interface

1. Create a VLAN to be used for interface. port gigabitethernet 0/3 is mandatory to be assigned as tagged.

```
RLGE2FE16R#config terminal
vlan 100
ports add gigabitethernet 0/3
end
write startup-cfg
```

2. Create an IP interface and static route (default gateway).

```
RLGE2FE16R#application connect
[/] router interface create address-prefix 172.17.212.10/24 vlan 100 purpose application-
host
 [/]router interface show
+------+---------+-----------------+-----------------+-------------+
| VLAN |   Name  |   IP/Subnet     |     Purpose     | Description |
+======+=========+=================+=================+=============+
| 100  | eth1.100 | 172.17.212.10/24 | application host |             |
+------+---------+-----------------+-----------------+-------------+
 [router/] static
router/static> enable
router/static# configure terminal
router/static(config)# ip route 0.0.0.0/0 172.17.212.100
router/static(config)# write
router/static(config)# exit
router/static# exit
 [/]router route show
Kernel IP routing table
Destination     Gateway         Genmask          Flags Metric Ref    Use Iface
172.17.212.0    0.0.0.0         255.255.255.0    U     0      0        0 eth1.100
0.0.0.0         172.17.212.100  0.0.0.0          UG    0      0        0 eth1.100
Completed OK
```

Diagnostic

System Environment

Environment Command Hierarchy

+ Root

+ config terminal

  - set switch maximum { RAM | CPU | flash } threshold <percentage>

  - set switch temperature {min|max} threshold <celsius>}

  + interface <type> <port id>

  - [no] snmp trap link-status

  - show system information

  - show env {all | temperature| RAM | CPU | flash | power}

  - show nvram

Environment Commands Description

Command	Description
Config terminal	
Interface <type> <port id>	
[no] snmp trap link-status	This command enables trap generation on the interface. The no form of this command disables trap generation on the interface. The interface generated linkUp or linkDown trap. The linkUp trap denotes that the communication link is available and ready for traffic flow. The linkDown trap denotes that the communication link failed and is not ready for traffic flow.
set switch maximum	This command sets the switch maximum threshold values of RAM, CPU, and Flash. When the current resource usage rises above the threshold limit, the SNMP trap message with maximum severity will be sent for the specified resource and the SNTP message will be displayed. This threshold value is represented in percentage and ranges between 1 and 100 percentage
{RAM | CPU | flash}	**RAM** : Indicates the maximum RAM usage of the switch in percentage to trigger a trap. **CPU** : Indicates the maximum CPU usage of the switch in percentage to trigger a trap. **Flash** : Indicates the maximum flash usage of the switch in percentage to trigger a trap.
threshold <percentage>	Percentage : 1-100 Default : 100
set switch temperature	This command sets the maximum and minimum temperature threshold values of the switch in Celsius. When the current temperature drops below the threshold, an SNMP trap with maximum severity will be sent to the manager. This threshold value ranges between -14 and 40 degree Celsius.
{min|max}	Sets the minimum /maximum temperature threshold value for the switch to trigger a trap. Defaults : Minimum : 10 degree Celsius Maximum : 40 degree Celsius threshold <celsius>}

Example

Below is a show example of a typical output

```
RLGE2FE16R# show env all
RAM Threshold                        : 95%
Current RAM Usage                    : 54%
CPU Threshold                        : 95%
Current CPU Usage                    : 0%
Current power supply                 :
Max Temperature                      : 76C
Current Temperature                  : 41.500C
Current Flash Usage                  : 32%
```

RMON

RMON (Remote Monitoring) is a standard monitoring specification that enables various network monitors and console systems to exchange network-monitoring data.

The RMON specification defines a set of statistics and functions that can be exchanged between RMON-compliant console managers and network probes. As such, RMON provides network administrators with comprehensive network-fault diagnosis, planning, and performance-tuning information.

Commands Hierarchy

+ root

    + config

    - set rmon {enable | disable}

    + interface <type> <id>

    - rmon collection stats <index (1-65535)> [owner <ownername (127)>]

    - show rmon [statistics [<stats-index (1-65535)>]] [alarms] [events] [overview]]

    - show running-config rmon

Commands Description

Command	Description
Config	
Set rmon	**Enable**: Enables the RMON feature in the system. On enabling, the RMON starts monitoring the networks both local and remote and provides network fault diagnosis **Disable**: Disables the RMON feature in the system. On disabling, the RMON's network monitoring is called off. **Default** :disabled
Interface <type> <id>	
rmon collection stats	This command enables history collection of interface statistics in the buckets for the specified time interval. The no form of the command disables the history collection on the interface <index (1-65535)> : Identifies an entry in the alarm table. The value ranges between 1 and 65535. Owner: Allows the user to enter the name of the owner of the RMON group of statistics.

Example

Following configuration example will enable RMON on port fast Ethernet 0/2

```
config terminal
set rmon enable
interface fastethernet 0/2
rmon collection stats 1 owner ComNet
RLGE2FE16R# show rmon statistics 1

RMON is enabled
Collection 1 on Fa0/1 is active, and owned by ComNet,
 Monitors ifEntry.1.1 which has
 Received 5449624 octets, 73797 packets,
 73797 broadcast and 0 multicast packets,
 0 undersized and 0 oversized packets,
 0 fragments and 0 jabbers,
 0 CRC alignment errors and 0 collisions.
 0 out FCS errors,
 # of packets received of length (in octets):
 64: 73291, 65-127: 228, 128-255: 0,
 256-511: 0, 512-1023: 0, 1024-1518: 506
```

System logs export

The system logs can be exported to a flash USB drive add-hoc or by time provisioning.

NOTE: In this version, the hardware configuration allows operation of a single USB device (cellular modem OR external USB interface). Therefore, if using an RLGE2FE16R unit with cellular modem, please make sure to select the correct configuration of active USB device for your purposes. To do so please address section Cellular modem as a USB device of this manual.

Commands Hierarchy

+ Root

- logs-export [flash:<file_name> | sftp://user:password@aa.bb.cc.dd/<file_name> | tftp://aa.bb.cc.dd/<file_name>]

+ application connect

+ schedule

- add task-name copy-logs [day |hour |minute |month |year]

- remove task-name copy-logs

- show

Commands Description

Command	Description
Logs-export	Export the logs to a server or to a USB flash drive. The USB must be fat32 formatted and must be mounted. To mount a USB drive insert it to the switch USB port and reboot the switch.
Application connect	Entering the Application Configuration Environment
Schedule	manage scheduled task to copy system logs to the USB drive. To mount a USB drive insert it to the switch USB port and reboot the switch.
add task-name copy-logs	Add a scheduled task to copy system logs to the switch drive. Day: <1-31> Month: <1-12> year: <2013-3000> hour: <1-24> minute: <1-60>
remove task-name copy-logs	Remove a scheduled task to copy system logs to the USB drive.
Show	Display tasks

Capture Ethernet service traffic

The system supports sniffing and capturing of Ethernet traffic for selected service IP interfaces. This capability is important in order to diagnose network traffic of a service for debugging.

The capturing is available for traffic passing via the application ports gigabitethernet 0/3-4.

The capture command is implemented on the IP interfaces eth1.<vlan id>, eth2 and mGRE where :

» eth1.<vlan id> : ACE IP interface configured by the user. Port gigabitethernet 0/3 is a tagged member at vlan x.

» eth2: ACE IP interface set internally by the system. Port gigabitethernet 0/4 is a tagged member at the service vlan. relevant for firewall services only (MODBUS, IEC104, DNP3)

» mGRE – VPN tunnel name.

Captures can be displayed at the terminal (up to 200 packets)or saved to the local flash (cyclic, up to 10M total size of last packets). The capture log can be exported from the flash to a USB drive or a tftp/sftp server.

Commands Hierarchy

+ root

  + application connect

    + router

      - interface {create | remove} address-prefix <IP address>/<netmask> vlan [vlan id] purpose {application-host |general}

      - interface show

    + capture

      - start –i eth1.<vlan id> [-C] [-s] [-y] [expression <>]

      - start –i eth2 {-C} [-s] [-y] [expression <>]

      - stop

      - delete

      - export remote-address <destination address,A.B.C.D>

      - show {captured-packets | status}

      - help

Commands Description

Command	Description
Application connect	Entering the Application Configuration Environment
Capture	**Start**: initiate Ethernet traffic capture on a selected ACE IP interface. -i : mandatory prefix to be followed with the IP interface name -eth1.<vlan id> : an ACE IP interface created by the user for a chosen vlan id. -eth2 : a system internal IP interface. -mGRE name -c : optional. Stop the capture after a defined number of packets. <1-200> -n : Don't convert addresses (i.e., host addresses, port numbers, etc.) to names **Stop** : stop Ethernet traffic capture **Delete** : delete capture files **Export remote-address**: export file to a tftp server. **Show** captured-packets –C<1-200>: display the captured content up to a chosen length (1-200) lines. **Show status** : display capture configuration **Help** : display help on settings options.

Example

1. Set a vlan for the service traffic. Assign an access port and the ACE port gi 0/3.

```
Config terminal
Vlan 20
ports add fastethernet 0/5 gigabitethernet 0/3 untagged fastethernet 0/5
exit
interface fastethernet 0/5
switchport pvid 20
end
```

2. Set an ip interface in the ACE for the vlan

```
application connect
router interface create address-prefix 172.18.212.235/24 vlan 20

[/] router interface show
+------+---------+------------------+-----------------+-------------+
| VLAN |   Name  |      IP/Subnet   |      Purpose    | Description |
+======+=========+==================+=================+=============+
|  20  | eth1.20 | 172.18.212.235/24 | application host |             |
+------+---------+------------------+-----------------+-------------+
```

3. Start capture

```
Capture start –i eth1.20
Capture show
[capture/] show status
capture is running
```

4. Stop the capture and display the output

```
Capture stop
capture show captured-packets -c 10
16:55:07.370814 IP 172.18.212.240.netbios-ns > 172.18.212.232.netbios-ns: NBT UDP PACKET(137): QUERY; POSITIVE; RESPONSE; UNICAST
16:55:07.616319 IP 172.18.212.240.17500 > 255.255.255.255.17500: UDP, length 112
16:55:07.616628 IP 172.18.212.240.17500 > 172.18.212.255.17500: UDP, length 112
16:55:07.926503 arp who-has 172.18.212.232 tell 172.18.212.64
16:55:08.122046 IP 172.18.212.240.netbios-ns > 172.18.212.232.netbios-ns: NBT UDP PACKET(137): QUERY; POSITIVE; RESPONSE; UNICAST
16:55:08.258801 arp who-has 172.18.212.232 tell 172.18.212.40
16:55:08.602306 IP 172.18.212.40.17500 > 255.255.255.255.17500: UDP, length 112
16:55:08.604927 IP 172.18.212.40.17500 > 255.255.255.255.17500: UDP, length 112
16:55:08.605016 IP 172.18.212.40.17500 > 172.18.212.255.17500: UDP, length 112
16:55:08.680664 CDPv2, ttl: 180s, Device-ID 'Switch'[|cdp]
```

DDM

The system supports DDM (digital diagnostics monitoring) information for Fiber SFP modules supporting this information.

The SFP ports are gigabitethernet 0/1 and 0/2. Depending if the SFP itself supports DDM, diagnostics is available at the CLI interface.

Commands Hierarchy

+ root

- show sfp-port detailed
- show sfp-port extended
- show sfp-port ddm [gigabitethernet <id>]

Example

Below is a show output of a DDM supporting SFP

```
RLGE2FE16R# show sfp-port ddm

         _ _ _ _ _ _ Diagnostic Data For gigabitethernet 0/1 _ _ _ _ _ _
Diagnostics Rev 9.5 supported on SFP

      _ _ _ _ _ _ ALARM Bits _ _ _ _ _ _ WARNING Bits _ _ _ _ _ _

Tx Power Low      : OK              : OK
Tx Power High     : OK              : OK
Tx Bias Low       : OK              : OK
Tx Bias High      : OK              : OK
Vcc Low           : OK              : OK
Vcc High          : OK              : OK
Temperature Low   : OK              : OK
Temperature High  : OK              : OK
Rx Power Low      : OK              : OK
Rx Power High     : OK              : OK

         _ _ _ _ _ _ Diagnostic Data For gigabitethernet 0/2 _ _ _ _ _ _
Diagnostics Rev 9.3 supported on SFP

      _ _ _ _ _ _ ALARM Bits _ _ _ _ _ _ WARNING Bits _ _ _ _ _ _

Tx Power Low      : OK              : OK
Tx Power High     : OK              : OK
Tx Bias Low       : OK              : OK
Tx Bias High      : OK              : OK
Vcc Low           : OK              : OK
Vcc High          : OK              : OK
Temperature Low   : OK              : OK
Temperature High  : OK              : OK
Rx Power Low      : FAIL            : FAIL
Rx Power High     : OK              : OK

RLGE2FE16R# show sfp-port detailed
Transceiver type :       SFP
Cable Connector       :  LC
Vendor Name           :  DELTA
Encoding              :  NRZ
```

```
Manufacture Date      :  2010/12/23 - 0
Media                  :  N/A
Serial Number         :  105100100009
Tx Laser Wavelength   :  N/A
Part Number           :  LCP-155A4HDRZR
Revision Level        :  C
Link Length Support   :  2000m for 62.5/125 mm fiber link
Transceiver type :       SFP
Cable Connector       :  LC
Vendor Name           :  MICROSENS
Encoding              :  NRZ
Manufacture Date      :  2013/03/29 - 0
Media                  :  N/A
Serial Number         :  0028 0004
Tx Laser Wavelength   :  N/A
Part Number           :  MS100190DX
Revision Level        :  0000
Link Length Support   :  2000m for 50/125 mm fiber link

RLGE2FE16R# show sfp-port extended

          _ _ _ _ _ _ Extended Data For gigabitethernet 0/1 _ _ _ _ _ _
Temperature       : 45. 0 C
Supply Voltage    : 3.2736 V
Tx Current Bias   : 17.0776 mA
Tx Output Power   : -16.216021Dbm 0.023900mW
Rx Input Power    : -20.000000Dbm 0.010000mW
          _ _ _ _ _ _ Status/Control Bits _ _ _ _ _ _
Data Ready Bar    : OK
Rx _ LOS            : OK
Tx Fault          : OK
Soft Rate Select : OK
Rate Select       : OK
RS(1)             : OK
Soft Tx Disable   : OK
Tx Disable        : OK
          _ _ _ _ _ _ Extended Data For gigabitethernet 0/2 _ _ _ _ _ _
Temperature       : 41.50 C
Supply Voltage    : 3.2792 V
Tx Current Bias   : 2.0544 mA
Tx Output Power   : -10.757207Dbm 0.084000mW
```

```
Rx Input Power    : -40.000000Dbm 0.000000mW
_ _ _ _ _ _ Status/Control Bits _ _ _ _ _ _
Data Ready Bar    : OK
Rx _ LOS            : FAIL
Tx Fault          : OK
Soft Rate Select : OK
Rate Select       : OK
RS(1)             : OK
Soft Tx Disable   : OK
Tx Disable        : OK
```

Debugging

Debug Logging allows related logs to be displayed at the terminal.

The debug logging is implemented per feature and is by default disabled on all.

Commands Hierarchy

+ root

- [no]debug aps ring {[all] [critical] [start-shut] [mgmt] [ctrl] [pkt-dump] [resource] [all-fail] [buff])>]}

- [no]debug dot1x {all | errors | events | packets | state-machine | redundancy | registry}

- [no]debug ethernet-cfm {global | {[all] | {[critical] [init] [resource] [failure][pkt][buffer] [ctrl] [func-entry] [func-exit]}}

- [no] debug interface [track] [enetpktdump] [ippktdump] [arppktdump] [trcerror] [os] [failall] [buffer] [all]

- [no]debug ip dhcp client { all | event | packets | errors | bind }

- [no]debug ip dhcp relay {all | errors}

- [no]debug ip igmp snooping {[init][resources][tmr][src][grp][qry] [vlan][pkt][fwd][mgmt] [redundancy] | all }

- [no]debug ip ospf

- [no]debug ip vrrp { all | init | pkt | timers | events | failures }

- [no]debug lacp

- [no]debug lldp

- [no]debug radius

- [no]debug sntp

- [no]debug spanning-tree { global | all | [errors] [init-shut] [management] [bpdu] [events]}

- [no]debug ssh ([all] [shut] [mgmt] [data] [ctrl] [dump] [resource] [buffer] [server]]

- [no]debug tacacs { all | info | errors | dumptx | dumprx }

- [no]debug vlan global

- show debugging

+ config terminal

    - debug-logging console

    - no debug-logging

Commands Description

Command	Description
debug-logging { console |file |flash }	**Console** : Displays the debug logs in the console. **File |flash** : Stores the debug logs in the file. This feature is planned for R4.0
No logging	Send the debug logs to the console.
debug interface	This command sets the debug traces for all the interfaces. The no form of the command resets the configured debug traces. **Track** : Generates debug messages for all track messages. **Enetpktdump** : Generates debug messages for ethernet packet dump messages. **Ippktdump** : Generates debug messages for IP protocol related packet dump messages **Arppktdump** : Generates debug messages for address resolution protocol related packet dump messages. **Trcerror** : Generates debug messages for trace error messages. **Os** : Generates debug messages for for OS resources. For example, when there is a failure in mem pool creation / deletion, this trace level is used. **Failall** : Generates debug messages for all failures including packet validation. **Buffer** : Generates debug messages for buffer trace levels where packet buffer is used.i.e in cases wher packet is enqueued **All** : Generates debug messages for all kinds of traces

Syslog

Syslog is a protocol used for capturing log information for devices on a network. The syslog protocol provides a transport to allow a machine to send event notification messages across IP networks to event message collectors, also known as syslog servers. The protocol is designed to transport the event messages.

One of the fundamental elements of the syslog protocol and process is its simplicity. The transmission of syslog messages may be started on a device without a receiver being configured, or even actually physically present. This simplicity has greatly aided the acceptance and deployment of syslog.

User enables syslog server and configures the syslog related parameters. The logging process controls the distribution of logging messages to the various destinations, such as the logging buffer, logging file, or syslog server.

Severity of logging can be set with its numeric value <0-7> or its name tag. When configuring a server, it should be set with priority tag, reflecting the level of the message and the facility.

Syslog messages are available for both GCE and ACE processes.

The Priority indicator

The Priority indicator is calculated as: Priority = 8x facility_coefficient + severity_level.

facility coefficient	facility	Priority
0	kernel messages	0x8 + level
1	user-level messages	1x8 + level
2	mail system	2x8 + level
3	system daemons	3x8 + level
4	security/authorization messages	4x8 + level
5	messages generated internally by syslog	5x8 + level
6	line printer subsystem	6x8 + level
7	network news subsystem	7x8 + level
8	UUCP subsystem	8x8 + level
9	clock daemon	9x8 + level
10	security/authorization messages	10x8 + level
11	FTP daemon	11x8 + level
12	NTP subsystem	12x8 + level
13	log audit	13x8 + level
14	log alert	14x8 + level
15	clock daemon (note 2	15x8 + level
16	Local0	16x8 + level
17	Local1	17x8 + level
18	Local2	18x8 + level
19	Local3	19x8 + level
20	Local4	20x8 + level
21	Local5	21x8 + level
22	Local6	22x8 + level
23	Local7	23x8 + level

Example, Syslog message priority tag with facility local0

Level purpose	Numeric level	Priority (w. local0)
emergencies	0	16x8+0=128
alerts	1	129
critical	2	130
errors	3	131
warnings	4	132
notification	5	133
informational	6	134
debugging	7	135

GCE Message Format

The following will describe the ComNet structure of syslog messages generated by GCE processes.

Console message format

The message format when sent to the CLI console is,

```
{<PRI> [Time Stamp] [Host Name] [App]}  {[MSG]}
```

Examples of messages received at the CLI

```
<134>May  8 15:46:00 RLGE2FE16R CFA Slot0/1 Link Status [UP]
<134>May  8 15:50:52 RLGE2FE16R CFA Slot0/1 Link Status [DOWN]
```

Server message format

The message format when sent to a SYSLOG server is,

```
{<PRI> [Host IP] [Time Stamp] [Host name] [App]} {[MSG]}
```

Examples of messages received at a server

```
Local0.Info  172.19.212.237      May 11 13:34:48 RLGE2FE16R CFA Slot0/2 Link Status [UP]
Local0.Info  172.19.212.237      May 11 13:34:42 RLGE2FE16R CFA Slot0/2 Link Status [DOWN]
```

ACE Message Format

The following will describe the ComNet structure of syslog messages generated by ACE processes.

ACE Message severity

Severity	S indicator	Description
0	S=E	Emergency: system is unusable
1	S=A	Alert: action must be taken immediately
2	S=C	Critical: critical conditions
3	S=E	Error: error conditions
4	S=W	Warning: warning conditions
5	S=N	Notice: normal but significant condition
6	S=I	Informational: informational messages
7	S=D	Debug: debug-level messages

Firewall TCP SCADA Protocols

The following describes the ComNet structure of syslog messages generated for firewall of IEC 104, DNP3 TCP, MODBUS TCP.

Console message format

The message format when sent to the CLI console is:

{[APP-NAME] [PROCID][Severity] [MSGID] [Time Stamp]} {[MSG]} {STRUCTURED-DATA}

The message structured data includes following information fields,

```
|S=SEVERITY|SG=VLAN _ ID|SRC=SRC _ IP _ ADDR:SRC _ IP _ PORT|DST=DEST _ IP _ ADDR:DEST _ IP _
PORT|LEN=DATA _ MSG _ LEN|TTL=TTL|PROTO=PRTOCOL _ NAME|MSG=VIOLATION _ DESCR|
```

Examples of messages received at the CLI. Use the command “firewall log show” at the ACE to retrieve following log entries.

1. Example for violation type “no rule configured”

```
-     RF _ Syslog : module 3 (firewall) severity 3 message : firewall
-     |ID=74|T=2014-05-12,11:52:43
|S=E|SG=3500|SRC=172.18.212.50:52011|DST=172.18.212.46:2404|LEN=56|TTL=128|PROTO=iec104|MSG=[0x100]
[45,0]:FW RULE - no rule configured| (164 bytes)
```

2. Example for violation type “protocol type mismatch”

```
-     RF _ Syslog : module 3 (firewall) severity 1 message : firewall
|ID=80|T=2014-05-12,11:52:59
|S=A|SG=3500|SRC=172.18.212.50:52011|DST=172.18.212.46:2404|LEN=56|TTL=128|PROTO=iec104|MSG=[0x101]
[45,0]:FW PROTOCOL protcol type missmatch| (170 bytes)
```

Server message format

The message format when sent to a SYSLOG server is,

```
{<PRI> [Host IP] [Time Stamp] [APP-NAME]} {MSG} {STRUCTURED-DATA}
```

The message structured data includes following information fields,

```
|S=SEVERITY|SG=VLAN _ ID|SRC=SRC _ IP _ ADDR:SRC _ IP _ PORT|DST=DEST _ IP _ ADDR:DEST _ IP _
PORT|LEN=DATA _ MSG _ LEN|TTL=TTL|PROTO=PRTOCOL _ NAME|MSG=VIOLATION _ DESCR|
```

Examples of messages received at server

1. Example for violation type “no rule configured”

```
- Local0.Error  172.18.212.183  May 12 11:52:54 SW RLGE2FE16R firewall
- |ID=79|T=2014-05-12,11:52:54
|S=E|SG=3500|SRC=172.18.212.50:52011|DST=172.18.212.46:2404|LEN=62|TTL=128|PROTO=iec104|MSG=[0x100]
[45,0]:FW RULE - no rule configured|
```

2. Example for violation type “protocol type mismatch”

```
- 05-12-2014  16:53:40  Local0.Alert  172.18.212.183  May 12 11:52:59 SW RLGE2FE16R firewall
- |ID=80|T=2014-05-12,11:52:59
|S=A|SG=3500|SRC=172.18.212.50:52011|DST=172.18.212.46:2404|LEN=56|TTL=128|PROTO=iec104|MSG=[0x101]
[45,0]:FW PROTOCOL protcol type missmatch| (170 bytes)
```

Firewall Serial SCADA Protocols

The following describes the ComNet structure of syslog mssages generated for firewall of IEC 101, DNP3 RTU, MODBUS RTU.

IP=IP_ADDR|SLOT=SLOT_NUMBER|PORT=PORT_NUMBER|DIR=DATA_MSG_DIR|LEN=DATA_MSG_LEN|PROTO=PROTOCOL_NAME|MSG=VIOLATION_DESCR|

Syslog message fields description

Command	Description
VLAN_ID	The VLAN number
SRC_IP_ADDR	The pointed string source IP address.
SRC_IP_PORT	The source IP port number
DEST_IP_ADDR	The pointed string destination IP address.
DEST_IP_PORT	The destination IP port number
DATA_MSG_LEN	The total data message length
TTL|	The ttl value of the IP header
PRTOCOL_NAME	The protocol name field. The following values are available: “any” “icmp” “tcp” “udp” “ipencap” “gre” “modbus_tcp” “modbus_rtu” “iec104” “iec101” “dnp3”

Command	Description
VIOLATION_DESCR	The FW violation description string. The following format is used: [Major Protocol Id,Minor Protocol Id]:Violation description string: Major Protocol Id: Major protocol id value, for ModBus – Function Code for IEC101/104 - Type Id for DNP3 - Function Code Minor Protocol Id: Minor protocol id value, for ModBus – Sub-Function Code for IEC101/104 - non used for DNP3 - non used Violation description string: The following values are available for general violations: "Flow is not allowed" "FW PROTOCOL no violation" "FW internal error (no drop)" "FW PROTOCOL SW problem" "FW PROTOCOL no free memory" "FW PROTOCOL illegal message length" "FW PROTOCOL illegal data length" "FW PROTOCOL illegal value", "FW PROTOCOL Timeout problem" "FW PROTOCOL message flow inconsistancy" "FW PROTOCOL invalid creation" "FW PROTOCOL general flow error" "FW PROTOCOL illegal message" "FW PROTOCOL general session problem" "FW PROTOCOL illegal identifier" "FW PROTOCOL illegal address" "FW PROTOCOL protcol type missmatch" "FW RULE - illegal flow" "FW RULE - illegal message" "FW RULE - illegal identifier" "FW RULE - illegal address" "FW RULE - no rule configured"

Command	Description
VIOLATION_DESCR	The following values are available for MODBUS protocol violations: "Modbus validity: illegal function" "Modbus validity: illegal sub-function" "Modbus validity: illegal encapsulated interface" "Modbus validity: unknown device ID" "Modbus validity: illegal quantity " "Modbus validity: illegal FIFO byte counter" "Modbus validity: illegal FIFO counter" "Modbus validity: illegal record number" "Modbus validity: illegal reference type" "Modbus validity: illegal byte counter" "Modbus validity: illegal length of File sub-record" "Modbus validity: illegal write quantity", "Modbus validity: illegal read quantity" "Modbus validity: illegal File sub-record length" "Rule violation: not allowed function" "Rule violation: not allowed sub function" "Rule violation: out of allowed address range" "Rule violation: not allowed quantity" "Rule violation: out of allowed value range" "Rule violation: not allowed sub function" "Rule violation: not allowed file number" "Rule violation: not allowed record number" "Rule violation: out of allowed READ address range" "Rule violation: out of allowed WRITE address range" "Rule violation: not allowed READ quantity" "Rule violation: not allowed WRITE quantity" "Rule violation: out of the allowed address range" "Rule violation: out of the allowed FIFO addresse range" "Rule violation: out of the allowed encapsulated interface range" "Rule violation: out of the allowed devise identifiers range" "Rule violation: out of the allowed object identifiers range" "Rule violation: address and quantity are out of the allowed range" "Rule violation: illegal operation" "Rule violation: inconsistent TCP Unit Identifier" The following values are available for IEC104/IEC101 protocol violations: "Iec104 validity: Illegal TypeId field" "Iec104 validity: Illegal Cause field" "Iec104 validity: Illegal APCI header" "Iec104 validity: Illegal Control field 1 in APCI header" "Iec104 validity: Illegal Control field 2 in APCI header" "Iec104 validity: Illegal Control field 3 in APCI header" "Iec104 validity: Illegal Control field 4 in APCI header" "Iec104 rule validity: Illegal type id, no rule" The following values are available for DNP3 protocol violations: "DNP3 validity: Illegal Function Code field" "DNP3 validity: Illegal Group Id field" "DNP3 validity: Invalid Object" "DNP3 validity: Parsing Error" "DNP3 validity: unused" "DNP3 validity: unused" "DNP3 validity: unused" "DNP3 validity: unused" "DNP3 validity: MAX"
SLOT_NUMBER	Serial Slot number on ComNet equipment
PORT_NUMBER	Serial port number on ComNet equipment

Command	Description
DATA_MSG_DIR	The field defines data message direction. The following values are available: "access", "network", "N/A"

DM-VPN logs

Syslog message fields description

Ssylg message	Description
"NHRP Event:<NHS-UP|NHS-DOWN>,i/f=<MGRE IF NAME>,NHS=<address>"	Appears when NHS status changed in spoke, happen when registered to NHS (NHS-UP) or NHS became unreachable (NHS-DOWN).
"<MGRE IF NAME>,<ip/mask>,<NBMA NAME>: state change <UP|DOWN> -> <UP|DOWN>"	Appears when status of mgre interface changed.
"Handle interface UP, walk over upper layer device via <ppp0>,Operator:<Mobile Operator>"	Appears when cellular interface connected to mobile network
"Handle interface DOWN, walk over upper layer devices via %s"	Appears when cellular interface disconnected from mobile network
"WTR expired for <ip/mask>,<MGRE IF NAME>"	Wait to restore timer expired. Relevant when protection group is configured between dm vpn interfaces
"WTR started for <MGRE IF NAME> <ip/mask>,<NBMA address> "	Relevant when protection group is configured between dm vpn interfaces
"WTR stopped for <MGRE IF NAME> <ip/mask>,<NBMA address> "	Relevant when protection group is configured between dm vpn interfaces
"Failed to create dm-vpn mGRE interface <MGRE IF NAME>"	Unexpected error while creating mGRE interface.
"Failed to reload config with <Mobile operator>"	Unexpected error trying to change configuration.
"Failed to create ipsec tunnel <IPSEC tunnel name>"	Failed to create ipsec tunnel
Failed to remove dm-vpn mGRE interface <MGRE IF NAME>"	Failed to remove dm-vpn mGRE interface
"Failed to remove ipsec-vpn tunnel <IPSEC tunnel name>"	Failed to remove ipsec-vpn tunnel

Cellular logs

Message fields description

Syslog message	Description
“admin status <UP|DOWN>”	Cellular enabled/disabled
“Modem is busy or no ready SIM, retrying...”	Modem is not responsive or SIM cards are not present
“Cellular Admin UP cannot be applied, SIMs are disabled. Stop operation”	SIMs are not configured.
“No ready SIMs”	A SIM is enabled, but not in READY state
“Only SIM in slot <1|2> is ready”	Only SIM in slot <1|2> is ready
“slot <1|2> is preferred”	slot <1|2> is selected as preferred
“<1|2> slot has better(or equal) RSSI (<RSSI>>=<RSSI>). Threshold is <Threshold>”	
“Both slots are below required threshold <RSSI>,<RSSI> (threshold=<Threshold>)”	Both slots are below required threshold
“<1|2> slot is above threshold as required <RSSI>>=<RSSI>. Other slot <RSSI>”	“<1|2> slot is above threshold as required
“disconnected... attempt moving to alternative provider will be performed”	Announced disconnection while other provider is configured
“disconnected... attempt to recover will be performed”	Announced disconnection while other provider is not configured
“failed to connect... attempt to recover will be performed”	Announced failure while trying to connect
“T2 expired - remove caveat on slot <1|2>”	Announce of T2 timer expiration
“T1 expired on slot <1|2>”	Announce of T1 timer expiration
“Wait to restore expired. Attempt to move to primary...”	Wait to restore expired. Attempt to move to primary SIM
“Wait to restore expired, but primary SIM is not present or disabled”	Wait to restore expired, but primary SIM is not present or disabled
“RSSI is <RSSI> - below required threshold (<Threshold>)”	RSSI is <RSSI> - below required threshold
“RSSI is <RSSI> - below required threshold (<Threshold>), but primary SIM is not present or disabled”	RSSI is <RSSI> - below required threshold (<Threshold>), but primary SIM is not present or disabled
“Continiuty check failed, attempt moving to alternative provider will be performed ”	Announce cont. check failure when alternative provider is configured
“Continiuty check failed, attempt to recover will be performed”	Announce cont. check failure when no alternative provider is configured
“unexpected failure, keep trying.... Retry within <SEC> sec”	Announce unexpected failure
“Clear caveat on slot <1|2>”	Announce clear caveat of specified slot
“Retry threshold exceeded <RETRIES>, reloading switch!”	Announce threshold exceeded of cellular failures while trying to connect
“<ppp0> connected to <Operator>,IP <address>, BAND=<WCDMA|GSM>, Channel=<channel>”	Cellular connection information
“Periodic echo check failed <NAME> LOSS=<%LOSS>(threshold=<%THRESHOLD>), RTT=<Round Trip>(threshold=<THRESHOLD>)”	Echo test failure
“change SIM slot to <1|2>”	SIM change

Syslog message	Description
"SIM[<1|2>] state chg: <UNKNOWN|DISABLED|NOT_PRESENT|PIN_LOCK|PUK_LOCK|READY|CONNECTING|FAILED|CONNECTED|CONNECTED-AS-ALTERNATIVE|CONNECTED-AS-SECONDARY> ->	
<UNKNOWN|DISABLED|NOT_PRESENT|PIN_LOCK|PUK_LOCK|READY|CONNECTING|FAILED|CONNECTED|CONNECTED-AS-ALTERNATIVE|CONNECTED-AS-SECONDARY>"	SIM state change
"Cellular experienced <NUM1> backpressure events in last <NUM2> seconds. Total since connected <NUM3>: <NUM4>"	This log is to help to fine tune the rate limit for cellular interface (Relevant when QOS is enabled)

Output example at CLI

Use the command "show logging" to retrieve following log entries.

```
<134>May 13 13:31:41 RLGE2FE16R Cellular admin status enabled
<133>May 13 13:32:08 RLGE2FE16R Cellular SIM[1] state chg: UNKNOWN -> READY
<134>May 13 13:32:16 RLGE2FE16R Cellular sim in slot 2 is disabled
<133>May 13 13:32:16 RLGE2FE16R Cellular SIM[2] state chg: UNKNOWN -> DISABLED
<134>May 13 13:32:16 RLGE2FE16R Cellular Only SIM in slot 1 is ready
<133>May 13 13:32:20 RLGE2FE16R Cellular SIM[1] state chg: READY -> CONNECTING...
<134>May 13 13:32:23 RLGE2FE16R Mgmt Handle interface DOWN, walk over upper layer devi
ces via ppp0
<134>May 13 13:32:28 RLGE2FE16R Cellular ppp0 connected to cellcom,IP 109.253.86.77, B
AND=WCDMA 850 MHz, Channel=4413
<133>May 13 13:32:28 RLGE2FE16R Cellular SIM[1] state chg: CONNECTING... -> CONNECTED!
<134>May 13 13:32:28 RLGE2FE16R Mgmt Handle interface UP, walk over upper layer device
 via ppp0,Operator:cellcom
```

Alarm Relay logs

```
"Got '<SET|CLEAR>' event from <Manual Alarm Test|Manual D-out1 Test|Manual D-out2 Test|CPU usage|Temperature|System Power|L2VPN|GIGA Ethernet Port 9|GIGA Ethernet Port 10|Cellular|IPSec|Serial|All>:<STRING from the module> (<Alarm|D-OUT1|D-OUT2> output port)"
```

<STRING from the module>
System up
CPU overload, CPU usage is very High
CPU usage is now back to normal usage-rate
Temperature exceeded, Temperature is too High
Temperature level is now back to normal extent
phase1 dead
phase1 down
phase1 up

Serial Services logs

<STRING from the module>
"connection with remote IP(<address>) for serial service id <SVC> is now resumed!!"
"no connection with remote IP(<address>) for serial service id <SVC>"
"no more missing data on Serial service id # <SVC>"
"Missing data on Serial service id # <SVC>"
"Serial Card on slot (<Slot>) is Active"
"Serial Card on slot (<Slot>) failure! Last seen <SEC>"
"Serial Station[<SLOT>,<PORT>]: Traffic is now resumed. Time=<TIME>, service-id <SVC>"
"Serial Point[<SLOT>,<PORT>,<SVC>]: No traffic since <TIME> (latest Rx=<NUM>)"

Scheduled Reload logs

Ssylog message
"Reload will happen every <SEC> seconds"
"Scheduled reload at <TIME> (within <SEC> seconds),daily=<TIME>"
"Next reload in <SEC> seconds"
"Scheduled reloading happens now!"

Commands Hierarchy

+ config terminal

- debug-logging [console | file | flash]
- +[no] logging
- On
- buffered <1-200>
- console
- facility {local0 | local1 |local2 | local3 | local4 | local5 | local6 | local7|}
- severity <level 0-7 > | emergencies | alerts | critical | errors |
  warnings | notification | informational |debugging
- logging-server <short(0-191)> {ipv4 <ucast_addr> | <host-name>}
  [port <0-65535>] [{udp | tcp | beep}]
- [no] syslog localstorage
- syslog {filename-one | filename-two | filename-three } <string(32)>
- [no] logging-file <short(0-191)> <string(32)>
- clear logs

- show logging
- show logging-file
- show syslog file-name
- show syslog role
- show debug-logging
- show system information
- show syslog localstorage
- show running-config syslog

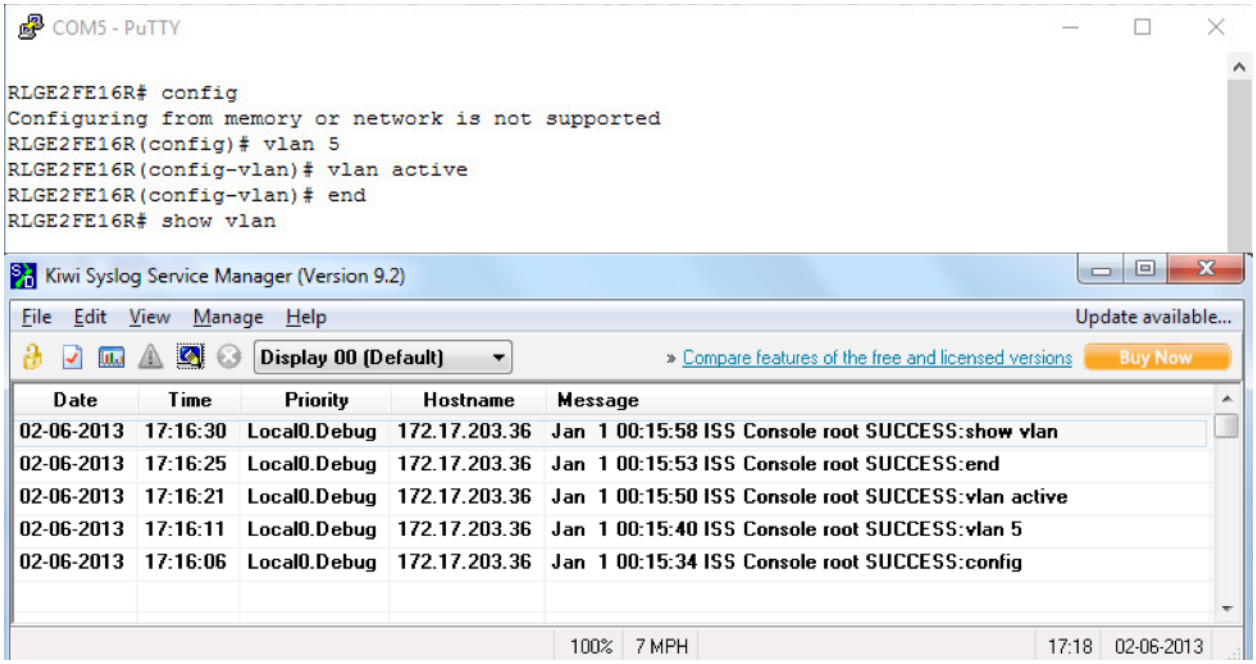
Commands Description

Command	Description
Config terminal	
logging	**buffered** - Limits Syslog messages displayed from an internal buffer. This size ranges between 1 and 200 entries. **console** - Limits messages logged to the console. **facility** - The facility that is indicated in the message. Can be one of the following values: local0, local1, local2, local3, local4,local5, local 6, local7. **severity** - Message severity level. Messages with severity level equal to or high than the specified value are printed asynchronously. This can be configured using numerical value or using the available option. The options are: 0 | emergencies - System is unusable. 1 | alerts - Immediate action needed. 2 | critical - Critical conditions. 3 | errors - Error conditions. 4 | warnings - Warning conditions. 5 | notification - Normal but significant conditions. 6 | informational - Informational messages. 7 | debugging – Debugging messages. Defaults : console - enabled severity - informational, when no option is selected while configuration. debugging, at system start-up. buffered - 50 facility - local0
logging-server	**<short(0-191)>** - Sets the priority for the syslog messages. 0-lowest priority, 191-highest priority. **ipv4** <ucast_addr>- Sets the server address type as internet protocol version 4. **Port** <integer(0-65535)> - Sets the port number through which it sends the syslog message. The value ranges between 0 and 65535. **udp** - Sets the forward transport type as udp, **tcp** - Sets the forward transport type as tcp, **beep** - Sets the forward transport type as beep.
syslog localstorage	enables the syslog file storage to log the status in the local storage path
syslog filename-one	configures a first file to store the syslog messages locally <string(32)>
logging-file <short(0-191)> <string(32)>	adds an entry in the file table
show logging	displays all the logging status and configuration information
show logging-file	displays the priority and file name of all the three files configured in the syslog file table
show syslog file-name	displays all the syslog local storage file names
show syslog role	displays the syslog role
show syslog localstorage	displays the syslog local storage

Configuration Example

```
Set a server with priority 135 for facility local0 and severity debugging (priority=135)
      RLGE2FE16R(config)# logging severity debugging
      RLGE2FE16R(config)# logging console
      RLGE2FE16R(config)# logging on
      RLGE2FE16R(config)# logging facility local0
      RLGE2FE16R(config)# logging-server 128 172.17.203.35 port 1234 udp
      RLGE2FE16R(config)# logging-server 129 172.17.203.35 port 1234 udp
      RLGE2FE16R(config)# logging-server 130 172.17.203.35 port 1234 udp
      RLGE2FE16R(config)# logging-server 131 172.17.203.35 port 1234 udp
      RLGE2FE16R(config)# logging-server 132 172.17.203.35 port 1234 udp
      RLGE2FE16R(config)# logging-server 133 172.17.203.35 port 1234 udp
      RLGE2FE16R(config)# logging-server 134 172.17.203.35 port 1234 udp
      RLGE2FE16R(config)# logging-server 135 172.17.203.35 port 1234 udp
      RLGE2FE16R(config)# end
```

The result of this configuration is that every action logged on the unit will be sent to the server. Below is shown how every cli command done on the local management is notified at the server



Output example

A typical output of syslog at console interface

```
RLGE2FE16R# show logging


<134>May 11 09:52:21 RLGE2FE16R CFA vlan1 Link Status [DOWN]
<133>May 11 09:52:21 RLGE2FE16R CFA IP Address change in Default vlan interface.
<134>May 11 09:52:21 RLGE2FE16R CFA vlan1 Link Status [UP]
<129>May  8 10:38:25 RLGE2FE16R FM [FM - MSR] : Configuration restored successfully.
<129>May  8 10:52:15 RLGE2FE16R CLI Attempt to login as su via console Succeeded
<129>May  8 10:56:31 RLGE2FE16R CLI Attempt to login as su via telnet from 172.18.212.239
Succeeded
<134>May  8 15:45:25 RLGE2FE16R MSR Saved configuration to flash successfully!
<134>May  8 15:46:00 RLGE2FE16R CFA Slot0/1 Link Status [UP]
<134>May  8 15:50:52 RLGE2FE16R CFA Slot0/1 Link Status [DOWN]
<134>May 13 14:07:37 RLGE2FE16R CFA Slot0/7 Link Status [UP]
<134>May 13 14:07:46 RLGE2FE16R CFA Slot0/7 Link Status [DOWN]
<133>May 11 09:52:21 RLGE2FE16R CFA IP Address change in Default vlan interface.
<134>May 11 13:34:52 RLGE2FE16R Mgmt Got 'SET' event from GIGA Ethernet Port 9: SFP port
#9 is Down (no output port)
<134>May 11 13:34:52 RLGE2FE16R Mgmt Got 'SET' event from GIGA Ethernet Port 10: SFP port
#10 is Down (no output port)
<129>May 11 13:34:56 RLGE2FE16R FM [FM - MSR] : Configuration restored successfully.
<129>May 11 11:38:12 RLGE2FE16R CFA Mac learning limit exceeded on Port  Fa 0/1 SRC MAC
54:53:ED:2B:19:86
<129>Jul  9 10:08:24 RLGE2FE16R FM [FM - SYS] : Temperature: 60 celsius crosses the
threshold limit. Min Temperature threshold is 10 celsius and Max Temperature threshold is
41 celsius
```

Alarm Relay

The switch has a capability to manifest system and features alarms as a relay output.

Two interfaces are available for the alarm to be set at:

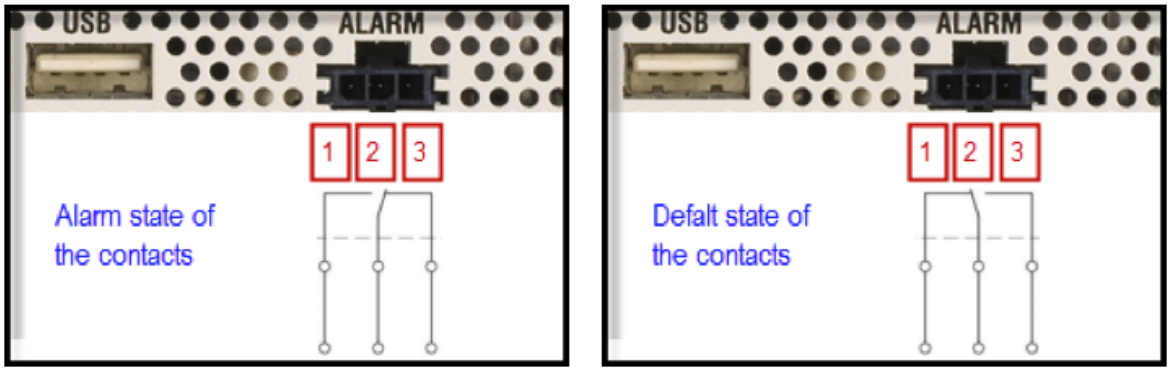
1. Dedicated 3 pole mechanical relay marked “ALARM” interface.

2. Optional 2 N/O relay contacts marked as “DRY CONTACT”.

NOTE: The physical interface used for this feature can be utilized as well for the purpose of manifesting system alarms acting as “Alarm-Relay”.
The physical interface cannot be assigned simultaneously to both feature types.
For the use of discrete channels please make sure the interface is not occupied by the Alarm-Relay service.

ALARM Interface

The relay is a 3 pole interface holding a Normally Closed (NC) state between terminals 2 and 3, and a Normally Open state between terminals 2 and 1.



Contact switching capabilities

Max DC voltage : 220v

Max current : 1A

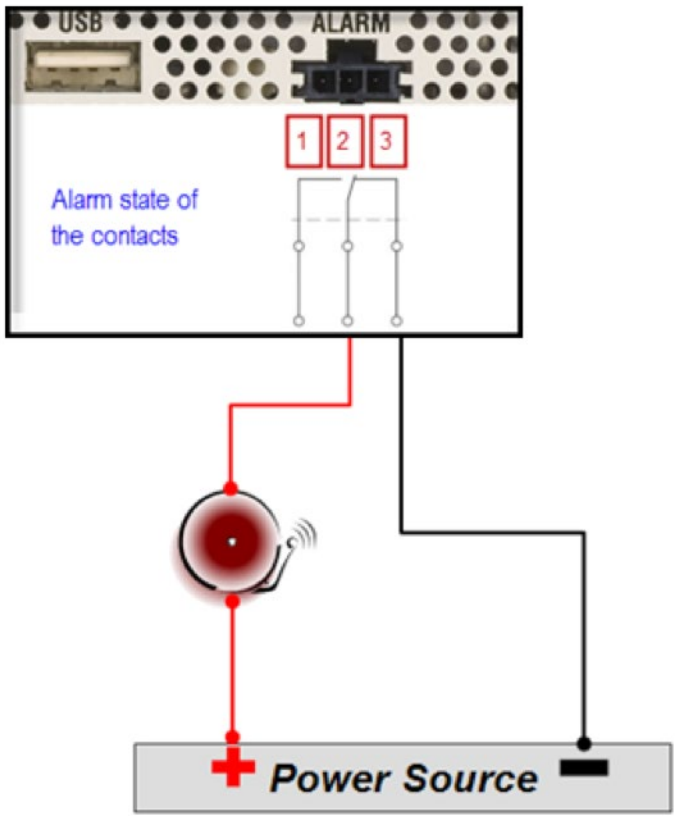
Max power : 30w

Wiring example

Below connection diagram illustrates the wiring of the alarm output at its N/O contact.

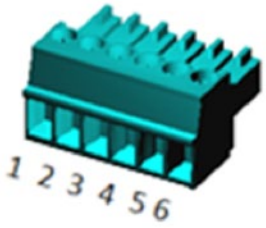
Poles 1 and 2 are normally open when no alarm trigger is available.

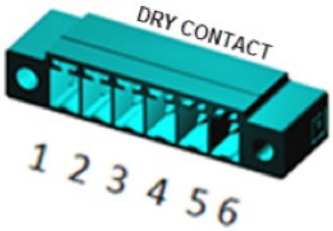
Once an alarm condition triggers the relay the contact will close as seen in this example.



DRY CONTACT Interface

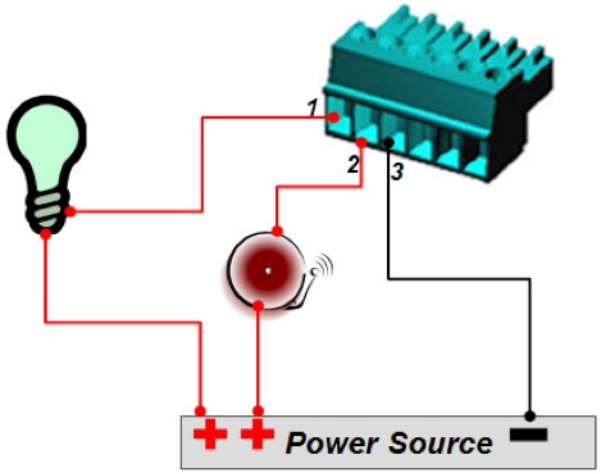
1. Digital Output 1
2. Digital Output 2
3. Digital Output Common
4. Not Applicable
5. Not Applicable
6. Not Applicable





Wiring example

Below connection diagram illustrates the wiring of the 2 alarm outputs.



Contact switching capabilities

Digital outputs are dry mechanical N/O relay contacts. Maximum power to be implemented at the contacts:

» AC: Max 250v, 37.5vA.

» DC: Max 220v, 30 watt.

Above mentioned power limitations should not be exceeded. Maximum current allowed at the contacts is 1A.

Supported Alarms

SFP port state

Two Gigabit SFP based ports are avaiable at the unit.

These are titles Gi 0/1 and Gi 0/2 (in the IF table are 9 and 10).

A state of port down for these interfaces is supported as alarm trigger (relay state change) on the chosen relay interface.

L2 VPN state

The state of a layer 2 VPN is monitored by the IPSec SA. A VPN failure is supported as alarm trigger (relay state change) on the chosen relay interface.

Temperature threshold

Alarm set if exceeds 76°C. Alarm clear when lower than 72°C.

CPU threshold

Alarm set if exceed 95% for more than 60 sec. Alarm clears when lower than 90% for more than 60 sec.

System up/down

Alarm set while system is in BOOT phase.

This specific alarm type can be associated only to the physical interface “alarm” and not to d-out1 or d-out2.

Once this alarm is activated ,no other alram types can be assigned to the interface.

Default state

No alarms are associated to the relay interfaces at default machine state.

The relay contacts are at their default mechanical state and are not triggered.

Commands Hierarchy

+ root

    + application connect

+ Alarm-relay

- Add condition { sfp_eth9| sfp_eth10| temperature| cpu-usage| l2vpn| system-power }

interface { alarm| d-out1| d-out2}

- admin-status {enable| disable}
- remove condition { sfp_eth9| sfp_eth10| temperature| cpu-usage| l2vpn| system-power }
- read interface { alarm| d-out1| d-out2}
- set interface { alarm| d-out1| d-out2} state { set| clear}
- update condition { sfp_eth9| sfp_eth10| temperature| cpu-usage| l2vpn| system-power } interface { alarm| d-out1| d-out2}
- show { admin-status| alarming_conditions| conditions| settings}

Commands Description

Command	Description
Config	
Application connect	Entering the ACE mode
Alarm-relay	Entering the alarm relay mode
Add | update	**Condition** : set the trigger condition for the alarm. temperature - Alarm set if exceeds 76°C. cpu-usage - Alarm set if exceed 95% for more than 60 sec. l2vpn – failure at the l2 VPN will trigger a relay change. sfp_eth9 – status down for this port will trigger a relay change. sfp_eth10 – status down for this port will trigger a relay change. system-power - Alarm set while in BOOT, and when the S/W performs reset. **interface** : set the target relay interface for the condition Alarm – the "ALARM" relay interface. d-out1 – Out channel 1 at the DRY-CONTACT interface. d-out2 – Out channel 2 at the DRY-CONTACT interface.
Admin-status	Enable | disable of all relay interfaces condition to alarms Default : disabled
Remove condition	Remove the assignment of trigger conditions l2vp
read interface	Read the current relay state at the interface Alarm – the "ALARM" relay interface. d-out1 – Out channel 1 at the DRY-CONTACT interface. d-out2 – Out channel 2 at the DRY-CONTACT interface.
set	**interface** : choose a target relay interface to set a static state to (not dependent on a trigger condition) Alarm – the "ALARM" relay interface. d-out1 – Out channel 1 at the DRY-CONTACT interface. d-out2 – Out channel 2 at the DRY-CONTACT interface. **State** : the static state to set the relay interface state to. Set – force to change the relay contacts from its default mechanical state. Clear - force the relay contacts to its default mechanical state.
show	Show the current state admin-status alarming_conditions conditions settings

Monitor Session

Commands Hierarchy

+ root

    + config terminal

        - monitor session <session name string> <(source | destination)> {interface <(port | port-channel)> <interface ID> | mac-acl <acl id> } [<(rx | tx | both)>]

        - set mirroring {enable | disable}

- show monitor <(all | range <mirror session range>)>

Commands Description

Command	Description
Config	
Monitor	Session name : string **Source | destination**: designation of the interface. **Interface** : source |destination interface to monitor **rx | tx | both** : monitor of tx, rx or bote. Default
set mirroring	Enable| disable the feature globally

Example

```
RLGE2FE16R# config terminal
RLGE2FE16R(config)# monitor session 1 source interface fa 0/1 both
RLGE2FE16R(config)# monitor session 1 destination interface fa 0/2
RLGE2FE16R(config)# end
```

ACE Watchdog

The ACE process availability can be verified using internal connectivity check from the GCE. If the ACE is identified as inavailable, the action can be set to reboot the unit to recover it. Such an action may help in recovering ACE services as VPN and serial tunneling.

Commands Hierarchy

+ application connect

    + watchdog

        - set do-reboot <no(no| yes)> keepalive-interval <60 seconds(5-600)> number-of-retries <3,(1-10)>

        - show

Commands Description

Command	Description
application connect	
set	do-reboot – set action to reboot the unit if the connectivity check results in fail. default- no. keepalive-interval – set the time interval in seconds for the connectivity test. default -60. number-of-retries – set the number of retries for the connectivity test. default- 3.

SNMP

Supported traps

The following traps are currently supported with version 1,2c,3.

» Port up.

» Port down.

SNMP command Hierarchy

+root

+ config

- set switch-host-name { default | <string(15)> }

- enable snmpagent

- disable snmpagent

- [no] snmp community index <CommunityIndex> name <CommunityName> security <SecurityName> [context <Name >] [{volatile | nonvolatile}] [transporttag <TransportTagIdentifier | none>] [contextengineid <ContextEngineID>]

- [no] snmp user <UserName> [auth {md5 | sha} <passwd> [priv DES <passwd>]] [{volatile | nonvolatile}] [EngineId <EngineID>]

- [no] snmp group {group name <string>} user {user name <string>} security-model {v1 | v2 | v3} [{volatile | nonvolatile}]

- [no] snmp access <GroupName> {v1 | v2c | v3 {auth | noauth | priv}} [read <ReadView | none>] [write <WriteView | none>] [notify <NotifyView | none>] [{volatile | nonvolatile}] [context <string(32)>]

- [no] snmp engineid <EngineIdentifier>

- [no] snmp view <ViewName> <OIDTree> [mask <OIDMask>] {included | excluded} [{volatile | nonvolatile}]

- [no] snmp targetaddr <Name> param <Name> <IPAddress> [timeout <1-1500>] [retries <1-3>] [taglist <TagIdentifier | none>] [{volatile | nonvolatile}] [port <1-65535>]

- [no] snmp targetparams <ParamName> user <UserName> security-model {v1 | v2c | v3 {auth | noauth | priv}} message-processing {v1 | v2c | v3} [{volatile | nonvolatile}] [filterprofile-name <profilename>] [filter-storagetype {volatile | nonvolatile}]

- snmp notify <NotifyName> tag <TagName> type {Trap | Inform} [{volatile | nonvolatile}]

- show snmp group
- show snmp user
- show snmp group access
- show snmp viewtree

SNMP Command Description

Command	Description
Config	
set switch-host-name	Set the system host name and the snmp name. configurable 15 character string. Special characters are supported except the symbol !. Default – 'RLGE2FE16R'.
enable snmpagent	This command enables SNMP agent which provides an interface between a SNMP manager and a switch. The agent processes SNMP packets received from the manager, frames the appropriate response packets and sends them to the manager. **Default** : SNMP agent is enabled.
disable snmpagent	This command disables SNMP agent
snmp community index	This command configures the SNMP community details. The no form of this command removes the SNMP community details. **<CommunityIndex>** - Creates a community index identifier which stores the index value of the row. This ID must be unique for every community name entry. default : NETMAN/PUBLIC **name<CommunityName>** - Creates a community name which stores the community string. Alpha-numeric characters are allowed. Special characters are allowed except the ! Sign. Default : NETMAN/PUBLIC **security<SecurityName>** - Stores the security model of the corresponding Snmp community name. default : none **Context <Name>** - Indicates the name of the context in which the management information is accessed when using the community string specified by the corresponding instance of snmp community name. default : null **volatile | non-volatile** - Sets the storage type as either volatile or non volatile. Default : Non Volatile **Volatile** – Sets the storage type as temporary and erases the configuration setting on restarting the system. **Non Volatile** – Sets the storage type as permanent and saves the configuration to the system. The saved configuration can be viewed on restarting the system. **<TransportTagIdentifier>** - Specifies a set of transport endpoints from which a command responder application can accept management request. default : null Contextengineid <ContextEngineID> - Indicates the location of the context through which the management information is accessed when using the community string specified by the corresponding instance of snmp community name. default : 80.00.08.1c.04.46.53

Command	Description
snmp group	This command configures SNMP group details. **Group Name** - Creates a name for an SNMP group. Default: iso/initial Default: none/initial/templateMD5/templateSHA **User** - Sets an user for the configured group. security-model - Sets the security model for SNMP V1 - Sets the SNMP version as Version 1. V2c - Sets the SNMP version as Version 2. V3 - Sets the SNMP version as Version 3. Default : v3 **volatile | non-volatile** - Sets the required storage type for the group entry default : non volatile volatile – Sets the storage type as temporary. Erases the configuration setting on restarting the system. non-volatile – Sets the storage type as permanent. Saves the configuration to the system. The saved configuration is viewed on restarting the system.
snmp access	This command configures the SNMP group access details. To configure an SNMP access along with the group, a group must have already been created using the snmp group command. Group Name - Sets the name of the group for which access is to be provided. default :iso v1 | v2c | v3- v1 – Sets the SNMP version as Version 1. v2c – Sets the SNMP version as Version 2. v3 – Sets the SNMP version as Version 3. It is the most secure model as it allows packet encryption with the priv key word **auth** - Enables Message digest (MD5) or Secure Hash Algorithm (SHA) packet authentication. **noauth**- Sets no-authentication **priv** - Sets both authentication and privacy **read** - Mentions the MIB view of the SNMP context to which read access is authorized by this entry default :iso **write** - Mentions the MIB view of the SNMP context to which write access is authorized by this entry default :iso **notify** - Mentions the MIB view of the SNMP context to which notification access is authorized by this entry default :iso **volatile | non-volatile** - Sets the required storage type for the group entry default :volatile Volatile – Sets the storage type as temporary. Erases the configuration setting on restarting the system. Non Volatile – Sets the storage type as permanent. Saves the configuration to the system. The saved configuration is viewed on restarting the system. **context** - Configures the name of the SNMP context. The maximum length of the string is 32.
snmp engineid	This command configures the engine ID that is utilized as a unique identifier of a SNMPv3 engine. This engine ID is used to identify a source SNMPv3 entity and a destination SNMPv3 entity to coordinate the exchange of messages between the source and the destination. The no form of the command resets the engine ID to the default value. Default : 80.00.08.1c.04.46.53 The Engine ID must be given as octets in hexadecimal separated by dots and the allowed length is 5 to 32 octets. SNMP engine ID is an administratively unique identifier. Changing the value of the SNMP engine ID has significant effects. All the user information will be updated automatically to reflect the change

Command	Description
snmp view	This command configures the SNMP view. To configure an SNMP view (read/write/notify), a group must have already been created using the snmp group command and SNMP group access must be configured using the snmp access command. **View Name** - Specifies the view name for which the view details are to be configured. **OID Tree** - Specifies the sub tree value for the particular view. default :1 **mask** - Specifies a mask value for the particular view. default :1 **view type** : default : included **Included** - Allows access to the subtree **excluded** - Denies access to the subtree **volatile** - Sets the storage type as temporary. Erases the configuration setting on restarting the system. default : non volatile
snmp targetaddr	This command configures the SNMP target address. **Target Address Name** - Configures a unique identifier of the Target. **Param** - Configures the parameters when generating messages to be sent to transport address. **IPAddress** - Configures a IP target address to which the generated SNMP notifications are sent. **IP6Address** - Configures a IP6 target address to which the generated SNMP notifications are sent. **Timeout** - Sets the time in which the SNMP agent waits for a response from the SNMP Manager before retransmitting the Inform Request Message. The value ranges between 1 and 1500 seconds. **Retries** - Sets the maximum number of times the agent can retransmit the Inform Request Message. The value ranges between 1 and 3. **taglist** - Sets the tag identifier that selects the target address for the SNMP. **volatile** - Sets the storage type as temporary. Erases the configuration setting on restarting the system default : volatile **nonvolatile** - Sets the storage type as permanent. Saves the configuration to the system. The saved configuration can be viewed on restarting the system. **port** <integer (1-65535)> - Configures a port number through which the generated SNMP notifications are sent to the target address. The value ranges between 1 and 65535. default : 162
snmp targetparams	This command configures the SNMP target parameters. **<ParamName>** - Sets a unique identifier of the parameter. **User** - Sets an user for which the target parameter is to bedone. **security-model** - Sets the security model default : v2c v1 – Sets the SNMP version as Version 1. v2c – Sets the SNMP version as Version 2. v3 – Sets the SNMP version as Version 3. It is the most secure model as it allows packet encryption with the priv key word **Auth** - Enables Message digest (MD5) or Secure Hash Algorithm (SHA) packet authentication **No auth** - Sets no-authentication **Priv** - Specifies both authentication and privacy **message-processing** - Sets the message processing model default : v2c v1 – Sets the SNMP version as Version 1. v2c – Sets the SNMP version as Version 2. v3 – Sets the SNMP version as Version 3. It is the most secure model as it allows packet encryption with the priv key word volatile Sets the storage type as temporary. Erases the configuration setting on restarting the system **Nonvolatile** - Sets the storage type as permanent. Saves the configuration to the system. The saved configuration can be viewed on restarting the system. **filterprofile-name** Configures the profile name filter-storagetype Sets the required storage type for the filter profile Volatile – Sets the storage type as temporary. Erases the configuration setting on restarting the system. Non Volatile – Sets the storage type as permanent. Saves the configuration to the system. The saved configuration is viewed on restarting the system.

Command	Description
snmp user	This command configures the SNMP user details. **User Name** - Configures an user name which is the User-based Security Model dependent security ID. **Auth** - Sets an authentication Algorithm. default : none. Options are: md5 - Sets the Message Digest 5 based authentication. sha - Sets the Security Hash Algorithm based authentication. **<Passwd>** - Sets the authentication password that will be used for the configured authentication algorithm. **priv DES** - Sets the DES encryption and also the password to be used for the encryption key. **volatile**- Sets the storage type as temporary. Erases the configuration setting on restarting the system **nonvolatile**- Sets the storage type as permanent. Saves the configuration to the system. You can view the saved configuration on restarting the system **Engine Id** - Sets the engine ID that is utilized as a unique identifier of a SNMPv3 engine. This engine ID is used to identify a source SNMPv3 entity and a destination SNMPv3 entity to coordinate the exchange of messages between the source and the destination.
snmp notify	This command configures the SNMP notification details. **<NotifyName>** - Configures an unique identifier associated with the entry. **Tag** - Sets a notification tag, which selects the entries in the Target Address Table. **type** - Sets the notification type. The list contains: Trap – Allows routers to send traps to SNMP managers. Trap is a one-way message from a network element such as a router, switch or server; to the network management system. Inform – Allows routers / switches to send inform requests to SNMP managers **volatile** - Sets the storage type as temporary. Erases the configuration setting on restarting the system. **Nonvolatile** - Sets the storage type as permanent. Saves the configuration to the system. You can view the Saved configuration on restarting the system

Example

1. Following configuration allows snmp v2 user WR, belonging to group corporate access to the entire tree using a view called v2all.

```
config
snmp community index ComNet name ComNet security none
snmp user WR
snmp group corporate user WR security-model v2c
snmp access corporate v2c  read v2all write v2all notify v2all
snmp view v2all 1.3 included
```

2. Allowing Traps

```
snmp targetaddr PC1 param paramlist1 172.18.212.36 taglist taglist1
snmp targetparams paramlist1 user none security-model v2c message-processing v2c
snmp notify ComNet tag taglist1 type Trap
```

Clock and Time

Local or server based time set and update are available. Clock configuration is available at both the ACE and GCE however the preferred method of configuration should be at the GCE.

Local Clock

Commands Hierarchy

+ root

- clock set-rt hh:mm:ss <day(1-31)>{january|february|march|april|may|june|july|august|september|october|november|december} <year (2000 - 2035)>

- show clock

    + config terminal

    + clock

    - time source [internal-oscillator | ntp]

    - utc-offset <offset>

    - accuracy <value(32-49)>

    - class <value(0-255)>

    - set time <time-nanoseconds>

    + application connect

    + date {[YYYY.]MM.DD-hh:mm[:ss] | hh:mm[:ss]}

    - date

Commands Description

Command	Description
Config terminal	
Clock set	
time source	Select the clock source option. internal-oscillator | ntp
Show clock	Show the GCE clock
Application connect	
Date	Set |show the ACE clock

Example

1. Example for GCE time configuration

```
RLGE2FE16R# clock set 14:00:00 20 august 2012
RLGE2FE16R# show clock
Sun Feb 02 09:42:50 2
```

2. Example for ACE time configuration

```
[/] date 2014.02.02-10:01:30
Sun Feb  2 10:01:30 UTC 2014
Current RTC date/time is 2-2-2014, 10:01:30.
[/] date
Sun Feb  2 10:01:34 UTC 2014
```

SNTP

The SNTP (Simple Network Time Protocol) is a simplified version or subnet of the NTP protocol. It is used to synchronize the time and date in RLGE2FE16R by contacting the SNTP Server. The administrator can choose whether to set the system clock manually or to enable SNTP. If SNTP is enabled, the SNTP implementation discovers the SNTP server and gets the time from the server. The SNTP implementation also has callouts to set the system time based on the time received from the SNTP server. It supports different time zones, where the user can set the required time zone.

SNTP command Hierarchy

+root

+ config terminal

+ sntp

- set sntp client {enabled | disabled}

- set sntp client version { v1 | v2 | v3 | v4 }

- set sntp client addressing-mode { unicast | broadcast | multicast | manycast }

- set sntp client port <portno(1025-65535)>

- set sntp client clock-format {ampm | hours}

- set sntp client time-zone <+/- UTC TimeDiff in Hrs:UTC TimeDiff in Min> Eg: +05:30

- set sntp client clock-summer-time <week-day-month,hh:mm> <week-day-month,hh:mm> Eg: set sntp client clock-summer-time First-Sun-Mar,05:10 Second-Sun-Nov,06:10

- set sntp client authentication-key <key-id> md5 <key>

- set sntp unicast-server auto-discovery {enabled | disabled}

- set sntp unicast-poll-interval <value (16-16284) seconds>

- set sntp unicast-max-poll-timeout <value (1-30) seconds>

- set sntp unicast-max-poll-retry <value (1-10) times>

- set sntp unicast-server {ipv4 <ucast_addr> | domain-name <string(64)>} [{primary | secondary}] [version { 3 | 4 }] [port <integer(1025-36564)>]

- set sntp broadcast-mode send-request {enabled | disabled}

- set sntp broadcast-poll-timeout [<value (1-30) seconds>]

- set sntp broadcast-delay-time [<value (1000-15000) microseconds>]

- set sntp multicast-mode send-request {enabled | disabled}

- set sntp multicast-poll-timeout [<value (1-30) seconds>]
- set sntp multicast-delay-time [<value (1000-15000) microseconds>]
- set sntp multicast-group-address {ipv4 {<mcast_addr> | default} | default}}
- set sntp manycast-poll-interval [<value (16-16284) seconds>]
- set sntp manycast-poll-timeout [<value (1-30) seconds>]
- set sntp manycast-poll-retry-count [<value (1-10)>]
- set sntp manycast-server { broadcast | multicast {ipv4 [<ipv4_addr>] }
- show sntp clock
- show sntp status
- show sntp unicast-mode status
- show sntp broadcast-mode status
- show sntp multicast-mode status
- show sntp manycast-mode status
- debug sntp (all | init-shut | mgmt | data-path | control | pkt-dump | resource | all-fail | buff)

SNTP Commands Descriptions

Command	Description
config terminal	Enters the Configuration mode
sntp	This command enters to SNTP configuration mode which allows the user to execute all the commands that supports SNTP configuration mode.
set sntp client	This command either enables or disables SNTP client module. **Enabled**: Sends a request to the host for time synchronization. **Disabled**: Does not send any request to the host for time synchronization. Defaults: Disabled.
set sntp client version	This command sets the operating version of the SNTP for the client. **v1**: Sets the version of SNTP client as 1 **v2**: Sets the version of SNTP client as 2 **v3**: Sets the version of SNTP client as 3 **v4**: Sets the version of SNTP client as 4 Defaults: v4

Command	Description
set sntp client addressing mode	This command sets the addressing mode of SNTP client. **Unicast**: Sets the addressing mode of SNTP client as unicast which operates in a point-to-point fashion. A unicast client sends a request to a designated server at its unicast address and expects a reply from which it can determine the time and, optionally, the roundtrip delay and local clock offset relative to the server. **Broadcast**: Sets the addressing mode of SNTP client as broadcast which operates in a point-to-multipoint fashion. The SNTP server uses an IP local broadcast address instead of a multicast address. The broadcast address is scoped to a single subnet, while a multicast address has Internet wide scope. **Multicast**: Sets the addressing mode of SNTP client as multicast which operates in point-to-multipoint fashion. The SNTP server uses a multicast group address to send unsolicited SNTP messages to clients. The client listens on this address and sends no requests for updates. **Anycast**: Sets the addressing mode of SNTP client as anycast which operates in a multipoint-to-point fashion. The SNTP client sends a request to a designated IPv4 local broadcast address or multicast group address. One or more anycast servers reply with their individual unicast addresses Defaults: unicast
set sntp client port	This command sets the listening port for SNTP client which refers to a port on a server that is waiting for a client connection. The value ranges between 1025 and 65535. The no form of this command deletes the listening port for SNTP client and sets the default value Defaults: 123
set sntp client clock-format	This command sets the system clock as either AM PM format or HOURS format. SNTP clock format configuration in the switch: Date – Hours, Minutes, Seconds, Date, Month and Year Month – Jan, Feb, Mar….. Year - yyyy **am-pm**: Sets the system clock in am/ pm format **hours**: Sets the system clock in 24 hours format Default: hours
set sntp client time zone	This command sets the system time zone with respect to UTC. The no form of command resets the system time zone to GMT. **+/-**: Sets the client time zone as after or before UTC. Plus indicates forward time zone and minus indicates backward time zone. Default: + 0: 0
set sntp client clock-summer- time	This command enables the DST (Daylight Saving Time). DST is a system of setting clocks ahead so that both sunrise and sunset occur at a later hour. The effect is additional daylight in the evening. Many countries observe DST, although most have their own rules and regulations for when it begins and ends. The dates of DST may change from year to year. The no form of this command disables the Daylight Saving Time. **week-day-month**: Week – First, Second, Third, Fourth or Last week of month. Day –Sunday, Monday, Tuesday, Wednesday, Thursday, Friday or Saturday. Month: January, February, March, April, May, June, July, August, September, October, November or December. **hh:mm**: Time in hours and minutes Default: Not set
set sntp client authentication-key	This command sets the authentication parameters for the key. Some SNTP severs requires authentication to be done before exchanging any data. This authentication key is used to authenticate the client to the SNTP server to which it tries to connect. The no form of this command disables authentication. **<key-id>**: Sets a key identifier (integer value) to provide authentication for the server. The value ranges between 1 and 65535. **md5**: Verifies data integrity. MD5 is intended for use with digital signature applications, which requires that large files must be compressed by a secure method before being encrypted with a secret key, under a public key cryptosystem. **<key>**: Sets the authentication code as a key value. Default: Authentication key ID not set

Command	Description
set sntp unicast-server auto-discovery	This command discovers the entire available SNTP client. **Enabled**: Automatically discovers the entire available SNTP client even if the necessary configuration is not done. **Disabled**: Does not discover any SNTP client. Defaults: Disabled
set sntp unicast-poll-interval	This command sets the SNTP client poll interval which is the maximum interval between successive messages in seconds. The value ranges between 16 and 16284 seconds. Default: 64
set sntp unicast-max-poll-timeout	This command configures SNTP client maximum poll interval timeout which is the maximum interval to wait for the poll to complete. The value ranges between 1 and 30 in seconds. Default: 5
set sntp unicast-max-poll-retry	This command configures SNTP client maximum retry poll count which is the maximum number of unanswered polls that cause a remote to identify the server as dead. The value ranges between 1 and 10 in times. Default: 3
set sntp unicast-server	This command configures SNTP unicast server. The no form of this command deletes the sntp unicast server attributes and sets to default value. **ipv4** <ucast_addr>: Sets the address type of the unicast server as Internet Protocol Version 4. **Primary**: Sets the unicast server type as primary server. **Secondary**: Sets the unicast server type as secondary server. **version 3**: Sets the SNTP version as 3. **version 4**: Sets the SNTP version as 4. **Port <integer(1025- 36564)>**: Selects the port identifier numbers in the selected server. The port number ranges between 1025 and 36564.
set sntp broadcast-mode send-request	This command either enables or disables the sntp to send status request. **Enabled**: Sends the SNTP request packet to broadcast server to calculate the actual delay. **Disabled**: Does not send any SNTP request packet to broadcast server instead default value for the delay is taken. Defaults: disabled
set sntp broadcast-poll-timeout	This command configures SNTP client poll interval in broadcast mode which is the maximum interval to wait for a poll to complete. The value ranges between 1 and 30 seconds. Default: 5
set sntp broadcast-delay-time	This command configures SNTP delay time in broadcast mode which is the time interval the SNTP client needs to wait for a response from the server. The value ranges between 1000 and 15000 in microseconds. Default: 8000
set sntp multicast-mode send-request	This command sets the status of sending the request to the multicast server to calculate the delay time. **Enabled**: Sends the SNTP request to the multicast server to calculate the actual delay time. **Disabled**: Does not send any SNTP request to the multicast server. Defaults: Disabled
set sntp multicast-poll-timeout	This command configures SNTP client poll interval in multicast mode which is the maximum interval to wait for the poll to complete. The value ranges between 1 and 30 seconds. Default: 5
set sntp multicast-delay-time	This command configures SNTP delay time in which there is no response from the multicast server. The value ranges between 1000 and 15000 in microseconds. Default: 8000
set sntp multicast-group-address	This command configures a group address for the SNTP so that all the SNTP client servers can be connected to this address. **ipv4**: Sets the Internet Protocol Version as version 4. <mcast_addr> - Sets the multicast group address. Default – Sets the multicast default address as a default value

Command	Description
set sntp manycast-poll-interval	This command configures SNTP client poll interval which is the maximum interval between successive messages. The poll interval value ranges between 16 and 16284 in seconds. Default: 64
set sntp manycast-poll-timeout	This command configures SNTP client poll timeout which is the maximum interval to wait for a poll to complete. The value ranges between 1 and 30 in seconds. Default: 5
set sntp manycast-poll-retry-count	This command configures SNTP poll retries count which is the maximum number of unanswered polls that cause a remote to identify the server as dead. The value ranges between 1 and 10 in seconds. Default: 3
set sntp manycast-server	This command configures SNTP multicast or broadcast server address in anycast mode. **Broadcast**: Configures SNTP broadcast server address in anycast mode **multicast**: Configures SNTP multicast server address in anycast mode. ipv4 <ipv4_addr> - Sets the multicast server address in internet protocol v4.
show sntp clock	This command displays the current time.
show sntp status	This command displays SNTP status.
show sntp unicast mode status	This command displays the status of SNTP in unicast mode.
show sntp broadcast mode status	This command displays the status of SNTP in broadcast mode.
show sntp multicast mode status	This command displays the status of SNTP in multicast mode.
show sntp manycast mode status	This command displays the SNTP anycast mode status.
debug sntp	This command enables SNTP trace. The no form of the command disables the SNTP trace. **All**: Generates debug statements for all kinds of traces **init-shut**: Generates debug statements for init and shutdown traces. This trace is generated on failed initialization and shutting down of SNTP related entries **mgmt**.: Generates debug statements for management traces. This trace is generated during failure in configuration of any of the SNTP features. **data-path**: Generates debug statements for data path traces. This trace is generated during failure in packet processing. **Control**: Generates debug statements for control path traces. This trace is generated during failure in modification or retrieving of SNTP entries. **pkt-dump**: Generates debug statements for packet dump traces. This trace is currently not used in SNTP module. **Resource**: Generates debug statements for OS resource related traces. This trace is generated during failure in message queues. **all-fail**: Generates debug statements for all failure traces of the above mentioned traces. **Buff**: Generates debug statements for SNTP buffer related traces. This trace is currently not used in SNTP module. Defaults: Debugging is Disabled

Example

1. Following is a configuration example

```
RLGE2FE16R# show clock
Sat Jan 01 02:00:33 2000
config
clock time source ntp
sntp
set sntp client enabled
set sntp client version v2
set sntp client clock-summer-time Last-Sun-Mar,02:00 Last-Sun-Oct,02:00
set sntp unicast-poll-interval 16
set sntp client time-zone +01:00
set sntp unicast-server ipv4 96.47.67.105 primary
set sntp unicast-server ipv4 165.193.126.229 secondary
RLGE2FE16R(config-sntp)#
<134>Feb  6 12:26:52 ISS SNTP Old Time:Sat Jan 01 2000 00:01:35  (UTC +00:00 ), New Time:Wed Feb 06 2013 12:26:52  (UTC +00:00 ), ServerIpAddress:96.47.67.105

set sntp client time-zone +01:00

RLGE2FE16R(config-sntp)# <134>Feb  6 14:34:09 ISS SNTP Old Time:Wed Feb 06 2013 12:34:02  (UTC +00:00 ), New Time:Wed Feb 06 2013 14:34:09  (UTC +02:00 ), ServerIpAddress:96.47.67.105

RLGE2FE16R# show clock

 Wed Feb 06 14:35:58 2013
RLGE2FE16R#
```

2. To remove configuration

```
config
sntp
no sntp unicast-server ipv4 96.47.67.105
```

NOTE: It is mandatory to set the clock source to ntp as shown above

SSH

SSH (Secure Shell) is a protocol for secure remote login and other secure network services over an insecure network. It consists of three major components:

» The Transport Layer Protocol provides server authentication, confidentiality and integrity.

» The User Authentication Protocol authenticates the client-side user to the server. It runs over the transport layer protocol.

The Connection Protocol multiplexes the encrypted tunnel into several logical channels. It runs over the user authentication protocol.

The client sends a service request once a secure transport layer connection has been established. A second service request is sent after user authentication is complete. This allows new protocols to be defined and coexist with these protocols.

The list of CLI commands for the configuration of SSH is as follows:

» ip ssh

» ssh

» debug ssh

» show ip ssh

SSH Command Hierarchy

+root

+config terminal

- [no] ip ssh {version compatibility | cipher ([des-cbc] [3des-cbc] [aes128- cbc] [aes256-cbc]) | auth ([hmac-md5] [hmac-sha1]) }

- ssh {enabled | disabled}

- [no] ssh server-address <IPv4> port <1-9999>

- [no] debug ssh (all | shut | mgmt | data | ctrl | dump | resource | buffer | server)

- show ip ssh

- show ssh-configurations

SSH Commands Descriptions

Command	Description
config terminal	Enters the Configuration mode
[no] ip ssh	This command configures the various parameters associated with SSH server. The no form of this command re-sets the various parameters associated with SSH server. The standard port used by SSH is 22. SSH server allows remote and secure configuration of the switch. The SSH server provides protocol version exchange, data integrity, cipher and key exchange algorithms negotiation between two communicating entities, key exchange mechanism, encryption and server authentication. The auth takes values as bit mask. Setting a bit indicates that the corresponding MAC-list will be used for authentication. **Version compatibility**: Configures the version of the SSH. When set to true, it supports both SSH version-1 and version-2. When set to false, it supports only the SSH version-2. **Cipher**: Configures the Cipher-List. This cipher-list takes values as bit mask. Setting a bit indicates that the corresponding cipher-list is used for encryption. **des-cbc** – This is a 1 bit cipherlist. It is based on a symmetric-key algorithm that uses a 56-bit key. **3des-cbc** – This is a 0 bit cipherlist. Triple DES provides a relatively simple method of increasing the key size of DES to protect against brute force attacks, without requiring a completely new block cipher algorithm. **Auth**: Configures Public key authentication for incoming SSH sessions. Defaults: version compatibility-False cipher - 3des-cbc auth - hmac-sha1
ssh	This command either enables or disables the ssh subsystem. When set to enable, the switch is accessible through ssh from a remote locations. Setting ssh to disable, removes the ssh access to the switch. **Enable**: Enables the ssh subsystem. **Disable**: Disables the ssh subsystem. Defaults: enable
ssh server-address	Set a specific GCE interface to be used for the SSH server. Other GCE interface will no longer accept incoming SSH connections. The command requires the IPv4 of a locaaly available GCE interface and the port to listen on. Port <1-9999>. The 'no' command will return the SSH server to its default state, allowing management to any GCE interface.
[no]debug ssh	This command enables the trace levels for SSH. The no form of this command re-sets the SSH trace levels. Trace. System errors such as memory allocation failures are notified using LOG messages and TRACE messages. Interface errors and protocol errors are notified using TRACE messages. Setting all the bits will enable all the trace levels and resetting them will disable all the trace levels. **All**: Generates debug statements for all traces. **Shut**: Generates debug statements for shutdown traces. This trace is generated on successful shutting down of SSH related module and memory. **mgmt**: Generates debug statements for management plane functionality traces. **data**: Generates debug statements for data path **ctrl**: Generates debug statements for Control Plane functionality traces **dump**: Generates debug statements for packets handling traces. This trace is generated when there is an error condition in transmission or reception of packets. **Resource**: Generates debug statements for traces with respect to allocation and freeing of all resource except the buffers. **Buffer**: Generates debug statements for traces with respect to allocation and freeing of buffer. **Server**: Generates debug statements while creating/ opening/ closing SSH server sockets and any failures to wake up SSH server sockets. Also generates debug statements during enabling / disabling of SSH server. Defaults: Debugging is Disabled
show ip ssh	This command displays the SSH server information such as version, cipher algorithm, authentication and trace level.

DHCP

The RLGE2FE16R supports the following DHCP modes:

1. DHCP client: local interfaces can send requests to retrieve IP from DHCP server.
2. DHCP Server: the RLGE2FE16R can allocate IP addresses to connected DHCP clients. Multiple instances are supported using the GCE and ACE services.
3. DHCP Snooping: forwarding of connected clients requests.
4. DHCP Relay: forward the DHCP packets between client and server when they are not in the same subnets.

NOTE: DHCP snooping is disabled by default. To pass clients request make sure to enable dhcp snooping.

DHCP Client and Snooping Commands Hierarchy

+ root

    + config terminal

        - ip dhcp snooping [vlan <1-3999>]

        - ip dhcp snooping verify mac-address

+ interface {fastethernet| gigabitethernet} <id>

    - [no] ip dhcp snooping trust

+ interface vlan <vlan id>

    - [no] shutdown

    - ip address dhcp

    - debug ip dhcp client all

    - show ip dhcp snooping

- release dhcp vlan <>

- renew dhcp vlan <>

- show interfaces

- show running-config dhcp

DHCP Server

The RLGE2FE16R supports DHCP Server functionality, allowing allocation of IP addresses to its local clients.

DHCP server maintains a configured set of IP address pools from which IP addresses are allocated to the DHCP clients, whenever they request the Server dynamically. Once the IP address is allocated, the Server will keep this IP as reserved until the lease time for that IP expires. If the client does not renew the IP before the lease time expiry, this will be returned into the free pool and will be offered to new clients.

The server supports IP address allocation per specific conditions as client MAC or physical port, allowing assurance for specific IP out of the pool range to be assigned.

DHCP Relay must be disabled before enabling the DHCP server. The DHCP server assumes that all pool addresses may be assigned to clients.

DHCP Server Commands Hierarchy

+ root

    + config terminal

        - no service dhcp-relay

        - service dhcp-server

+ [no] ip dhcp pool <index (1-2147483647)>

        - [no] network <network- IP> [{ <mask> | / <prefix-length (1-31)> }] [end ip]

        - [no] ip dhcp server offer-reuse <timeout (1-120)>

        - lease { <days (0-365)> [<hours (0-23)> [<minutes (1-59)>]] | infinite }

        - excluded-address <low-address> <high-address>

        - host hardware-type <1-2147483647 > {[client-identifier {mac} option <id>] | [port-identifier [interface <type> <id>]} ip {ip address}

        - option < 1-2147483647> ip {ip address}

- show ip dhcp server information

- debug ip dhcp server all

    - show ip dhcp server binding

    - renew dhcp vlan <>

    - show ip dhcp server statistics

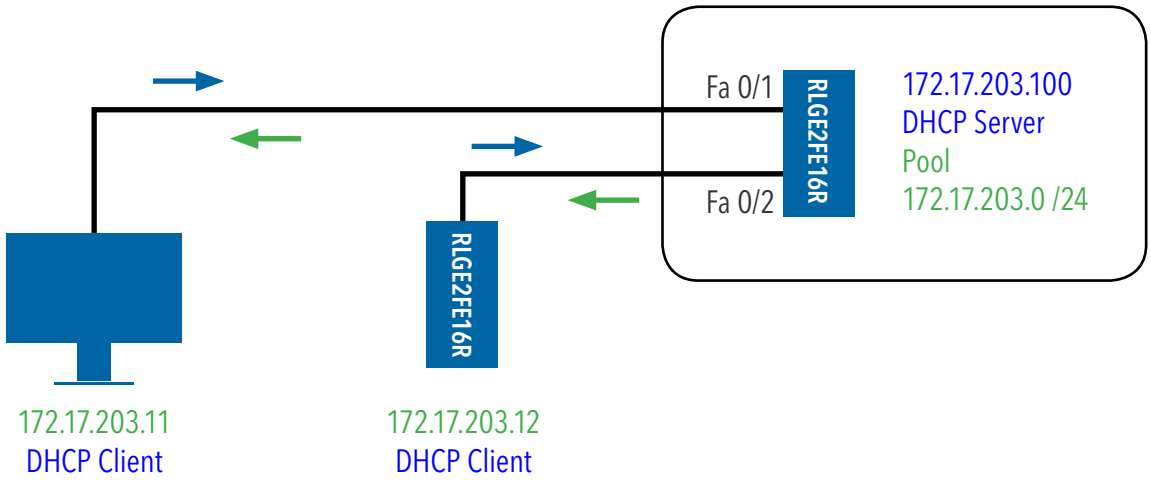
    - show running-config dhcp

DHCP Relay Commands Description

Command	Description
no service dhcp-relay	Disabling dhcp relay is mandatory in order to activate dhcp server
[no] service dhcp-server	Enable | disable dhcp server
Config terminal	
[no] ip dhcp pool	This command creates a DHCP server address pool and enters in to the DHCP pool configuration mode in which the pool is customized.
[no] ip dhcp	This command enables ICMP echo mechanism or configures offer-reuse timeout for the DHCP server. These parameters are used to control the allocation of IP address to a DHCP client. ping packets - Enables / disables ICMP echo mechanism. This mechanism allows the DHCP server to verify the availability of an IP address before assigning it to a DHCP client. DHCP server sends ping packets to the IP address that is intended to be assigned for the DHCP client. If the ping operation fails, DHCP server assumes that the address is not in use and assigns the address to the requesting DHCP client. server offerreuse - Configures the amount of time (in seconds), the DHCP server entity should wait for the DHCP REQUEST from the DHCP client before reusing the lease offer for other DHCP client. Binding - Deletes the specified IP address entry from the server binding table. This frees the IP address allocated to a DHCP client, so that the IP address can be allocated for another DHCP client.
[no] network	This command creates a subnet pool that defines a network IP subnet address for the corresponding DHCP address pool and contains IP addresses to be assigned to the DHCP client.
ip dhcp server offer-reuse	
Lease	This command configures, for the corresponding DHCP server, the DHCP lease period for an IP address that is assigned from a DHCP server to a DHCP client.
excluded-address	This command creates an excluded pool that defines a range of IP addresses which needs to be excluded from the created subnet pool. That is, the IP addresses in this range including start and end IP address of the excluded pool are not assigned to any DHCP client.
Host hardware-type	This command configures host hardware type and its DHCP option with specific values for the corresponding DHCP server address pool. client-identifier: assign specific IP address from the pool range to be assigned to a specific MAC. The IP will be reserved for that MAC. port-identifier: assign specific IP address from the pool range to be assigned to a host connected at specific port. The IP will be reserved for that port, regardless of the host MAC. A single host (dhcp client) is allowed to be connected at a port for which this option is used for.

Example

Following example will demonstrate allocation of IP addresses by a RLGE2FE16R set as dhcp server to two different clients.



DHCP Server

1. set system host name (optional)

```
set host-name dhcp-server
```

2. set GCE interface

```
config
interface vlan 1
ip address 172.17.203.100 255.255.255.0
no shutdown
exit
```

3. enable dhcp server

```
no service dhcp-relay
service dhcp-server
```

4. set IP range pool as 172.17.203.0/24 with excluded range of 1-10.

```
ip dhcp pool 1
network 172.17.203.0 255.255.255.0
excluded-address 172.17.203.1  172.17.203.10
exit
```

5. set a default router ip to be sent to the clients as default gateway.

```
ip dhcp pool 1
default-router 172.17.203.100
end
write startup-config
```

DHCP Client

1. set system host name (optional)

```
set host-name dhcp-client
```

2. set GCE interface

```
config
interface vlan 1
ip address dhcp
no shutdown
end
write startup-config
```

DHCP Server show outputs

```
dhcp-server# show ip dhcp server binding
Ip                Hw          Hw                   Binding    Expire
Address           Type        Address              State      Time
-------           -------     ------               --------   ----------
172.17.203.12     Ethernet    54:53:ed:2b:19:22   Assigned   Apr   7 06:34:51 2000
172.17.203.11     Ethernet    54:53:ed:2b:19:86   Assigned   Apr   7 06:49:57 2000
dhcp-server# show ip dhcp server pools
Pool Id                          : 1
-----------------------------------------
Subnet                           : 172.17.203.0
Subnet Mask                      : 255.255.255.0
Lease time                       : 3600 secs
Utilization threshold            : 75%
Start Ip                         : 172.17.203.11
End Ip                           : 172.17.203.254
Subnet Options
--------------
Code        :      1, Value       : 255.255.255.0
```

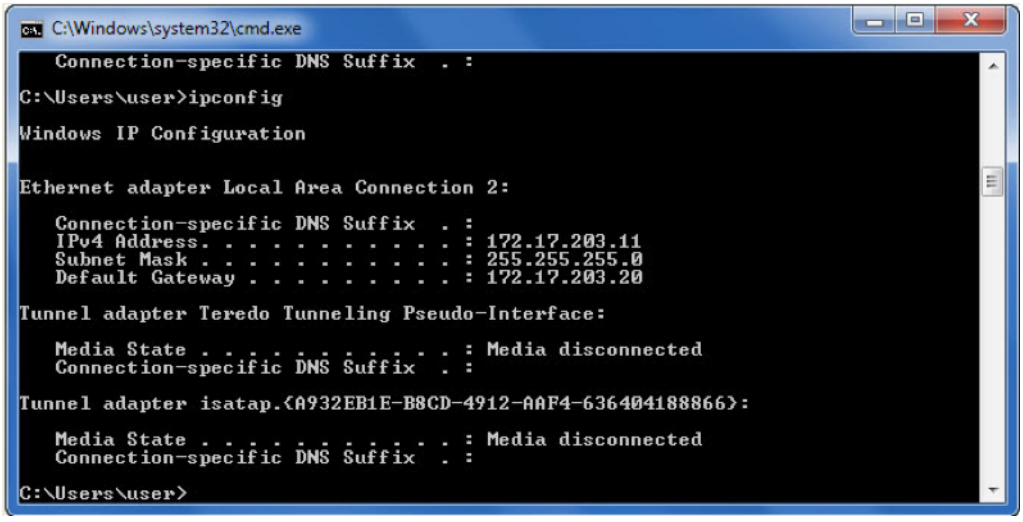
```
Code        :      3, Value       : 172.17.203.100
dhcp-server# show ip dhcp server information
DHCP server status                    : Enable
Send Ping Packets                     : Disable
Debug level                            : None
Server Address Reuse Timeout         : 5 secs
Next Server Adress                    : 0.0.0.0
Boot file name
dhcp-server# show ip dhcp server statistics
Address pools : 1
Message                   Received
-------                   --------
DHCPDISCOVER             2
DHCPREQUEST              5
DHCPDECLINE              0
DHCPRELEASE              0
DHCPINFORM               0
Message                   Sent
-------                   ----
DHCPOFFER                2
DHCPACK                  5
DHCPNAK                  0
dhcp-server#
```

DHCP Client show outputs

```
dhcp-client# show ip interface
vlan1 is up, line protocol is up
Internet Address is 172.17.203.12/24
Broadcast Address  172.17.203.255
IP address allocation method is dynamic
IP address allocation protocol is dhcp
dhcp-client#
dhcp-client# show ip dhcp client stats
Dhcp Client Statistics
--------------------------
Interface                        : vlan1
Client IP Address               : 172.17.203.12
Client Lease Time               : 3600
Client Remain Lease Time        : 2550
```

```
Message Statistics
------------------
DHCP DISCOVER                    : 4
DHCP REQUEST                     : 3
DHCP DECLINE                     : 0
DHCP RELEASE                     : 0
DHCP INFORM                      : 0
DHCP OFFER                       : 1
DHCP ACKS IN REQ                 : 1
DHCP NACKS IN REQ                : 0
DHCP ACKS IN RENEW               : 2
DHCP NACKS IN RENEW              : 0
DHCP ACKS IN REBIND              : 0
DHCP NACKS IN REBIND             : 0
DHCP ACKS IN REBOOT              : 0
DHCP NACKS IN REBOOT             : 0
DHCP COUNT ERROR IN HEADER       : 0
DHCP COUNT ERROR IN XID          : 0
DHCP COUNT ERROR IN OPTIONS      : 0
dhcp-client#
```

PC Client view



DHCP Relay

DHCP relay agent is used to forward the DHCP packets between client and server when they are not in the same subnets. The relay receives packets from the client and inserts certain information like the network in which the packet is received and then forwards it to the server. The Server identifies the client's network from this information and allocates IP accordingly, then sends the reply to the relay. The Relay then strips the information inserted and broadcasts the packets into the client's network.

A maximum of 5 servers can be configured. If no servers are configured, then the DHCP packets will be broadcasted to entire network, except to the network from which packet is received.

DHCP-Relay is supported at both the GCE and ACE. The ACE should be used if segregation of DHCP relay services is required. The ACE and GCE DHCP services are each a separate service and thus the user is supported with multiple, segregated services.

NOTE: By default, DHCP-Relay is disabled.

With ComNet systems supporting DHCP Server (future feature) mode, the server must be disabled prior to enabling DHCP-Relay mode.

DHCP Relay GCE Command Hierarchy

+root

+config terminal

- no server dhcp-server

- [no] service dhcp-relay

- ip dhcp server <A.B.C.D>

- ip dhcp relay circuit-id option [router-index] [vlanid] [recv-port]

- ip dhcp relay information option

+ interface vlan <>

    - [no] shutdown

- ip address < A.B.C.D > <subnet>

- ip dhcp relay circuit-id <numeric circuit-id>

- ip dhcp relay information option

- ip dhcp relay remote-id <remote-id name>

- debug ip dhcp relay all
- show ip dhcp relay information [vlan <>]
- show ip interface
- show running-config dhcp

DHCP Relay GCE Commands Description

Command	Description
Config terminal	
no server dhcp-server	DHCP server is not available at the system and must be disabled to activate DHCP relay function
service dhcp-relay	This command enables the DHCP relay agent in the switch. The no form of the command disables the DHCP relay agent. DHCP relay agent relays DHCP messages between DHCP client and DHCP server located in different subnets.
ip dhcp server <A.B.C.D>	This command adds the configured IP address to the IP address list created for the DHCP server. The switches or systems having these IP addresses represent the DHCP servers to which the DHCP relay agent can forward the packets that are received from DHCP clients. The no form of the command deletes the mentioned IP address from the IP address list. The DHCP relay agent broadcasts the received packets to entire network except the network from which the packets are received, if the DHCP server list is empty (that is IP address is configured as 0.0.0.0).
ip dhcp relay circuit-id option	This command defines the type of information to be present in circuit ID sub-option that is used in the DHCP relay agent information option. **router-index** - Adds information related to router interface indexes in the circuit ID sub-option. **vlanid** - Adds information related to VLAN IDs in the circuit ID sub-option. **recv-port** - Adds information related to physical interfaces or LAG ports in the circuit ID sub-option
ip dhcp relay information option	This command enables the DHCP relay agent to perform processing related to DHCP relay agent information option. The no form of the command disables the processing related to DHCP relay agent information option. The options contains a sub-option for agent circuit ID details and another sub-option for agent remote ID details. The processing involves: Insertion of DHCP relay information option in DHCP request messages forwarded to a DHCP server from a DHCP client. Examining / removing of DHCP relay information option from DHCP response messages forwarded to the DHCP client from the DHCP server.
interface vlan <id>	
ip dhcp relay circuit-id	This command configures circuit ID value for an interface. The no form of the command deletes the circuit ID configuration for the interface (that is, the circuit ID is configured as 0). The circuit ID uniquely identifies a circuit over which the incoming DHCP packet is received. In DHCP relay, it is used to identify the correct circuit over which the DHCP responses should be relayed. The configured circuit ID is used in the DHCP relay agent information option to inform the DHCP server about the interface from which DHCP packet is received. The circuit ID is unique for the interfaces and ranges from 1 to 2147483647.

Command	Description
ip dhcp relay information option	This command enables the DHCP relay agent to perform processing related to DHCP relay agent information option. The no form of the command disables the processing related to DHCP relay agent information option. The options contains a sub-option for agent circuit ID details and another sub-option for agent remote ID details. The processing involves: Insertion of DHCP relay information option in DHCP request messages forwarded to a DHCP server from a DHCP client. Examining/removing of DHCP relay information option from DHCP response messages forwarded to the DHCP client from the DHCP server.
ip dhcp relay remote-id	This command configures remote ID value for an interface. The no form of the command deletes the remote ID configuration for the interface (that is, the remote ID is set with a string of length zero). The configured remote ID is used to inform the DHCP client about the remote circuit to which the DHCP packets should be forwarded from the interface. The remote ID is globally unique and an octet string of maximum size of 32. The remote ID should not be same as that of the default value.

DHCP Relay ACE Command Hierarchy

+ application connect

    + router dhcp

- add-interface {vlan <vlan-id>] |[interface-name <eth1.<vlan-id>]} {server-address <A.B.C.D>}

- remove-interface {vlan <vlan-id>] |[interface-name <eth1.<vlan-id>]}

- update option-82 {enable| disable}

- enable

- disable

+ show

- allowed-interfaces

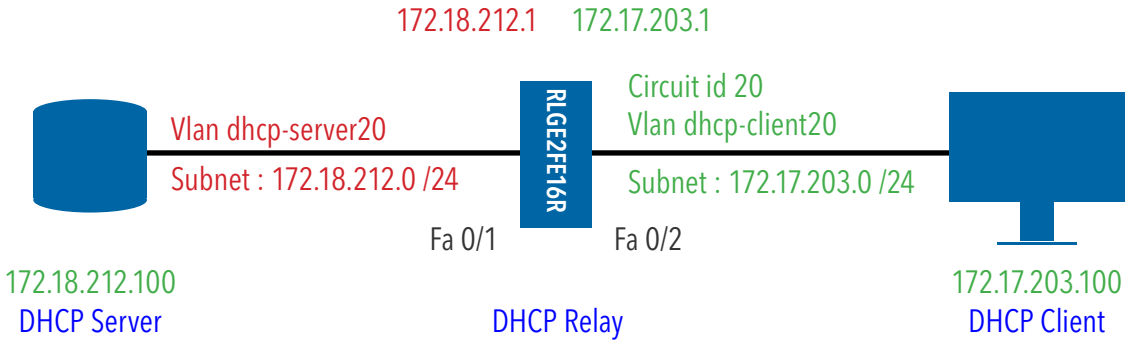
- status

DHCP Relay ACE Commands Description

Command	Description
application connect	Access the ACE mode
Add| remove interface	Add interface behind which the DHCP server is connected. Server-address: IPv4 address of the DHCP server. VLAN: identify the local ACE interface behind which the DHCP clients reside by its VLAN. Interface-name: identify the local ACE interface behind which the DHCP clients reside by its name. eth1<vlan-id>
update option-82	Enable| disable support of option 82
Enable| disable	Enable/disable the DHCP relay
Show	Show output of the DHCP configuration and state
ip dhcp relay information option	This command enables the DHCP relay agent to perform processing related to DHCP relay agent information option. The no form of the command disables the processing related to DHCP relay agent information option. The options contains a sub-option for agent circuit ID details and another sub-option for agent remote ID details. The processing involves: Insertion of DHCP relay information option in DHCP request messages forwarded to a DHCP server from a DHCP client. Examining / removing of DHCP relay information option from DHCP response messages forwarded to the DHCP client from the DHCP server.
interface vlan <id>	
ip dhcp relay circuit-id	This command configures circuit ID value for an interface. The no form of the command deletes the circuit ID configuration for the interface (that is, the circuit ID is configured as 0). The circuit ID uniquely identifies a circuit over which the incoming DHCP packet is received. In DHCP relay, it is used to identify the correct circuit over which the DHCP responses should be relayed. The configured circuit ID is used in the DHCP relay agent information option to inform the DHCP server about the interface from which DHCP packet is received. The circuit ID is unique for the interfaces and ranges from 1 to 2147483647.

Example, GCE DHCP Relay

Following setup will illustrate DHCP-Relay configuration.



1. Configure vlan and ip interface towards the server

```
config
vlan 10
ports fastethernet 0/1 untagged fastethernet 0/1 name dhcp-server
exit
interface fastethernet 0/1
switchport pvid 10
exit

interface vlan 10
ip address 172.18.212.1 255.255.255.0
no shutdown
exit
```

2. Configure vlan and ip interface towards the client

```
vlan 20
ports fastethernet 0/2 untagged fastethernet 0/2 name dhcp-client
exit
interface fastethernet 0/2
switchport pvid 20
exit
interface vlan 20
ip address 172.17.203.1 255.255.255.0
no shutdown
exit
```

3. Enable dhcp-relay option

```
no service dhcp-server
service dhcp-relay
ip dhcp relay information option
```

4. Set the address of the dhcp server

```
ip dhcp server 172.18.212.100
```

5. set a circuit id to the client interface

```
interface vlan 20
ip dhcp relay circuit-id 20
end
write startup-cfg
```

The configuration will result in following state

```
RLGE2FE16R# sh ip dhcp relay information

Dhcp Relay                    : Enabled
Dhcp Relay Servers only      : Enabled

DHCP server 1                 : 172.18.212.100

Dhcp Relay RAI option        : Enabled
Default Circuit Id information : router-index
Debug Level                   : 0x1

No of Packets inserted RAI option                : 0
No of Packets inserted circuit ID suboption     : 0
No of Packets inserted remote ID suboption      : 0
No of Packets inserted subnet mask suboption    : 0
No of Packets dropped                             : 0
No of Packets which did not inserted RAI option : 0

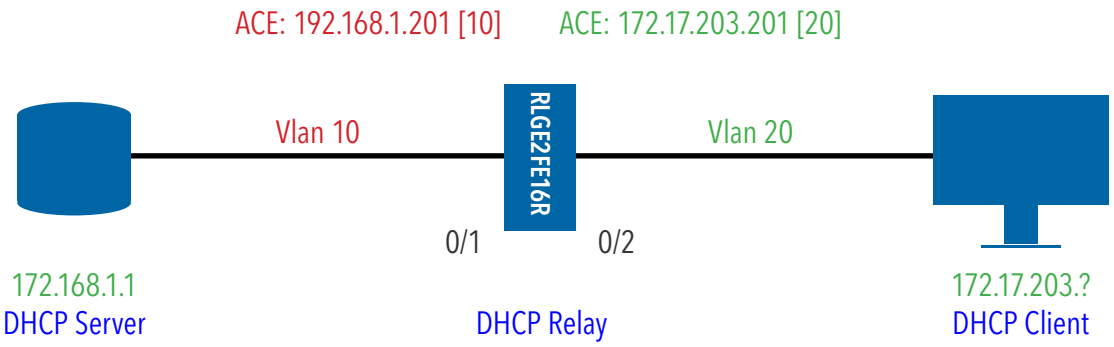


Interface  vlan20
Circuit ID : 20
Remote  ID : XYZ
```

```
RLGE2FE16R#
```

Example, ACE DHCP Relay

Following setup will illustrate DHCP-Relay configuration.



1. Configure vlan and ip interface towards the server

```
config
vlan 10
ports fastethernet 0/1 gigabitethernet 0/3 untagged fastethernet 0/1 name dhcp-server
exit
interface fastethernet 0/1
switchport pvid 10
exit
interface vlan 10
ip address 172.18.212.101 255.255.255.0
no shutdown
exit
```

2. Configure vlan and ip interface towards the client

```
vlan 20
ports fastethernet 0/2 gigabitethernet 0/3 untagged fastethernet 0/2 name dhcp-client
exit
interface fastethernet 0/2
switchport pvid 20
end
```

3. Create ACE interfaces for the dhcp relay

```
application connect
router interface create address-prefix 172.17.203.201/24 vlan 20 purpose application-host
router interface create address-prefix 192.168.1.201/24 vlan 10 purpose general
```

4. Set the configuration of the dhcp

```
router dhcp-relay add-interface server-address 192.168.1.1 vlan 20
router dhcp-relay enable
exit
write startup-cfg
```

5. Verify configuration

```
[/]router interface show
+----+------+---------+------------------+------+-----------------+-------------+----------
---+
| Id | VLAN |  Name   |      IP/Subnet      | Mtu  |      Purpose       | Admin status |
Description |
+====+======+=========+==================+======+=================+=============+====
=========+
| 1  |  10  | eth1.10 | 192.168.1.201/24  | 1500 |      general       |    enable    |
|
+----+------+---------+------------------+------+-----------------+-------------+----------
---+
| 2  |  20  | eth1.20 | 172.17.203.201/24 | 1500 | application host |    enable    |
|
+----+------+---------+------------------+------+-----------------+-------------+----------
---+
[/]
[/]router dhcp-relay show allowed-interfaces
+---------+-----------------+-------------+
| If name |       If IP        |  Server IP  |
+=========+=================+=============+
| eth1.10 | 192.168.1.201/24 | 192.168.1.1 |
+---------+-----------------+-------------+
Completed OK
[/]router dhcp-relay show status
+--------------+-----------+
| Admin Status | Option 82 |
+==============+===========+
|    enable    |  enable   |
+--------------+-----------+
Completed OK
[/]
```

RADIUS

RADIUS (Remote Authentication Dial-In User Service), widely used in network environments, is a Client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. It is commonly used for embedded network devices such as routers, modem servers, switches and so on.

RADIUS is currently the de-facto standard for remote authentication. It is very prevalent in both new and legacy systems. It is used for several reasons:

» RADIUS facilitates centralized user administration (Authentication, Authorization and Accounting).

» RADIUS consistently provides some level of protection against an active attacker.

The list of CLI commands for the configuration of RADIUS is as follows:

» radius-server host

» debug radius

» show radius server

» show radius statistics

RADIUS Command Hierarchy

+ root

+ config terminal

- login authentication radius [local]

- [no]radius-server host {ipv4-address | host-name} [auth-port <integer(1-65535)>] [acct-port <integer(1-65535)>] [timeout <1-120>] [retransmit <1-254>] [key <secret-key-string>] [primary]

- show radius server

RADIUS Commands Descriptions

Command	Description
config terminal	Enters the Configuration mode
[no]radius-server host{ipv4-address | host-name} [auth-port <integer(1-65535)>] [acct-port <integer(1-65535)>] [timeout <1-120>] [retransmit <1-254>] [key <secret-key-string>] [primary]	This command configures the RADIUS client with the parameters (host, timeout, key, retransmit).The no form of the command deletes RADIUS server configuration. **ipv4-address**: Configures the IPv4 address of the RADIUS server host. **host-name**: Configures the DNS (Domain Name System) name of the RADIUS server host. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported. **auth-port <integer(1-65535)>**: Configures a specific UDP (User Datagram Protocol) destination port on this RADIUS server to be used solely for the authentication requests. The value of the auth port ranges between 1 and 65535. **acct-port <integer (1-65535)>**: Configures a specific UDP destination port on this RADIUS to be solely used for accounting requests. The value of the auth port ranges between 1 and 65535. **timeout <1-120>**: Configures the time period in seconds for which a client waits for a response from the server before re-transmitting the request. The value of the time out in ranges between 1 to 120 in seconds. **retransmit <1- 254>**: Configures the maximum number of attempts the client undertakes to contact the server. The value number of retransmit attempts ranges between 1 and 254 **key <secret-keystring>**: Configures the Per-server encryption key which specifies the authentication and encryption key for all RADIUS communications between the authenticator and the RADIUS server. The value of the maximum length of the secret key string is 46. should be 1-46 characters length. May include small letters. May include capitol letter. must include numbers May include special symbol. allowed symbols: @#$%^&*()-+./<\` **Primary**: Sets the RADIUS server as the primary server. Only one primary server will be replaced, when the command is executed with this option. server can be configured as the primary server, any existing Defaults: timeout - 3 seconds Retransmit - 3 attempts key- empty string
show radius server	This command displays RADIUS server Host information which contains, Index, Server address, Shared secret, Radius Server status, Response Time, Maximum Retransmission, Authentication Port and Accounting Port. **<ucast_addr>**: Displays the related information of the specified unicast address of the RADIUS server host. **<string>**: Displays the name of the RADIUS server host. This maximum value of the string is of size 32.
show radius statistics	This command displays RADIUS Server Statistics for the data transfer between server and the client from the time of initiation.

Example

1. configure server list and selected primary

```
RLGE2FE16R(config)# radius-server host 172.18.212.65 timeout <1-120> retransmit <1-254>
                key <key> primary
RLGE2FE16R(config)# radius-server host 172.18.212.45 timeout <1-120> retransmit <1-254>
                key <key>
```

2. set default login authentication method

```
      RLGE2FE16R(config)# login authentication radius local
      RLGE2FE16R(config)# end
      RLGE2FE16R# write startup-cfg
```

Output example

```
RLGE2FE16R# show radius server
Primary Server            : 172.18.212.65

Radius Server Host Information
------------------------------
Index                      : 1
Server address             : 172.18.212.65
Shared secret              :
Radius Server Status      : Enabled
Response Time              : 10
Maximum Retransmission    : 3
Authentication Port       : 1812
Accounting Port            : 1813
-----------------------------------------
Index                      : 2
Server address             : 172.18.212.45
Shared secret              :
Radius Server Status      : Enabled
Response Time              : 10
Maximum Retransmission    : 3
Authentication Port       : 1812
Accounting Port            : 1813
-----------------------------------------
```

TACACS

TACACS (Terminal Access Controller Access Control System), widely used in network environments, is a client/server protocol that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. It is commonly used for providing NAS (Network Access Security). NAS ensures secure access from remotely connected users. TACACS implements the TACACS Client and provides the AAA (Authentication, Authorization and Accounting) functionalities. TACACS is used for several reasons:

» Facilitates centralized user administration.

» Uses TCP for transport to ensure reliable delivery.

» Supports inbound authentication, outbound authentication and change password request for the Authentication service.

» Provides some level of protection against an active attacker.

The list of CLI commands for the configuration of TACACS is as follows:

» tacacs-server host

» tacacs use-server address

» tacacs-server retransmit

» debug tacacs

» show tacacs

TACACS+ is a security application that provides centralized validation of users attempting to gain access to a router or Network Access Server. TACACS+ allows a client to accept a username and password and sends a query to a TACACS+ authentication server, sometimes called TACACS+ daemon or simply TACACS+D.

The TACACS+ server is generally a program running on a host. The host determines whether to accept or deny the request and sends a response back. A Network Access Server (NAS) operates as a TACACS+ Client.

TACACS+ services (the user and group profiles with the authentication and the authorization information) are maintained in a central security database on a TACACS+ daemon running typically on a UNIX or Windows NT workstation. .TACACS+ is commonly used for embedded network devices such as routers, modem servers, switches, etc.

Default Configurations

Feature	Default Setting
tacacs-server timeout	5 seconds
login authentication	Local

TACACS Command Hierarchy

+root

+ config terminal

- [no] tacacs-server host {ipv4-address} [timeout <5,(1-255)>] [key <secret-key-string>]

- tacacs-server host {ipv4-address} {port <40,(1-65535)>}

- tacacs-server retransmit <2,(1-100)>

- [no] tacacs use-server address{ipv4-address }

- [no] login authentication tacacs [local]

- show tacacs

- show system-information

- show running-config tacacs

TACACS Commands Descriptions

Command	Description
tacacs-server host	This command configures the TACACS server with the parameters (host, timeout, key) and specifies the IP address of one or more TACACS and it specifies the names of the IP host or hosts maintaining a TACACS+ server. The no form of the command deletes server entry from the TACACS server table. **<ipv4-address>**: Configures the IPv4 address of the host **Port <tcp port (1- 65535)>**: Configures the TCP port number in which the multiple sessions are established. The value ranges between 1 and 65535. **Timeout <time out in seconds(1-255)>**: Configures the time period (in seconds) till which a client waits for a response from the server before closing the TCP connection. The link between the server and the client gets disconnected, if the specified time is exceeded. The value ranges from 1 to 255 seconds. **Key <secret key>**: Specifies the authentication and encryption key for all TACACS communications between the authenticator and the TACACS server. The value is string of maximum length 64. should be 1-64 characters length. May include small letters. May include capitol letter. must include numbers May include special symbol. allowed symbols: @#$%^&*()-+./<\` Defaults: port – 40, Timeout - 5 seconds
tacacs use-server address	This command configures the server IP address and an active server from the list of servers available in the TACACS server table. The no form of the command disables the configured client active server. **<ipv4-address>**: Configures the IPv4 address of the host
tacacs-server retransmit	Number of times the client searches the active server from the list of servers maintained in the TACACS client. The retransmit value ranges from 1 to 100 seconds. Defaults: 2 seconds
debug tacacs	This command sets the debug trace level for TACACS client module. The no form of the command disables the debug trace level for TACACS client module. **All**: Generates debug messages for all possible traces (Dumptx, Dumprx, Error, Info). **Info**: Generates debug statements for server information messages such as TACACS session timed out, server unreachability, Session ID exceeded and so on. **Errors**: Generates debug statements for error debug messages such as failure caused during packet transmRLGE2FE16Rion and reception. **Dumptx**: Generates debug statements for handling traces. This trace is generated when there is an error condition in transmRLGE2FE16Rion of packets. **Dumprx**: Generates debug statements for handling traces. This trace is generated when there is an error condition in reception of packets. Defaults: Debugging is Disabled
show tacacs	This command displays the server (such as IP address, Single connection, Port and so on) and statistical log information (such as Authen. Starts sent, Authen. Continues sent, Authen. Enables sent, Authen. Aborts sent and so on) for TACACS+ client.

Configuration Example

1. configure server list

```
RLGE2FE16R(config)# tacacs-server host 172.18.212.210 key secretkey
RLGE2FE16R(config)# tacacs-server host 172.18.212.49  timeout 5 key secretkey
```

2. configure default server

```
      RLGE2FE16R(config)# tacacs use-server address 172.18.212.210
```

3. set default login authentication method

```
      RLGE2FE16R(config)# login authentication tacacs local
      RLGE2FE16R(config)# end
      RLGE2FE16R# write startup-cfg
```

4. remove tacacs configuration

```
config
no tacacs use-server
no tacacs-server host 172.18.212.210
login authentication local
```

Output example

```
RLGE2FE16R# show tacacs
Server : 1
Server address            : 172.18.212.49
Address Type              : IPV4
        Single Connection : no
        TCP port          : 49
        Timeout           : 5
        Secret Key        :
Server : 2
Server address            : 172.18.212.210
Address Type              : IPV4
        Single Connection : no
        TCP port          : 49
        Timeout           : 5
        Secret Key        :
 Active Server address: 172.18.212.210
```

802.1x

802.1X defines a client-server based access control and authentication protocol. It provides a means of authenticating and authorizing devices attached to a port, thus preventing access to unauthorized clients. The authentication server authenticates each client connected to a switch port before allowing any services offered by the switch.

Until the client is authenticated, 802.1X access control allows only EAPOL (Extensible Authentication Protocol over LAN) traffic through the port on which the client is connected. When the port connecting the client (Port-Based authentication) is authenticated, normal traffic is allowed through the port. If MAC based authentication is enabled on the port, and if the Client MAC-address session is authenticated, then the traffic from the client is allowed.

802.1x Commands Hierarchy

+ root

+ config terminal

- [no] aaa authentication dot1x default { group {radius | tacacsplus | tacacs+} |local}

- [no] dot1x local-database <username> password <password> permission {allow | deny} [<auth-timeout (value(1-7200))>] [interface <interface-type> <interface list>]

- [no] dot1x system-auth-control

- [no] shutdown dot1x

- [no] dot1x timeout {quiet-period <value (0-65535)> | {reauth-period | servertimeout | supp-timeout | tx-period | start-period | held-period | auth-period} <value (1-65535)>}

+ interface <type> <id>

- [no] dot1x max-req <count(1-10)>

- [no] dot1x max-start <count(1-65535)>

- [no] dot1x reauthentication

- [no] dot1x port-control {auto|force-authorized|force-unauthorized}

- [no] dot1x auth-mode {port-based | mac-based}

- show dot1x [{ interface <interface-type> <interface-id> | statistics interface <interface-type> <interface-id> | supplicant-statistics interface <interfacetype> <interface-id>|local-database | mac-info [address <aa.aa.aa.aa.aa.aa>] |mac-statistics [address <aa.aa.aa.aa.aa.aa>] | all }]

802.1x Commands Descriptions

Command	Description
config terminal	Enters the Configuration mode
aaa authentication dot1x default	This command enables the dot1x local authentication or RADIUS server or TACACS PLUS server based remote authentication method for all ports. The actual authentication of the supplicant happens at the authentication server. The no form of the command disables dot1x in the switch. **radius** - Configures Radius as the authentication server. Radius offers Authentication, Authorization and Accounting management for computers to access a network. **tacacsplus** - Configures TACACS PLUS as the remote authentication server. Tacacs offers Authentication, Authorization and Accounting management for computers to access a network. This is mainly used for backward compatibility. **tacacs+** - Configures TACACS+ as the authentication server. This feature has been included to adhere to the Industry Standard CLI syntax. **local** - Configures Local authentication as the authentication mode. It provides authentication based on usernames and password using EAPMD5 authentication mechanism.
dot1x local-database	This command configures dot1x authentication server local database with user name and password. The no form of the command deletes an entry from the dot1x authentication server database. **<username>** - Configures the User name for the new entry in the database. **password<password>** - Configures the Password for the new entry in the database. **permission**- Configures the permission for access for the user on a set of ports. The options are: Allow- Provides access to the user Deny- Denies access to the user. **<auth-timeout(value(1-7200))>** - Configures the time in seconds after which the authentication allowed to the user expires. Maximum value is 7200 seconds. When the timeout value is 0, the authenticator uses the re-authentication period of the authenticator port. **<interface-type>** - Configures the interface type for the specified type of interface. Default : Permission – allow interface-list -all
dot1x system-auth-control	This command enables dot1x in the switch. The dot1x is an authentication mechanism. It acts as mediator between the authentication server and the supplicant (client). If the client accesses the protected resources, it contacts the authenticator with EAPOL frames. The no form of this command disables dot1x in the switch. Default – enabled
shutdown dot1x	This command shuts down dot1x feature. By shutting down the dot1x feature, the supplicant authenticator- authentication server architecture is dissolved. The data transport and authentication are directly governed by the authentication server/server. When shutdown, all resources acquired by dot1x module are released to the system. The no form of the command starts and enables dot1x Default – enabled
dot1x timeout	This command sets the dot1x timers. The timer module manages timers, creates memory pool for timers, creates timer list, starts and stops timer. It provides handlers to respective expired timers. Default – 60 seconds
Interface <type> <id>	

dot1x max-req	This command sets the maximum number of EAP (Extensible Authentication Protocol) retries to the client by the authenticator before restarting authentication process. The count value ranges between 1 and 10. The no form of the command sets the maximum number of EAP retries to the client to default value Default – 2
dot1x max-start	This command sets the maximum number of EAPOL retries to the authenticator. The no form of the command sets the maximum number of EAPOL retries to the authenticator to its default value. The value range is 1 to 65535. Default – 3
dot1x reauthentication	This command enables periodic re-authentication from authenticator to client. The periodic re-authentication is requested to ensure if the same supplicant is accessing the protected resources. The amount of time between periodic re-authentication attempts can be configured manually. Default – Periodic re-authentication is disabled
dot1x port-control	This command configures the authenticator port control parameter. The dot1x exercises port based authentication to increase the security of the network. The different modes employed to the ports offer varied access levels. The 802.1x protocol is supported on both Layer 2 static-access ports and Layer 3 routed ports The no form of the command sets the authenticator port control state to force authorized **auto** - Configures the 802.1x authentication process in this port. Causes the port to begin the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up or when an **EAPOL**-start frame is received. The switch requests the identity of the client and begins relaying authentication messages between the client and the authentication server. The switch can uniquely identify each client attempting to access the network by the client's MAC address. **force-authorized** - Configures the port to allow all the traffic through this port. Disables 802.1X authentication and causes the port to transit to the authorized state without requiring authentication exchange. The port transmits and receives normal traffic without 802.1X-based authentication of the client. **forceunauthorized**- Configures the port to block all the traffic through this port. Causes the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the interface.
Default – force-authorized	
dot1x auth-mode	This command configures the authentication mode of a port as either port-based (which is also known as multi-host) or mac-based (which is also known as single-host). Port based authentication has different modes of authentication. MAC based authentication allows secured mac addresses to pass through the port. Non secure mac addresses are dropped. The no form of the command configures the port authentication mode to its default values. **port-based** - Configures the port's authentication mode to Port-based. The port authenticates the host to use the restricted resource. The port state is changed to authorize. The traffic flows through the port without any access restriction till any event that causes the port state to become unauthorized. **mac-based** - Configures the port to MAC-based authentication. On receiving tagged/ untagged data/control frames from theCFA Module, it checks if the source MAC is present in the Authenticator Session Table and is authorized. If it is present in the table and is authorized, the result is passed to CFA, which then forwards the frame to the appropriate destination module. If it is present in the table but not authorized, the CFA Module is intimated and the frame is dropped at the CFA Module. If neither of the above occurs, the Authenticator will initiate a new authentication session for that source MAC address and return the unauthorized status to the CFA Module, which then drops the frame Default – port based

Examples

1. Port based authentication with RADIUS

```
configure terminal
dot1x system-auth-control
aaa authentication dot1x default group radius
radius-server host 172.18.212.142 timeout 20 retransmit 20 key 12345

interface fa 0/5
dot1x port-control auto
end
```

2. Port based authentication with local database

```
configure terminal
dot1x system-auth-control
dot1x local-database fsoft password admin123 permission allow
dot1x local-database fsoft1 password admin123 permission deny

interface fa 0/5
dot1x port-control auto
end
```

3. MAC based authentication with RADIUS

```
configure terminal
dot1x system-auth-control
aaa authentication dot1x default group radius
radius-server host 172.18.212.142 timeout 20 retransmit 20 key 12345

interface fa 0/5
dot1x port-control auto
dot1x auth-mode mac-based
end
```

4. MAC based authentication with local database

```
configure terminal
dot1x system-auth-control
dot1x local-database fsoftA password admin123 permission allow
dot1x local-database fsoftB password admin123 permission allow
dot1x local-database fsoftC password admin123 permission allow

interface fa 0/5
dot1x port-control auto
dot1x auth-mode mac-based
end
```

IGMP Snooping

Internet Group Multicast Protocol, (IGMP) is a protocol, which a host uses to inform a router when it joins (or leaves) an Internet multicast group. IGMP is only used on a local network; a router must use another multicast routing protocol to inform other routers of group membership. IGMP Snooping (IGS) is a feature that allows the switch to "listen in" on the IGMP conversation between hosts and routers. In IGS, a host computer uses IGMP to inform a router that it intends to listen to a specific multicast address. The multicast packet transfer happens only between the source and the destination computers. Broadcasting of packets is avoided. IGMP snooping significantly reduces traffic from streaming media and other bandwidth-intensive IP multicast applications.

IGS Commands Hierarchy

+ root

+ config terminal

- [no] shutdown snooping

- [no] ip igmp snooping [vlan <vlanid>]

- [no] ip igmp snooping clear counters [vlan <vlanid>]

- [no] ip igmp snooping group-query-interval <(2,2 - 5) seconds>

- [no] ip igmp snooping mrouter-time-out <(125,60 - 600) seconds>

- [no] ip igmp snooping port-purge-interval <(260,130 - 1225) seconds>

- [no] ip igmp snooping query-forward {all-ports | non-router-ports}

- [no] ip igmp snooping report-forward {all-ports | router-ports | non-edge-ports}

- [no] ip igmp snooping retry-count <1 - 5>

- [no] ip igmp snooping send-query { enable | disable }

- [no] ip igmp snooping vlan <vlanid (1-4094)> mrouter <ifXtype> <0/a-b, 0/c, ...>

- [no] ip igmp snooping vlan <vlanid(1-4094)> immediate-leave

    + [no] vlan <vlan id>

        -[no] ip igmp snooping

- ip igmp snooping fast-leave

- ip igmp snooping mrouter <interface-type> <0/a-b, 0/c, ...>

- ip igmp snooping mrouter-port <ifXtype> <iface_list> version {v1 | v2 | v3}

- ip igmp snooping static-group <mcast_addr> ports <ifXtype><iface_list>

- ip igmp snooping version {v1 | v2 | v3}

IGS Commands Descriptions

Command	Description
config terminal	Enters the Configuration mode
[no] shutdown snooping	Enable /disable snooping at the switch. default: enabled (no shut)
[no] ip igmp snooping [vlan<vlanid(1-4094)>]	This command creates IP ACLs and enters the IP Access-list configuration mode. Standard access lists create filters based on IP address and network mask only (L3 filters only). Depending on the standard or extended option chosen by the user, this command returns a corresponding IP Access list configuration mode. The no form of the command deletes the IP access-list. default: IGMP snooping is globally disabled, and in all VLANs
[no] ip igmp snooping clear counters [vlan <vlanid>]	This command clears the IGMP snooping statistics maintained for VLAN(s).
[no] ip igmp snooping group-query-interval	This command sets the time interval after which the switch sends a group specific query to find out if there are any interested receivers in the group when it receives a leave message. If it does not receive a response from the group, the port is removed from the group membership information in the forwarding database. default: 2 seconds
ip igmp snooping mrouter-time-out	This command sets the IGMP snooping router port purge time-out interval. Snooping learns the available router ports and initiates router port purge time-out timer for each learnt router port. The router sends control messages to the ports. If the router ports receive such control messages, the timer is restarted. If no message is received by the router ports before the timer expires, the router port entry is purged. The purge time-out value ranges between 60 and 600 seconds. default: 125 seconds
ip igmp snooping port-purge-interval	This command configures the IGMP snooping port purge time interval. When the port receives reports from hosts, the timer is initiated. If the port receives another report before the timer expires, the timer is restarted. If the port does not receive any report from hosts till the timer expires, then the port entry is purged from the multicast database. The purge time interval value ranges between 130 and 1225 seconds. default: 260 seconds
ip igmp snooping query-forward	This command configures the IGMP queries to be forwarded to all VLAN member ports or only to non-router ports. This configuration directs the queries to the selected ports to avoid flooding of the network. The queries are forwarded to multicast groups. If the VLAN module is enabled, IGMP snooping sends and receives the multicast packets through VLAN module. Defaults : non-router-ports
ip igmp snooping report-forward	This command configures the IGMP reports to be forwarded to all ports, router ports of a VLAN or non-edge ports. The configuration enables the switch to forward IGMP report messages to the selected ports thus avoiding flooding of the network. Defaults : router-ports
ip igmp snooping retry-count	This command sets the maximum number of group specific queries sent by the switch to check if there are any interested v2 receivers for the group when it receives a leave message in the proxy/ proxy-reporting mode. The port is deleted from the group membership information in the forwarding database if the maximum retry count exceeds set number. Defaults 2
ip igmp snooping send-query	This command configures the IGMP general query transmission feature upon the topology change in the switch
ip igmp snooping vlan <> mrouter	This command enables IGMP snooping and configures a list of multicast router ports for a specific VLAN, if IGMP snooping is globally enabled. This will enable IGMP snooping only for the specific VLAN, if IGMP snooping is globally disabled. Any IGMP message received on a switch is forwarded only on the router-ports and not on host ports. In this manner, the IGMP snooping functionality avoids flooding of IGMP query messages from the host to the entire network.

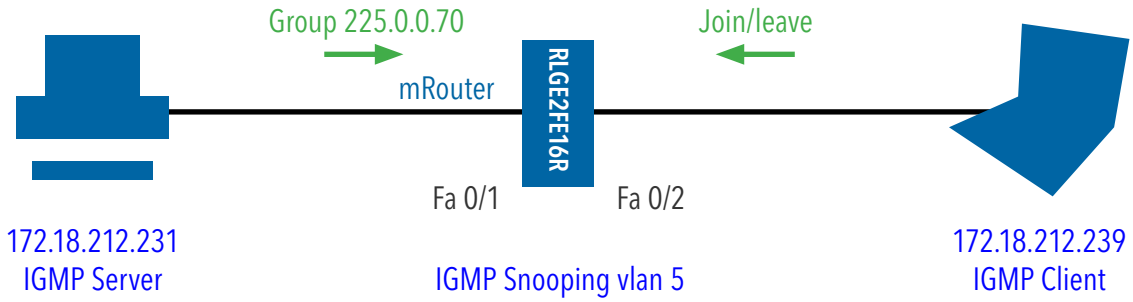
Command	Description
ip igmp snooping vlan<> immediate-leave	This command enables fast leave processing and IGMP snooping for a specific VLAN, It enables IGMP snooping only for the specific VLAN, when IGMP snooping is globally disabled. When the fast leave feature is enabled, port information is removed from a multicast group entry immediately after fast leave message is received. The ID of the VLAN ranges between 1 and 4094.
Vlan <id>	
[no] ip igmp snooping	This command enables IGMP snooping in the switch/ a specific VLAN. When snooping is enabled in a switch or interface, it learns the hosts intention to listen to a specific multicast address. When the switch receives any packet from the specified multicast address, it forwards the packet to the host listening for that address. Broadcasting is avoided to save bandwidth. When IGMP snooping is enabled globally, it is enabled in all the existing VLAN interfaces.
ip igmp snooping fast-leave	This command enables fast leave processing and IGMP snooping for a specific VLAN, It enables IGMP snooping only for the specific VLAN, when IGMP snooping is globally disabled. When the fast leave feature is enabled, port information is removed from a multicast group entry immediately after fast leave message is received.
ip igmp snooping mrouter	This command enables IGMP snooping and configures a list of multicast router ports for a specific VLAN, when IGMP snooping is globally enabled. This will enable IGMP snooping only for the specific VLAN, if IGMP snooping is globally disabled. Any IGMP message received on a switch is forwarded only on the router-ports and not on the host ports. In this manner, the IGMP snooping functionality avoids flooding of IGMP query messages from the host to the entire network.
ip igmp snooping mrouter-port	This command configures the router port purge time-out interval for a VLAN. The time interval after which the proxy assumes there are no v1/v2 routers present on the upstream port. While the older querier timer is running, the proxy replies to all the queries with consolidated v1/v2 reports. When the timer expires, if the v2/v3 queriers are not present and the port is dynamically learnt, the port is purged. If the port is static, router port, the proxy replies to all queries with new version of v2/v3 consolidated reports.
ip igmp snooping version	This command configures the operating version of the IGMP snooping switch for a specific VLAN. The version can be set manually to execute condition specific commands. Default : v3

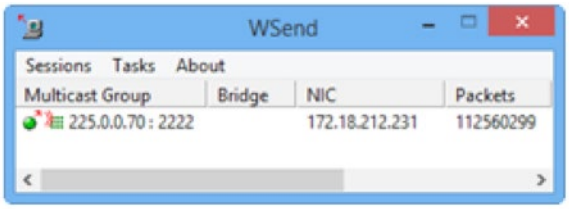
Example

The following setup is an example for IGMP setup and configuration.

The server sends multicast traffic with group 225.0.0.70 and port 2222.

The client and server ports are members of VLAN 5. IGMP snooping is enabled on both these ports. Port 0/1 is set as mrouter port.





Switch configuration

1. Create the service vlan

```
Config
Vlan 5
Port fastethernet 0/1,0/5 untagged fastethernet 0/1,0/5
Exit
Interface fastethernet 0/1
Switchport pvid 5
Exit
Interface fastethernet 0/5
Switchport pvid 5
Exit
```

2. Enable igmp snooping

```
ip igmp snooping
```

3. activate igmp snooping on vlan 5

```
ip igmp snooping vlan 5 mrouter fastethernet 0/1
vlan 5
ip igmp snooping mrouter fastethernet 0/1
end
write startup-cfg
```

Output result after client “join” request

```
RLGE2FE16R# show ip igmp snooping forwarding-database
 Vlan   MAC-Address           Ports
 ----   -----------------     -----
    5   01:00:5e:00:00:46     Fa0/1, Fa0/5
    5   01:00:5e:7f:ff:fa     Fa0/1, Fa0/5

 Total Group Mac entries = 2
```

Output result after client “leave” request

```
RLGE2FE16R# show ip igmp snooping forwarding-database

 Vlan   MAC-Address           Ports
 ----   -----------------     -----
    5   01:00:5e:7f:ff:fa     Fa0/1, Fa0/5

 Total Group Mac entries = 1
```

ACLs

ACLs (Access Control Lists) filter network traffic by controlling whether routed IP packets are forwarded or blocked at the router's interfaces. The router examines each packet to determine whether to forward or to drop it, based on the criteria specified within the access lists. Access list criteria can be the source address of the traffic, the destination address of the traffic, the upper-layer protocol or other information.

There are many reasons to configure ACLs - access lists can be used to restrict contents of routing updates or to provide traffic flow control. One of the most important reasons to implement ACLs is providing security for the network. ACLs must be used to provide a basic level of security for accessing the network. If no ACLs are configured at the router, all packets passing through the router are allowed onto all parts of the network. For example, access lists can allow one host to access a part of the network and prevent another host from accessing the same area.

ACL Flow validation at a port

Access lists are divided in to two main types: IP based and MAC based.

Each ACL contains the following information:

» Action: allow or deny.

» Priority (1-255). Applies to extended ACLs only.

» Rule: the condition for the packet to be validated with. Only one rule can be defined per ACL.

» Sub action: optional for additional traffic manipulation.

At the port level, the ACL assignment is referred to as ACG (Access Group). The ACGs are also separated to IP and MAC, relating to the matching ACL types.

A packet arriving at incoming direction to a port will be evaluated using the steps below:

1. IP based ACG entries

    a. The order of execution between multiple ACGs is derived from the ACL priority set at each individual ACL

    b. Only the priority value determines the order of execution at the port, not the ACL number neither its name.

    c. At any and all ports to which IP ACGs are assigned, the operating system automatically creates the last rule of "permit ip any any". This rule allows all other IP traffic which was not addressed by user ACLs to enter the port.

    d. IP ICMP ACLs are subset of IP ACLs and follow the same priority based flow of execution between them.

2. MAC based ACG entries

    a. The order of execution between multiple ACGs is derived from the ACL priority set at each individual ACL

    b. The ACL number or its name, does not determine of affect the order of execution at the port.

    c. At any and all ports at which MAC ACGs are assigned, the operating system automatically creates the last rule of "permit mac any any". This rule allows all other MAC and Ether-Type traffic which was not addressed by user ACLs to enter the port.

To add a rule of blocking all traffic which is not explicitly permitted, use a MAC based ACL of "deny any any".

When implementing MAC based ACLs, consider permitting ARP traffic explicitly as dropping this traffic entirely may result in unintentional connections failure.

NOTE: The way to control the order of execution of ACGs at a port is to define a priority for each ACL.

The lower the priority value is (1-255), the earlier its execution will be (priority 1 will be executed before priority 255).

NOTE: IP ACGs are executed first at a port, then MAC ACGs.

NOTE: ACLs of IN direction only are supported.

NOTE: IP ACLs of 'standard' type are not supported in current version.

ACL Commands Hierarchy

+ config terminal

+[no] ip access-list standard {<string(20)>}|[description <string(64)>]}

- permit {any|host <src-ip-address>|<src-ip-address><mask>}[{any|host <dest-ip-address>|<dest-ip-address><mask>}] {priority <1-255>}[redirect {interface ifXtype <ifnum>}][sub-action {modify-vlan <short (1-4094)>}]

- deny {any | host <src-ip-address> | <src-ip-address> <mask> } [{any |host <dest-ip-address> | <dest-ip-address> <mask>}] {priority <1-255>}

+[no] ip access-list extended {<string(20)> | [description < string(64)>]}

- {permit| deny} {ip | ospf | <protocol-type (1-255)>} { any | host <src-ip-address> | <src-ip-address> <mask>} {any | host <dest-ip-address> | <dest-ip-address> <mask>} {priority <1-255>}

- {permit| deny} icmp {any |host <src-ip-address>|<src-ip-address> <mask>} {any | host <dest-ip-address> | <dest-ip-address> <mask>} [<message-type (0-255)>] [<message-code (0-255)>] {priority <value (1-255)>} [svlan-id <vlan-id (1-4094)>] [svlan-priority <value (0-7)>] [cvlan-id <vlan-id (1-4094)>] [cvlan-priority <value (0-7)>] [{single-tag | double-tag}] [redirect {interface <ifXtype> <ifnum>}] [sub-action {modify-vlan <short (1-4094)>}]

- {permit| deny} tcp {any | host <src-ip-address> | <src-ip-address> <src-mask>} [{gt <port-number(1-65535)> | lt <port-number(1-65535)> |eq <port-number(1-65535)> | range <port-number(1-65535)><port-number(1-65535)>}] {any | host <dest-ip-address> | <dest-ip-address> <dest-mask> } [{gt <port-number (1-65535)> | lt <port-number(1-65535)> | eq <port-number(1-65535)> | range <port-number(1-65535)><port-number(1-65535)>}][{ack|rst}] [{tos{max-reliability|max-throughput|min-delay|normal|<tos-value(0-7)>} | dscp <value (0-63)>}] {priority <short (1-255)>}[svlan-id <vlan-id (1-4094)>] [svlan-priority <value (0-7)>] [cvlan-id <vlan-id (1-4094)>] [cvlan-priority <value (0-7)>] [{single-tag | double-tag}] [redirect {interface <ifXtype> <ifnum>}] [sub-action {modify-vlan <short (1-4094)>}]

- {permit | deny} udp {any | host <src-ip-address> | <src-ip-address> <src-mask>} [{gt <port-number(1-65535)> | lt <port-number(1-65535)> | eq <port number(1-65535))> | range <port-number (1-65535)><port-number (1-65535)>}] {any | host <dest-ip-address> | <dest-ip-address> <dest-mask> } [{ gt <port-number (1-65535)> | lt <port-number (1-65535)> | eq <port-number(1-65535)> | range <port-number(1-65535)> <port-number(1-65535)>}] [{tos{max-reliability|max-throughput|min-delay|normal|<tos-value(0-7)>} | dscp <value (0-63)>}] {priority <1-255>} [svlan-id <vlan-id (1-4094)>] [svlan-priority <value (0-7)>] [cvlan-id <vlan-id (1-4094)>] [cvlan-priority <value (0-7)>] [{ single-tag | double-tag }] [redirect {interface <ifXtype> <ifnum>}] [sub-action {modify-vlan(1-4094)}]

+[no] mac access-list extended {<string (20)> | [description <string(64)>]}

- {permit | deny}{any | host <src-mac-address>}{any | host <dest-mac-address>} [{ aarp | amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 | etype-8042 | lat | lavc-sca | mop-console | mop-dump | msdos | mumps | netbios | vines-echo | vines-ip | xns-

id | <short (0-65535)>}] [encaptype(1-65535)] [vlan <vlan-id (1-4094)>] {priority <1-255>} [outerEtherType(1-65535)] [svlan-id <vlan-id (1-4094)>] [cvlan-priority <value (0-7)>] [svlan-priority <value (0-7)>] [{single-tag | double-tag}] [redirect {interface <ifXtype> <ifnum>}] [sub-action {modify-vlan (1-4094)}]

+ interface <port type> <port ID>

- [no] ip access-group <string (20)> in

- [no] mac access-group <string (20)> in

- show access-lists [[{ip | mac | user-defined }] < access-list-number (1-65535)>]

- show running-config acl

ACL Commands Descriptions

Command	Description
config terminal	Enters the Configuration mode
[no] ip access-list standard	This command creates IP ACLs and enters the IP Access-list configuration mode. Standard access lists create filters based on IP address and network mask only (L3 filters only). Depending on the standard or extended option chosen by the user, this command returns a corresponding IP Access list configuration mode. The no form of the command deletes the IP access-list. The ACL identifier is a name of up to 20 characters. **Description**: Optional parameter, specifies a description of the ACL, up to 64 characters long.
permit	The standard permit command specifies the packets to be forwarded depending upon the associated parameters. Standard IP access lists use source addresses for matching operations. **any | host <src-ip-address> | <src-ip-address><mask>**: Source IP address can be: 'any', or the word 'host' followed by a dotted decimal IP address, or the network IP address and the network mask to use with the source IP address. **any | host <dest-ip-address> | <dest-ip-address><mask>**: Destination IP address can be: 'any', or the word 'host' followed by a dotted decimal IP address, or the network IP address and the network mask to use with the destination IP address. **Redirect**: Redirects the action to the destination interface or set of interfaces: **ifXtype** – Specifies the interface type, **ifnum** – Specifies the interface number. **sub-action**: Specifies the VLAN specific sub action to be performed on the packet: none – Actions relating to the VLAN ID will not be considered, **modify-vlan** – Modifies the VLAN ID to which the packet gets classified. The packet could be an untagged or VLAN tagged packet. nested-vlan – Adds an outer VLAN tag to the packet with the VLAN ID as configured. **priority**: lower value implies a higher priority. Default -1. Although this is a required paremeter it is disregarded in standard ACL (auto priority 0).
deny	This command denies traffic if the conditions defined in the deny statement are matched. **any | host <src-ip-address> | <src-ip-address><mask>**: Source IP address can be: 'any', or the word 'host' followed by a dotted decimal IP address, or the network IP address and the network mask to use with the source IP address. **any | host dest-ip-address | <network-destip><mask>**: Destination IP address can be: 'any', or the word 'host' followed by a dotted decimal IP address, or the network IP address and the network mask to use with the destination IP address. **priority**: lower value implies a higher priority. Default -1. Although this is a required paremeter it is disregarded in standard ACL (auto priority 0).

Command	Description
[no] ip access-list extended	Extended access lists enables specification of filters based on the type of protocol, range of TCP/UDP ports as well as the IP address and network mask (Layer 4 filters), and additional parameters as specified below. The no form of the command deletes the IP access-list. The ACL identifier is a name of up to 20 characters. **Description**: Optional parameter, specifies a description of the ACL, up to 64 characters long.
permit| deny	This command forwards (or drops for deny) all protocol specific traffic between specified source and destination. The protocol can be specified as ip, ospf or any number between 1 and 255 **any | host <src-ip-address> | host <src-ip-address><mask>**: Source IP address can be: 'any', or the word 'host' followed by a dotted decimal IP address, or the network IP address and the network mask to use with the source IP address. **any | host <dest-ip-address> | host <dest-ip-address><mask>**: Destination IP address can be: 'any', or the word 'host' followed by a dotted decimal IP address, or the network IP address and the network mask to use with the destination IP address. **priority**: 0 to 255.Lower value implies a higher priority. Default -1.
permit icmp, deny icmp	This command specifies the ICMP packets to be forwarded (or dropped for deny command) based on the IP address and the associated parameters. **any | host <src-ip-address> | host <src-ip-address><mask>**: Source IP address can be: 'any', or the word 'host' followed by a dotted decimal IP address, or the network IP address and the network mask to use with the source IP address. **any | host <dest-ip-address> | host <dest-ip-address><mask>**: Destination IP address can be: 'any', or the word 'host' followed by a dotted decimal IP address, or the network IP address and the network mask to use with the destination IP address. **message-type**: ICMP Message type **message-code**: ICMP Message code **priority**: 0 to 255.Lower value implies a higher priority. Default -1. **svlan-id** <vlan-id (1-4094)> - allows or denies packets with the specified server VLAN ID **svlan-priority** <value (0-7)>: allow/deny packets for outer VLAN with specified priority. **cvlan-id** <vlan-id (1-4094)> allows or denies packets with the specified client (nested) VLAN ID **cvlan-priority** <value (0-7)>: allow/deny packets for inner VLAN with specified priority. single-tag | double-tag: allows/denies single tagged or double tagged packets **Redirect**: Redirects the action to the destination interface. ifXtype – Specifies the interface type. ifnum – Specifies the interface number. **sub-action**: Specifies the VLAN specific sub action to be performed on the packet: none – Actions relating to the VLAN ID will not be considered. **modify-vlan** – Modifies the VLAN ID to which the packet gets classified. The packet could be an untagged or VLAN tagged packet.

Command	Description
permit tcp, deny tcp	This command specifies the TCP packets to be forwarded (or dropped for the deny command) based on the associated parameters. **any | host <src-ip-address> | host <src-ip-address> <src-mask>**: Source IP address can be: 'any', or the word 'host' followed by a dotted decimal IP address, or the network IP address and the network mask to use with the source IP address. **port-number**: Port Number. The input for the source and the destination port-number is prefixed with one of the following operators. **eq**=equal **lt**=less than **gt**=greater than **range**=a range of ports; two different port numbers must be specified **any | host<dest-ip-address> | <dest-ip-address><dest-mask>**: Destination IP address can be: 'any', or the word 'host' followed by a dotted decimal IP address, or the network IP address and the network mask to use with the destination IP address. **ack**: TCP ACK bit to be checked against the packet. It can be establish (1), non-establish (2) or any (3). Default value is 'any' (3) (indicates that the TCP ACK bit will not be checked to decide the action) **Rst**: TCP RST bit to be checked against the packet. It can be set (1), notset (2) or any (3).Default value is 'any' (3) (indicates that the TCP RST bit will not be checked to decide the action) **Tos**: Type of service. Can be max-reliability, max throughput, min-delay, normal or a range of values from 0 to 7. Default value is 0. **Dscp**: Differentiated services code point provides the quality of service control. The various options available are: 0-63 - Differentiated services code point value. The parameters newly added in the existing commands for industry standard CLI are: af11 - Matches packets with AF11 DSCP (001010) af12 - Matches packets with AF12 DSCP (001100) af13 - Matches packets with AF13 DSCP (001110) af21 - Matches packets with AF21 DSCP (010010) af22 - Matches packets with AF22 DSCP (010100) af23 - Matches packets with AF23 DSCP (010110) af31 - Matches packets with AF31 DSCP (011010) af32 - Matches packets with AF32 DSCP (011100) af33 - Matches packets with AF33 DSCP (011110) af41 - Matches packets with AF41 DSCP (100010) af42 - Matches packets with AF42 DSCP (100100) af43 - Matches packets with AF43 DSCP (100110) cs1 - Matches packets with CS1 (precedence 1) DSCP (001000) cs2 - Matches packets with CS2 (precedence 2) DSCP (010000) cs3 - Matches packets with CS3 (precedence 3) DSCP (011000) cs4 - Matches packets with CS4 (precedence 4) DSCP (100000) cs5 - Matches packets with CS5 (precedence 5) DSCP (101000) cs6 - Matches packets with CS6 (precedence 6) DSCP (110000) cs7 - Matches packets with CS7 (precedence 7) DSCP (111000) default - Default DSCP (000000) ef - Matches packets with EF DSCP (101110) **priority**: 0 to 255. Lower value implies a higher priority. Default -1 **svlan-id** <vlan-id (1-4094)> - allows or denies packets with the specified server VLAN ID **svlan-priority** <value (0-7)>: allow/deny packets for outer VLAN with specified priority. **cvlan-id** <vlan-id (1-4094)> allows or denies packets with the specified client (nested) VLAN ID **cvlan-priority** <value (0-7)>: allow/deny packets for inner VLAN with specified priority. **single-tag | double-tag**: allows/denies single tagged or double tagged packets Redirect: Redirects the action to the destination interface. ifXtype – Specifies the interface type. ifnum – Specifies the interface number. **sub-action**: Specifies the VLAN specific sub action to be performed on the packet: none – Actions relating to the VLAN ID will not be considered. **modify-vlan** – Modifies the VLAN ID to which the packet gets classified. The packet could be an untagged or VLAN tagged packet.

Command	Description
permit udp, deny udp	This command specifies the UDP datagrams to be forwarded (or blocked for the deny command) based on the associated parameters. **any | host <src-ip-address> | host <src-ip-address><mask>**: see permit | deny tcp command. **port-number**: see permit | deny tcp command. **any | host<dest-ip-address> | <dest-ip-address><dest-mask>**: see permit | deny tcp command. **Tos**: see permit | deny tcp command. **Dscp**: see permit | deny tcp command. **priority**: see permit | deny tcp command. **svlan-id**: see permit | deny tcp command. **svlan-priority**: see permit | deny tcp command. **cvlan-id**: see permit | deny tcp command. **cvlan-priority**: see permit | deny tcp command. **single-tag | double-tag**: see permit | deny tcp command. **Redirect**: see permit | deny tcp command. **sub-action**: see permit | deny tcp command.
[no] mac access-list extended	Creates Layer 2 MAC ACL and returns the MAC-Access list configuration mode to the user. The no form of the command deletes the MAC access-list. The ACL identifier is a name of up to 20 characters. **Description**: Optional parameter, specifies a description of the ACL, up to 64 characters long.
Permit | deny	Main action to be set as permit or deny. **any | host <src-mac-address>** : Source MAC address to be matched with the packet or 'any'. **any | host <dest-mac-address>** : Destination MAC address to be matched with the packet. **Redirect**: Redirects the action to the destination interface. **ifXtype** – Specifies the interface type. **ifnum** – Specifies the interface number. **sub-action** - Specifies the VLAN specific sub action to be performed on the packet; none or **modify-vlan** : Modifies the VLAN ID to which the packet gets classified. The packet could be an untagged or VLAN tagged packet. **aarp | amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 | etype-8042 | lat | lavc-sca | mop-console | mop-dump | msdos | mumps | netbios | vines-echo | vines-ip | xns-id | <short (0-65535)>:** **encaptype(1-65535):** **vlan <vlan-id (1-4094)>**: optional. **priority <1-255>** : 0 to 255.Lower value implies a higher priority. **outerEtherType(1-65535)** : Optional. **svlan-id** <vlan-id (1-4094)> - allows or denies packets with the specified server VLAN ID **svlan-priority** <value (0-7)>: allow/deny packets for outer VLAN with specified priority. **cvlan-id** <vlan-id (1-4094)> allows or denies packets with the specified client (nested) VLAN ID **cvlan-priority** <value (0-7)>: allow/deny packets for inner VLAN with specified priority. **single-tag | double-tag**: allows/denies single tagged or double tagged packets
interface <port type> <port ID>	Entering to the relevant interface to be configured
[no] ip access-group <access-list-number (1-65535)> {in | out}	This command enables access control for the packets on the interface. It controls access to a Layer 2 or Layer 3 interface. The no form of this command removes all access groups or the specified access group from the interface. The direction of filtering is specified using the token in or out. **access-list-number**: IP access control list number **in**: Inbound packets **out**: Outbound packets
-[no] mac access-group <access-list-number (1-65535)> in	This command applies a MAC access control list (ACL) to a Layer 2 interface. The no form of this command can be used to remove the MAC ACLs from the interface. **access-list-number**: Access List Number **in**: Inbound packets **out**: Outbound packets
show access-lists [[{ip | mac | user-defined}] <access-list-number(1-65535)>]	This command displays the access lists configuration. ip: IP Access List mac: MAC Access List user-defined: user defined access list

Configuration Examples

```
RLGE2FE16R# config terminal
```

Example for IP ACL, allow specific IP traffic:

```
RLGE2FE16R(config)# ip access-list extended 1001
RLGE2FE16R(config-1001)# permit ip any 172.18.212.0 255.255.255.0 priority 10
RLGE2FE16R(config-1001)# exit
RLGE2FE16R(config)# int fa 0/3
RLGE2FE16R(config-if)# ip access-group 1001 in
RLGE2FE16R(config-if)# end
```

Example for IP ACL, allow specific IP traffic:

```
RLGE2FE16R(config)# ip access-list extended 1001
RLGE2FE16R(config-1001)# permit ip host 10.10.10.10 host 11.11.11.11 priority 15
RLGE2FE16R(config-1001)# exit
RLGE2FE16R(config)# int fa 0/3
RLGE2FE16R(config-if)# ip access-group 1001 in
RLGE2FE16R(config-if)# end
```

Example for IP ACL, deny all IP traffic:

```
RLGE2FE16R(config)# ip access-list extended 1002
RLGE2FE16R(config-1002)# deny ip  any any priority 100
RLGE2FE16R(config-1002)# exit
RLGE2FE16R(config)# int fa 0/2
RLGE2FE16R(config-if)# ip access-group 1002 in
RLGE2FE16R(config-if)# end
```

Example how to allow ICMP ACL:

```
RLGE2FE16R(config)# ip access-list extended 1001
RLGE2FE16R(config-1001)# permit icmp any any priority 10
RLGE2FE16R(config-1001)# exit
RLGE2FE16R(config)# int fa 0/1
RLGE2FE16R(config-if)# ip access-group 1001 in
RLGE2FE16R(config-if)# end
```

Example for MAC ACL:

```
RLGE2FE16R(config)# mac access-list extended 1
RLGE2FE16R(config-1)#permit host 00:11:11:11:22:33 host 00:11:11:11:22:44 priority 10
RLGE2FE16R(config-1)# exit
RLGE2FE16R(config)# interface fastethernet 0/3
RLGE2FE16R(config-if)# mac access-group 1 in
RLGE2FE16R(config-if)# end
```

Example for MAC ACL:

```
RLGE2FE16R(config)# mac access-list extended 1
RLGE2FE16R(config-1)# permit any any priority 20
RLGE2FE16R(config-1)# exit
RLGE2FE16R(config)# interface fastethernet 0/3
RLGE2FE16R(config-if)# mac access-group 1 in
RLGE2FE16R(config-if)# end
```

Example how to deny MAC Traffic ACL:

```
RLGE2FE16R# config terminal
RLGE2FE16R(config)# mac access-list extended 25
RLGE2FE16R(config-ext-macl)# deny any any priority 250
RLGE2FE16R(config-ext-macl)# exit
RLGE2FE16R(config)# interface fastethernet 0/3
RLGE2FE16R(config-if)# mac access-group 25 in
RLGE2FE16R(config-if)# end
```

Example TCP ACL:

```
RLGE2FE16R# config terminal
RLGE2FE16R(config)# ip access-list extended tcp-502
RLGE2FE16R(config-tcp-502)# permit tcp any eq 502 any range 100 200 priority 10
RLGE2FE16R(config-tcp-502)# exit
RLGE2FE16R(config)# interface fastethernet 0/3
RLGE2FE16R(config-if)# ip  access-group tcp-502 in
RLGE2FE16R(config-if)# end
```

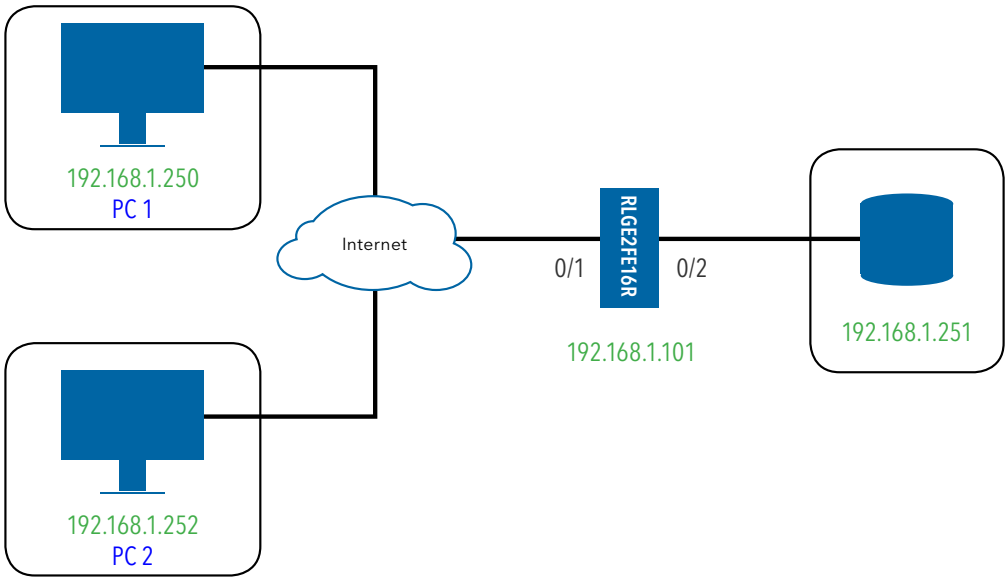
Example Redirect ACL:

```
RLGE2FE16R# config terminal
RLGE2FE16R(config)# ip access-list extended redirect _ example
RLGE2FE16R(config-redirect _ example)# permit ip host 1.1.1.1 host 2.2.2.2 priority 15
redirect interface fastethernet 0/4
RLGE2FE16R(config-redirect _ example)# exit
RLGE2FE16R(config)# interface fastethernet 0/3
RLGE2FE16R(config-if)# ip  access-group redirect _ example in
RLGE2FE16R(config-if)# end
```

Example how to allow ARP ACL:

```
RLGE2FE16R# config terminal
RLGE2FE16R(config)# mac access-list extended 1
RLGE2FE16R(config-1)# permit any any 0x0806 priority 5
RLGE2FE16R(config-1)# exit
RLGE2FE16R(config)# interface fa 0/3
RLGE2FE16R(config-if)# mac access-group 1 in
RLGE2FE16R(config-if)# end
```

Flow Example



For the above setup, ACLs will be implemented at port fast 0/1 and traffic result will be reviewed.

Test 1

```
RLGE2FE16R(config)#
ip  access-list extended 1010
permit  ip host 192.168.1.250 host 192.168.1.101  priority 20
!
ip  access-list extended 1020
deny  ip  any  host 192.168.1.101  priority 10
!
interface fastethernet 0/1
ip access-group 1010 in
!
interface fastethernet 0/1
ip access-group 1020 in
!
```

Results

PC1 SSH management to the switch: blocked.

PC1 ping to the switch: blocked.

PC1 ping to the server: allowed.

PC2 SSH management to the switch: blocked.

PC2 ping to the switch: blocked.

PC2 ping to the server: allowed.

Test 2

```
RLGE2FE16R(config)#
ip  access-list extended 1001
permit  icmp  any   any  priority 50
!
ip  access-list extended 1010
permit  ip host 192.168.1.250 host 192.168.1.101  priority 10
!
ip  access-list extended 1020
deny  ip  any  host 192.168.1.101  priority 20
!
interface fastethernet 0/1
ip access-group 1001 in
!
interface fastethernet 0/1
ip access-group 1010 in
!
interface fastethernet 0/1
ip access-group 1020 in
!
```

Results

PC1 SSH management to the switch: allowed.

PC1 ping to the switch: allowed.

PC1 ping to the server: allowed.

PC2 SSH management to the switch: blocked.

PC2 ping to the switch: blocked.

PC2 ping to the server: allowed.

Test 3

```
RLGE2FE16R(config)#
ip  access-list extended 1001
permit  icmp  any   any  priority 5
!
ip  access-list extended 1010
permit  ip host 192.168.1.250 host 192.168.1.101  priority 30
!
ip  access-list extended 1020
deny  ip  any  host 192.168.1.101  priority 40
!
interface fastethernet 0/1
ip access-group 1001 in
!
interface fastethernet 0/1
ip access-group 1010 in
!
interface fastethernet 0/1
ip access-group 1020 in
!
```

Results

PC1 SSH management to the switch: allowed.

PC1 ping to the switch: allowed.

PC1 ping to the server: allowed.

PC2 SSH management to the switch: blocked.

PC2 ping to the switch: allowed.

PC2 ping to the server: allowed.

Test 4

```
RLGE2FE16R(config)#
ip  access-list extended 1001
permit  icmp  any   any  priority 5
!
ip  access-list extended 1010
permit  ip host 192.168.1.250 host 192.168.1.101  priority 100
!
mac access-list extended 10
permit  any any 2054  priority 1
!
mac access-list extended 100
deny  any any priority 250
!
interface fastethernet 0/1
ip access-group 1001 in
!
interface fastethernet 0/1
ip access-group 1010 in
!
interface fastethernet 0/1
mac access-group 10 in
!
interface fastethernet 0/1
mac access-group 100 in
```

Results

PC1 SSH management to the switch: allowed.

PC1 ping to the switch: allowed.

PC1 ping to the server: blocked.

PC2 SSH management to the switch: blocked.

PC2 ping to the switch: blocked.

PC2 ping to the server: allowed.

Test 5

```
RLGE2FE16R(config)#
ip  access-list extended 1010
permit  ip host 192.168.1.250 host 192.168.1.101  priority 100
!
mac access-list extended 10
permit  any any 2054  priority 1
!
mac access-list extended 100
deny  any any priority 20
!
interface fastethernet 0/1
ip access-group 1010 in
!
interface fastethernet 0/1
mac access-group 10 in
!
interface fastethernet 0/1
mac access-group 100 in
```

Results

PC1 SSH management to the switch: allowed.

PC1 ping to the switch: allowed.

PC1 ping to the server: blocked.

PC2 SSH management to the switch: blocked.

PC2 ping to the switch: blocked.

PC2 ping to the server: blocked.

QOS

QoS (Quality of Service) defines the ability to provide different priorities to different applications, users or data flows or the ability to guarantee a certain level of performance to a data flow. QoS refers to resource reservation control mechanisms rather than the achieved service quality and specifies a guaranteed throughput level.

QOS Commands Hierarchy

+ config

- [no] shutdown qos

- qos {enable | disable}

- qos interface <iftype> <ifnum> def-user-priority <0-7>

- [no] priority-map <1-65535>

+ [no] class-map <1-65535>

- [no] set class <1-65535> [pre-color { green | yellow | red | none }] [regen-priority <0-7> group-name <string(31)>]

+ [no] meter <1-65535>

- meter-type { simpleTokenBucket | avgRate| srTCM | trTCM | tswTCM | mefCoupled| mefDeCoupled } [color-mode { aware | blind }] [interval <short(1-10000)>][cir <0-65535>] [cbs <0-65535>] [eir <0-65535>][ebs <0-65535>] [next-meter 0-65535>]

+ [no] policy-map <1-65535>

- set policy [class <0-65535>] [interface <iftype> <ifnum>] defaultpriority- type { none | { vlanPri | ipTos } <0-63)>}

- set meter <1-65535> [conform-action { none | set-cos-transmit <short(0-7> set-de-transmit <short(0-1> | set-port <iftype> <ifnum> | setinner- vlan-pri <short(0-7> | set-ip-prectransmit <short(0-7> | set-ip-dscp-transmit <short(0-63> }] [exceed-action {drop | set-cos-transmit <short(0-7> set-de-transmit <short(0-1> |setinner-vlan-pri <short(0-7> | set-ipprec- transmit <short(0-7> | set-ip-dscp-transmit <short(0-63> }] [violateaction {drop | set-cos-transmit <short(0-7> set-de-transmit <short(0-1> | set-inner-vlan-pri <short(0-7> |set-ipprec-transmit <short(0-7> | set-ip-dscp-transmit <short(0-63> }] setconform- newclass <0-65535>] [set-exceed-newclass <0-65535>]
[set-violate-newclass <0-65535>]

- [no] queue-type <1-65535>

- set algo-type { tailDrop | headDrop | red | wred } [queue-limit <1-65535>] [queue-drop-algo {enable | disable }]

- [no] shape-template <1-65535> [cir <1-65535>] [cbs <0-65535)>]
  [eir <0-65535>] [ebs <0-65535>]
- [no] scheduler <1-65535> interface <iftype> <ifnum> [sched-algo
  {strictpriority| rr | wrr | wfq | strict-rr | strict-wrr | strict-wfq
  | deficit-rr}][shaper <0-65535>] [hierarchy-level <0-10>]
- [no] scheduler <1-65535> interface <iftype> <ifnum>
  [sched-algo {strictpriority| rr | wrr | wfq | strict-rr | strict-wrr
  | strict-wfq | deficit-rr}][shaper <0-65535>]
  [hierarchy-level < 0-10>]
- [no] queue < 1-65535> interface <iftype> <ifnum>
  [qtype < 1-65535>][scheduler < 1-65535>] [weight <0-1000>]
  [priority <0-15>] [shaper <0-65535>]
- [no] queue-map { CLASS <1-65535> | regn-priority {vlanPri | ipTos} <0-63>}
  [interface <iftype> <ifnum>] queue-id <1-65535>
- [no] sched-hierarchy interface <iftype> <ifnum> hierarchy-level <1-10>
  sched-id <1-65535> {next-level-queue <0-65535> | next levelscheduler
  <0-65535>} [priority <0-15>] [weight <0-1000>]
+ [no] map [interface <iftype> <ifnum>] [vlan <1-4094>] in-priority-type
  { vlanPri | ipTos } [in-priority <0-63>]regen-priority <0-63>
  [regen-inner-priority <0-7>]

+ match access-group { [mac-access-list <0-65535>] [ip-access-list <0-65535>] | priority-map <0-65535> }

- show qos global info
- show priority-map [<priority-map-id(1-65535)>]
- show class-map [<class-map-id(1-65535)>]
- show class-to-priority-map <group-name(31)>
- show meter [<meter-id(1-65535)>]
- show policy-map [<meter-id(1-65535)>]

- show queue-template [<queue-template-Id(1-65535)>]
- show shape-template [<shape-template-Id(1-65535)>]
- show scheduler [interface <iftype> <ifnum>]
- show queue [interface <iftype> <ifnum>]
- show queue-map [interface <iftype> <ifnum>]
- show sched-hierarchy [interface <iftype> <ifnum>]
- show qos def-user-priority [interface <iftype> <ifnum>]
- show qos meter-stats [<Meter-Id(1-65535)>]
- show qos queue-stats [interface <iftype> <ifnum>]

QOS Commands Descriptions

Command	Description
config terminal	Enters the Configuration mode
shutdown qos	shuts down the QoS subsystem. The no form of the command starts the QoS subsystem
qos	{enable | disable} enables or disables the QoS subsystem.
priority-map	adds a Priority Map entry. The no form of the command deletes a Priority Map entry. **Priority-map-Id** : Priority map index for the incoming packet received over ingress Port/VLAN with specified incoming priority. This value ranges between 1 and 65535.
class-map	adds a Class Map entry. The no form of the command deletes a Class Map entry. **class-map-id** : Index that enumerates the MultiField Classifier table entries. This value ranges between 1 and 65535.
meter	This command creates a Meter. The no form of the command deletes a Meter. **meter-id** : Index that enumerates the Meter entries. This value ranges between 1 and 65535.
policy-map	creates a policy map. The no form of the command deletes a policy map. **policy-map-id** : Index that enumerates the policy-map table entries. This value ranges between 1 and 65535.
queue-type	creates a Queue Template Type. The no form of the command deletes a Queue Template Type. **Q-Template-Id** : Queue Template Table index. This value ranges between 1 and 65535
shape-template	creates a Shape Template. The no form of the command deletes a Shape Template **Shape-Template-Id** : Shape Template Table index. **cir** : Committed information rate for packets through the queue. **cbs** : Committed burst size for packets through the queue. **eir** : Excess information rate for packets through the hierarchy. **ebs** : Excess burst size for packets through the hierarchy

Command	Description
scheduler	creates a Scheduler and configures the Scheduler parameters. The no form of the command deletes a scheduler. **Scheduler-Id** : Scheduler identifier that uniquely identifies the scheduler in the system/egress interface **Iftype** : Interface type **Ifnum** : Interface number **sched-algo** : Packet scheduling algorithm for the port. The algorithms are: strict-priority – strictPriority. - rr – roundRobin. - wrr – weightedRoundRobin. - wfg – weightedFairQueing. - strict-rr – strictRoundRobin. -strict-wrr – strictWeightedRoundRobin. -strict-wfg – strictWeightedFairQueing. - deficit-rr – deficitRoundRobin **Shaper** : Shaper identifier that specifies the bandwidth requirements for the scheduler. hierarchy-level : Depth of the queue/scheduler hierarchy
queue	creates a Queue and configures the Queue parameters. The no form of the command deletes a Queue. **Queue** : Queue identifier that uniquely identifies the queue in the system/port. **Iftype** : Interface type **Ifnum** : Interface number **Qtype** : Queue Type identifier. **Scheduler** : Scheduler identifier that manages the specified queue. **Weight** : User assigned weight to the CoS queue **Priority** : User assigned priority for the CoS queue. **Shaper** : Shaper identifier that specifies the bandwidth requirements for the queue.
queue-map	creates a Map for a Queue with Class or regenerated priority. The no form of the command deletes a Queue map entry. **CLASS** : Input CLASS that needs to be mapped to an outbound queue. **regn-priority** : Regenerated-priority type and regenerated-priority that needs to be mapped to an outbound queue. The types are vlanPri – VLAN Priority. ipTos – IP Type of Service. **Iftype** : Interface type **Ifnum** : Interface number **queue-id** : Queue identifier that uniquely identifies a queue relative to an interface.
sched-hierarchy	This command creates a Scheduler Hierarchy. The no form of the command deletes a Scheduler Hierarchy **hierarchy-level** : Depth of the queue/scheduler hierarchy **sched-id** : Scheduler identifier. next-level-queue – Next-level queue to which the scheduler output needs to be sent. next-level-scheduler – Next-level scheduler to which the scheduler output needs to be sent.
qos interface	sets the default ingress user priority for the port. **def-user-priority** : Default ingress user priority for the port

Command	Description
map	This command adds a Priority Map Entry for mapping an incoming priority to a regenerated priority. The no form of the command sets default value to the Interface, VLAN, regenerated inner priority. **in-priority-type** : Type of the incoming priority. The types are: vlanPri – VLAN Priority. ipTos – IP Type of Service. ipDscp – IP Differentiated Services Code Point. **in-priority** : Incoming priority value determined for the received frame. This value ranges between 0 and 63. **regen-priority** : Regenerated priority value determined for the received frame. This value ranges between 0 and 63. **regen-innerpriority** : Regenerated inner-VLAN (CVLAN) priority value determined for the received frame. This value ranges between zero and seven. Defaults: Vlan – 0 in-priority-type – vlanPri in-priority - -1 regen-priority - 0
match access-group	This command sets Class Map parameters using L2and/or L3 ACL or Priority Map ID. **mac-access-list** : Identifier of the MAC filter. This value ranges between 0 and 65535. **ip-access-list** : Identifier of the IP filter. This value ranges between 0 and 65535. **priority-map** : Priority Map identifier for mapping incoming priority against received packet. This value ranges between 0 and 65535. Defaults: mac-access-list – 0 ip-access-list– 0 priority-map- -1
set class	This command sets CLASS for L2and/or L3 filters or Priority Map ID and adds a CLASS to Priority Map entry with regenerated priority. The no form of the command deletes a CLASS to Priority Map Table entry. **Class** : Traffic CLASS to which an incoming frame pattern is classified. **pre-color** : Color of the packet prior to metering. This can be any one of the following: None – Traffic is not pre-colored. green – Traffic conforms to SLAs (Service Level Agreements. yellow – Traffic exceeds the SLAs. red – Traffic violates the SLAs. **regen-priority** : Regenerated priority value determined for the input CLASS. This value ranges between zero and seven. **group-name** : Unique identification of the group to which an input CLASS belongs.
meter-type	This command sets Meter parameters CIR, CBS, EIR, EBS, Interval, meter type and color awareness. **simpleTokenBucket** - Two Parameter Token Bucket Meter **avgRate** - Average Rate Meter. **srTCM** - Single Rate Three Color Marker Metering as defined by RFC 2697. **trTCM** - Two Rate Three Color Marker Metering as defined by RFC 2698 tswTCM **color-mode** - Indicates the color mode of the Meter. The color modes are: * aware – The Meter considers the pre-color of the packet. * blind – The Meter ignores the pre-color of the packet. **interval** - Time interval used with the token bucket. This value ranges between 1 and 10000. **cir** - Committed information rate. This value ranges between 0 and 65535. **cbs** - Committed burst size. This value ranges between 0 and 65535. **eir** - Excess information rate. This value ranges between 0 and 65535. **ebs** - Excess burst size. This value ranges between 0 and 65535. **next-meter** - Meter entry identifier used for applying the second/next level of conformance on the incoming packet. This value ranges between 0 and 65535.

Command	Description
set policy	This command sets CLASS for policy. The no form of the command sets the default value for interface in this policy **default-prioritytype** : Per-Hop Behaviour (PHB) type to be used for filling the default PHB for the policy-map entry. The types are: none – No specific PHB type is set. vlanPri – VLAN priority. ipTos – IP Type of Service. ipDscp – IP Differentiated Services Code Point.
set meter	This command sets Policy parameters such as Meter and Meter Actions. The no form of the command removes the Meter from the Policy and the Meter Actions. **meter** - Meter table identifier which is the index for the Meter table. **conform-action** - Action to be performed on the packet, when the packets are found to be In profile (conform). Options are: none – No action is configured. set-cos-transmit – Sets the VLAN priority of the outgoing packet. set-de-transmit – Sets the VLAN Drop Eligible indicator of the outgoing packet. set-port – Sets the new port value. set-inner-vlan-pri – Sets the inner VLAN priority of the outgoing packet. set-ip-prec-transmit – Sets the new IP TOS value. set-ip-dscp-transmit – Sets the new DSCP value. **exceed-action** - Action to be performed on the packet, when the packets are found to be In profile (exceed). Options are: drop – Drops the packet. set-cos-transmit – Sets the VLAN priority of the outgoing packet. set-de-transmit – Sets the VLAN Drop Eligible indicator of the outgoing packet. set-inner-vlan-pri – Sets the inner VLAN priority of the outgoing packet. set-ip-prec-transmit – Sets the new IP TOS value. set-ip-dscp-transmit – Sets the new DSCP value. **violate-action** - Action to be performed on the packet, when the packets are found to be out of profile. Options are: drop – Drops the packet. set-cos-transmit – Sets the VLAN priority of the outgoing packet. set-de-transmit – Sets the VLAN Drop Eligible indicator of the outgoing packet. set-inner-vlan-pri – Sets the inner VLAN priority of the outgoing packet. set-ip-prec-transmit – Sets the new IP TOS value. set-ip-dscp-transmit – Sets the new DSCP value. **set-conformnewclass** - Represents the Traffic CLASS to which an incoming frame pattern is classified after metering. set-exceednewclass - Represents the Traffic CLASS to which an incoming frame pattern is classified after metering. set-violatenewclass - Represents the Traffic CLASS to which an incoming frame pattern is classified after metering.
set algo-type	This command sets Q Template entry parameters. **algo-type** - Type of drop algorithm used by the queue template.Options are: tailDrop – Beyond the maximum depth of the queue, all newly arriving packets will be dropped. headDrop – Packets currently at the head of the queue are dropped to make room for the new packet to be enqueued at the tail of the queue, when the current depth of the queue is at the maximum depth of the queue. red – On packet arrival, an Active Queue Management algorithm is executed which may randomly drop a packet. wred – On packet arrival, an Active Queue Management algorithm is executed which may randomly drop a packet. **queue-limit** - Queue size. This value ranges between 1 and 65535. **queue-drop-algo** - Enable/disable Drop Algorithm for Congestion Management. Options are: enable – Enables Drop Algorithm. disable – Disables Drop Algorithm.

Command	Description
random-detect dp	This command sets Random Detect Table entry parameters. The no form of the command deletes the entry. **dp** - Drop Precedence. Options are: 0 – low drop precedence. 1 – medium drop precedence. 2 – high drop precedence. **min-threshold** - Minimum average threshold for the random detect algorithm. Value ranges between 1 and 65535. **max-threshold** - Maximum average threshold for the random detect algorithm. Value ranges between 1 and 65535. **max-pkt-size** - Maximum allowed packet size. Value ranges between 1 and 65535. **mark-probabilitydenominator** : Maximum probability of discarding a packet in units of percentage. Value ranges between 1 and 100. **exponential-weight** - Exponential weight for determining the average queue size. This value ranges between 0 and 31.

Packet Queue Assignment

Each port has 8 transmit queues. A single packet can be assigned for transmission in one of those queues.

Addressing a data packet to a desired QOS port queue can be done using the following measures.

- Port based assignment of priority- all packets coming into the port will be assigned with a specific common priority.
- ACL mapping- ACLs at a port will determine the assigned queue for packets meeting the condition.
- VPT/DSCP- setting VPT or DSCP values to packets based on ACL conditions. The VPT/DSCP values are mapped to queues.

These measures will reflect on the internal Forwarding Class (FC) and will result in a queue assignment as per following table.

Forwarding Class	QOS queue	Priority
Be	1	lowest
l2	2	
af	3	
l1	4	
h2	5	
ef	6	
h1	7	
nc	8	highest

Port based assignment of priority

1. Following script will assign static priority to all ingress UNTAGGED traffic at ports 1 and 2. The ports are assigned the same pvid.

Packets origin from these ports will be egressed at the out port in accordance to their assigned priority.

```
Config
interface fastethernet 0/1
no shutdown
switchport pvid 100
switchport priority default 1
exit
interface fastethernet 0/2
no shutdown
switchport pvid 100
switchport priority default 2
exit
```

ACL Map to COS

The following will demonstrate how to map incoming packets to a desired queue.

1. Create a mac based access list and assign to the a port as in type

```
Config
mac access-list extended 10
permit any any
exit
interface fastethernet 0/1
mac access-group 10 in
exit
```

2. create a class map to assign a queue id to packets which comply with the acl. all packets ingress at port 0/1 will thus be assigned to queue 7

```
class-map 10
match access-group mac-access-list 10
set class 10
exit
queue-map class 10 queue-id 7
```

Set VPT or DSCP

Map VPT to COS

Addressing a packet to a desired queue can be done by its VLAN priority tag (VPT). The following table details the relation of VPT value to a queue assignment.

VPT	Fc	QOS queue	
0	Be	1	lowest
1	l2	2	
2	af	3	
3	l1	4	
4	h2	5	
5	ef	6	
6	h1	7	
7	nc	8	highest

Map DSCP to COS

Addressing a packet to a desired queue can be done by its DSCP value. The following table details the relation of DSCP value to a queue assignment.

DSCP	Fc	QOS queue	
0-7	Be	1	lowest
8-15	l2	2	
16-23	af	3	
24-31	l1	4	
32-39	h2	5	
40-47	ef	6	
48-55	h1	7	
56-63	nc	8	highest

The following will demonstrate how to set the vpt or dscp values using ACL rules. The values of the DSCP/VPT will determine the target queue for the packet.

1. Create ACLs

```
Config
ip access-list extended 1001
permit ip any 172.18.212.0 255.255.255.0
exit
ip access-list extended 1002
permit ip any any
exit
interface fastethernet 0/1
ip access-group 1001 in
ip access-group 1002 in
exit
```

2. Enable QOS

```
qos enable
```

3. Create policer for ACL 1001 to determine dscp to 5

```
class-map 20
match access-group ip-access-list 1001
set class 200
exit
policy-map 20
set policy class 200 default-priority-type  ipDscp 5
exit
```

4. Create policer for ACL 1002 to determine vpt to 2

```
class-map 30
match access-group ip-access-list 1002
set class 300
exit
policy-map 30
set policy class 300 default-priority-type  vlanPri 2
exit
write startup-cfg
RLGE2FE16R# show policy-map
```

```
QoS Policy Map Entries
----------------------
PolicyMapId  : 20
IfIndex      : 0
Class        : 200
DefaultPHB   : IP DSCP 5
MeterId      : 0
ConNClass    : 0
ExcNClass    : 0
VioNClass    : 0
ConfAct      : None.
ExcAct       : None.
VioAct       : None.
QoS Policy Map Entries
----------------------
PolicyMapId  : 30
IfIndex      : 0
Class        : 300
DefaultPHB   : VlanPri 2
MeterId      : 0
ConNClass    : 0
ExcNClass    : 0
VioNClass    : 0
ConfAct      : None.
ExcAct       : None.
VioAct       : None.
RLGE2FE16R# show class-map
QoS Class Map Entries
---------------------
ClassMapId                    : 20
L2FilterId                    : None
L3FilterId                    : 1001
PriorityMapId                 : None
CLASS                         : 200
PolicyMapId                   : 20
PreColor                      : None
Status                        : Active
QoS Class Map Entries
---------------------
ClassMapId                    : 30
```

```
L2FilterId                      : None
L3FilterId                      : 1002
PriorityMapId                   : None
CLASS                           : 300
PolicyMapId                     : 30
PreColor                        : None
Status                          : Active
```

Setting a Scheduling Algorithms

1. Following script will Configures scheduler-1 for the outgoing interface Fa 0/4 as wrr. The Qs with weights configured will be serviced with Weighted Round Robin

```
Config
scheduler 1 interface Fa 0/4   sched-algo wrr
queue 1 interface Fa 0/4 weight 1
queue 2 interface Fa 0/4 weight 2
queue 3 interface Fa 0/4 weight 4
queue 4 interface Fa 0/4 weight 4
queue 5 interface Fa 0/4 weight 4
queue 6 interface Fa 0/4 weight 8
queue 7 interface Fa 0/4 weight 8
queue 8 interface Fa 0/4 weight 16
```

2. Following script will configure scheduler-1 for the outgoing interface Fa 0/4 as strict. The Q with weight 0 will be serviced with strict priority. The Qs with weights configured will be serviced with Weighted Round Robin.

```
Config
scheduler 1 interface Fa 0/4   sched-algo strict-wrr
queue 1 interface fastethernet 0/4 weight 0
queue 2 interface fastethernet 0/4 weight 2
queue 3 interface fastethernet 0/4 weight 2
queue 4 interface fastethernet 0/4 weight 2
queue 5 interface fastethernet 0/4 weight 4
queue 6 interface fastethernet 0/4 weight 4
queue 7 interface fastethernet 0/4 weight 4
queue 8 interface fastethernet 0/4 weight 4
```

Traffic Filtering at Ingress

In this example, ICMP packets from 12.0.0.100 are filtered at ingress to port 0/1.

```
RLGE2FE16R# configure terminal
RLGE2FE16R(config)# ip access-list extended 1001
RLGE2FE16R(config-ext-nacl)# deny icmp host 12.0.0.100 any
RLGE2FE16R(config-ext-nacl)# exit
RLGE2FE16R(config)# interface gigabitethernet 0/1
RLGE2FE16R(config-if)# ip access-group 1001 in
RLGE2FE16R# show access-lists
```

Setting a Shaper per Egress Port

The following script will configure a “rate-limiter” shaper CIR/CBS based per output port.

rate-limit output [CIR (Kbps)] [CBS(Kbytes)]

```
Config
interface Fa 0/4

rate-limit output 2000 15000
```

Link Aggregation

Link Aggregation allows aggregation of point-to-point links operating at the same data rate. Link Aggregation is supported only on point-to-point links with MAC clients operating in full duplex mode.

A MAC client communicates with a set of ports through an Aggregator, which presents a standard IEEE 802.3 service interface to the MAC client. The Aggregator binds to one or more ports within a system.

LACP (Link Aggregation Control Protocol) is used for automatic communication of aggregation capabilities and automatic configuration of Link Aggregation between systems.

The list of ports that are aggregated to a particular aggregator is transparent to the higher modules (such as Spanning Tree).

Few of the salient features of Link Aggregation are as follows:

» Load sharing
» Increased availability
» Increased bandwidth
» Linear incremental bandwidth
» Low risk of duplication or mis-ordering

Upon Link Aggregation, individual point-to-point ports/interfaces are aggregated into a group that is regarded as a single port/interface by the higher layers such as Spanning-tree. The total capacity of such an aggregated group is the sum of the capacities of the individual links composing the aggregate, thus providing higher bandwidth to the MAC client (such as Spanning Tree). As shown in Figure 2-1 multiple ports are aggregated together to form a single link.

ComNet LA is responsible for taking frames from the aggregator and submitting them for transmission on the appropriate port. The physical port for transmission is chosen based on the selection policy in the chipset. LA is responsible for collecting the frames received on various ports of the aggregator.

The user can configure a specific distribution policy for the traffic flow based on the deployment scenario. This allows the switches to get the advantage of increased bandwidth for the traffic between the hosts and the server. Also, if one of the links in the aggregation group is made down, say, for maintenance purpose, and then it will not affect the traffic between the hosts and the server.

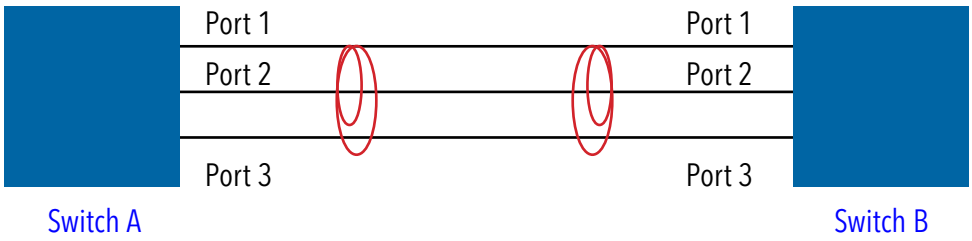


Figure 2-1: Link Aggregation - Example

The guidelines for the configuration of LA are as follows:

» Port-channel must be enabled in the system for Link aggregation configuration to take effect.

» If 802.1x is enabled on a port, then Link Aggregation can be enabled on that port only when the port is in the authorized state. Link Aggregation cannot be enabled on unauthorized ports.

NOTE: Up to eight interfaces of the same type and speed can be configured for the same group.

The Default Configurations of LA are as follows:

Feature	Default Setting
Port-channel	Disabled
Channel-groups	None
LACP System Priority	0x8000 or 32768
Load balancing	Source and Destination MAC address based
LACP Port Priority	128 on all interfaces
LACP Wait time	2
LACP timeout	Long: The long timeout value means that LACP PDU will be sent every 30 seconds and LACP timeout value (no packet is received from peer) is 90 seconds
MAC-selection	Dynamic: Port-channel MAC address is address of an active port

Configure the physical port in a port channel and specify the mode by which the port becomes part of the port-channel. The channel-group-number ranges from 1 to 64. Each port-channel can have up to eight compatibly configured Ethernet interfaces.

Whenever a port-channel is created, it is added as an untagged member port of the default VLAN 1. For other VLANs, it needs to be explicitly configured (or dynamically learnt through GVRP) as a member port. It does not inherit the VLAN membership of its member ports. When a port is aggregated into a bundle, that port will not be visible to higher Layer 2 applications like VLAN, STP, etc., only the port-channel port will be visible to them. Hence, when the port gets aggregated into a port channel port, then it will be removed from the membership of the specific VLAN. Similarly, when a port is disaggregated from a port-channel, it is added as a member port of the default VLAN 1.

NOTE: When the MTU of a port in a bundle differs from the Port Channel's MTU, then the port will not be up in the bundle. However, if we change the MTU of the port channel then it will be applied on all the ports in the bundle. All the port-channel member ports will become up in bundle in Switch A.

LAG command Hierarchy

+ root

+ config terminal

    - [no] shutdown port-channel

    - set port-channel {enable | disable}

- channel-protocol lacp

- [no] lacp system-identifier <aa:aa:aa:aa:aa:aa>

- port-channel load-balance ([src-mac][dest-mac][src-dest-mac][src ip][destip][src-dest-ip][vlan-id] [service-instance][mac-src-vid][mac-dest vid][macsrc-dest-vid][l3-protocol][dest-l4-port][src-l4 port])[<port-channel index(1-65535)>]

-[no] interface port-channel <LAG ID>

        -[no] description DESCRIPTION

        -[no] shutdown

    - interface <port type> <port ID>

        -[no] lacp port-priority (0-65535)

        -[no] channel-group <channel-group-number(1-65535)> mode on

-[no] default port <interface-type> <interface-id>

- port-channel max-ports <integer (2-8)>

    - port-channel load-balance <policy> <LAG ID>

- show etherchannel

- show etherchannel summary

- show etherchannel <> detail

- show interfaces etherchannel

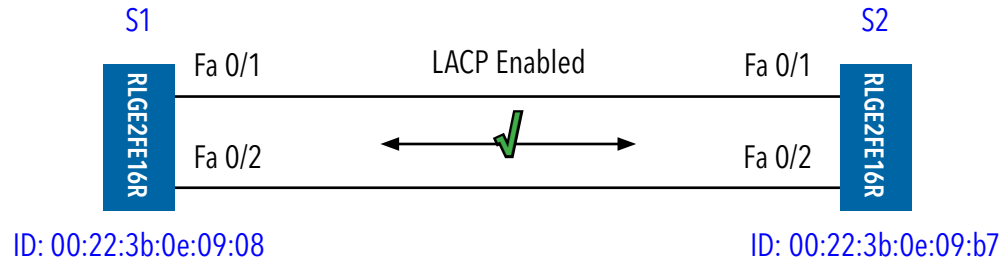
- show lacp counters

- show lacp neighbor

LAG Commands Descriptions

Command	Description
config terminal	Enters the Configuration mode
[no] shutdown port-channel	This command shuts down LA feature in the switch and releases all resources allocated to the LA feature. The no form of the command starts and enables LA feature in the switch, and allocates required memory to the LA module. The LA feature is made available in the switch only if the LA is enabled in the switch. LA feature allows to aggregate individual point-to-point links into a port channel group, so that the capacity and availability of the communications channel between devices are increased using the existing interface technology. Defaults: LA is started in the switch, but not enabled. That is LA operational status is disabled.
set port-channel (enable | disable)	This command configures the admin status of LA in the switch. The LA feature is made available in the switch only if the LA is enabled in the switch. LA feature allows you to aggregate individual point-to-point links into a port channel group, so that the capacity and availability of the communications channel between devices are increased using the existing interface technology. Defaults: disable
[no] interface port-channel <LAG ID>	This command creates logical interface that represents an aggregator which contains several ports aggregated together.
[no] description DESCRIPTION	Add description to port channel
[no] shutdown	Enable/ Disable port channel
interface <port type> <port ID>	Entering to the relevant interface to be configured
[no] lacp port-priority (0-65535)	This command configures the LACP port priority. The no form of the command resets the LACP port priority to its default value. This port priority is used in combination with LACP port identifier during the identification of best ports in a port channel. The priority determines if the link is an active link or a standby link, when the number of ports in the aggregation exceeds the maximum number supported by the hardware. The links with lower priority becomes active links. This value ranges between 0 and 65535 Defaults: 128
channel-group <channel-group-number(1-65535)> mode on	This command adds the port as a member of the specified port channel that is already created in the switch. The no form of the command deletes the aggregation of the port from all port channels. **channel-group-number(1-65535)**: Adds the port as a member of the specified port channel. This is a unique value that represents the specific port channel created. This value ranges from 1 to 65535.
port-channel load-balance <policy> <LAG ID>	This command configures the load balancing policy for all port channels created in the switch. The no form of the command resets the load balancing policy to its default value. The policy sets the rule for distributing the Ethernet traffic among the aggregated links to establish load balancing. The load-balance policy can be configured as: **src-mac**: Load distribution is based on the source MAC address in the frame. Packets from different hosts use different ports in the channel, but packets from the same host use the same port. **dest-mac**: Load distribution is based on the destination MAC address in the frame. Packets to the same destination are sent on the same port, but packets to different destinations are sent on different ports in the channel. **src-dest-mac**: Load distribution is based on the source and destination MAC addresses. **src-ip**: Load distribution is based on the source IP address. **dest-ip**: Load distribution is based on the destination IP address. **src-dest-ip**: Load distribution is based on the source and destination IP addresses. **vlan-id**: Load distribution is based on VLAN Identifier.
show interfaces etherchannel	This command shows LAG detailed info
show etherchannel	This command shows LAG feature status on the switch

Example



1. Configure port channel

```
config
set port-channel enable
interface port-channel 1
no shutdown
exit
```

2. Assign the interfaces

```
interface fastethernet 0/1
channel-group 1 mode active
exit
interface fastethernet 0/2
channel-group 1 mode active
end
```

Output of show commands, switch S1

1. show ether channel summary

```
S1# show etherchannel summary
Port-channel Module Admin Status is enabled
Port-channel Module Oper Status is enabled
Port-channel Independent mode is disabled
Port-channel System Identifier is 00:22:3b:0e:09:08
LACP System Priority: 32768

Flags:
D - down          P - in port-channel
I - stand-alone   H - Hot-standby (LACP only)
U - in-use        d - default port
```

```
Number of channel-groups in use: 1
Number of aggregators: 1

Group   Port-channel     Protocol    Ports
------------------------------------------------------------------------
1       Po1(U)            LACP        Fa0/1(P),Fa0/2(P)
```

2. show lacp neighbor

```
S1# show lacp neighbor
Flags:
A - Device is in Active mode
P - Device is in Passive mode
Channel group 1 neighbors
Port Fa0/1
----------
Partner System ID                : 00:22:3b:0e:09:08
Flags                             : A
LACP Partner Port Priority       : 128
LACP Partner Oper Key             : 1
LACP Partner Port State          : 0xbc
Port Fa0/2
----------
Partner System ID                : 00:22:3b:0e:09:b7
Flags                             : A
LACP Partner Port Priority       : 128
LACP Partner Oper Key             : 1
LACP Partner Port State          : 0xbc
```

3. show counters

```
S1# show lacp counters

         LACPDUs             Marker      Marker Response     LACPDUs
Port    Sent   Recv       Sent   Recv       Sent    Recv       Pkts Err
---------------------------------------------------------------------
Channel group: 1
-----------------
Fa0/1     75     76          0      0          0      0          0      0
Fa0/2     73     72          0      0          0      0          0      0
```

STP

The following sections describe the configuration of the Spanning Tree Protocol.

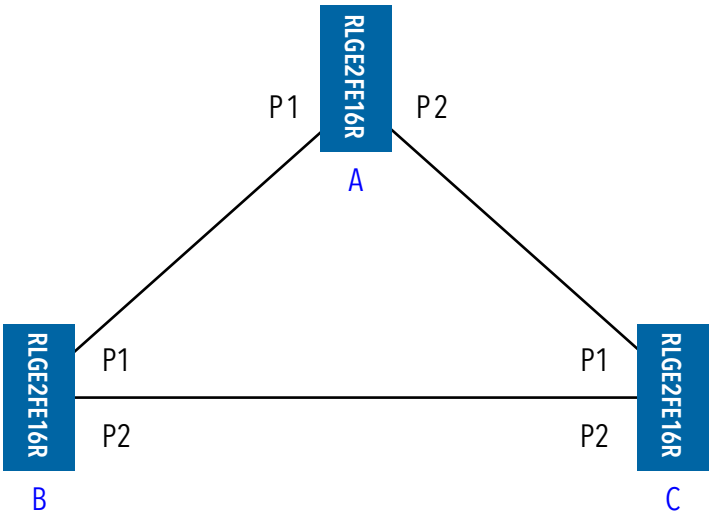


Figure 2-1: Spanning Tree Topology

Switch A:

MAC Address: 00:01:02:03:04:01

VLAN 1 - 10.0.0.1/255.0.0.0

Switch B:

MAC Address: 00:02:02:03:04:01

VLAN 1 – 10.0.0.2 /255.0.0.0

Switch C:

MAC Address: 00:03:02:03:04:01

VLAN 1 – 10.0.0.3/255.0.0.0

STP Description

The Bridge allows interconnection of end stations attached to separate LANs and allows them to communicate as if they were attached to a single LAN. The Bridge operates below the MAC service boundary, and is transparent to the protocols operating above this boundary. In complex networks, a loop may occur when there are two or more paths between two end points. This leads to the duplication of frames, which in turn leads to heavy traffic in the network. To avoid this, STP (Spanning Tree Protocol) is used in the ComNet RLGE2FE16R software. STP forms a logical, loop-free topology from the physical topology and forwards the frames without duplication. To avoid prolonged stabilization time following a reconfiguration event in Spanning Tree algorithm, ComNet RLGE2FE16R provides support for RSTP (Rapid Spanning Tree Protocol). The operation of RSTP provides for rapid recovery of connectivity following the failure of a Bridge/ Bridge Port or a LAN.

To isolate link fluctuations specific to a particular VLAN segment(s) and to provide for load balancing, ComNet RLGE2FE16R supports Multiple Spanning Trees. These can be configured on a per VLAN basis or multiple VLANs can be mapped to the same spanning tree. A switch can take the role of either a root or a designated switch. Spanning tree operation provides path redundancy while preventing undesirable loops in the network that are created by multiple active paths between stations. It logically breaks such loops and prevents looping traffic from clogging the network.

STP calculates the best loop free path by assigning port roles to the port of switch as follows:

» Root: The port that offers the lowest cost path towards the Root bridge.

» Designated: A forwarding port elected for every switched LAN segment.

» Alternate: A blocked port providing an alternate path to the root bridge of the spanning tree.

» Backup: A blocked port that acts as a backup for the path provided by a Designated Port.

The stable, active spanning-tree topology of a switched network is determined by the following elements.

» Bridge ID (Switch Priority and MAC address)

» Path Cost to the Root Switch

» Port Identifier (Port priority and the Port Number)

When switches in a network come up, each switch assumes itself to be the Root Bridge and starts sending configuration messages through all its ports. BPDUs are used to communicate and compute the spanning tree topology. These BPDUs contain the following information:

» Unique Bridge ID of the switch that has been identified as the Root

» The spanning-tree path cost to the Root

» The Bridge ID of the sending switch

» Message age

» The identifier of the sending interface (port priority and port number)

» Values for the hello, forward-delay, and max-age protocol timers

When a switch receives a superior configuration BPDU on a port, it stores the received information for that port. If the port is a root port, it forwards the updated message to all the attached LANs

for which this switch is the designated bridge. If the switch receives an inferior configuration BPDU to that currently stored for that port, it discards the BPDU. If the switch is a designated switch for that LAN from which the inferior information was received, then it sends up-to-date information stored for that port, thus discarding inferior information and propagating superior information in the network. Each Layer 2 interface in the switch running spanning tree protocol can be in one of the following states.

» Blocking: The interface in this state discards the frames and does not learn the MAC addresses.

» Listening: This is the first state that a port can transition to after blocking. The interface enters this state when spanning tree decides that the interface must participate in frame forwarding.

» Learning: An interface enters this state from listening state. In this state, the interface gets ready to participate in frame forwarding and learns MAC addresses from the packet received.

» Forwarding: In this state, the interface receives and forwards frames received on that port or forwards frames switched from another port. This transition from blocking to forwarding takes 30 seconds.

Bridge ID and Switch Priority

Each switch has a unique bridge identifier (bridge ID), which determines the selection of the Root Switch. The bridge ID is an 8-byte field that is composed of two subfields, Bridge Priority and MAC.

Bridge Identifier 8 bytes

2 bytes Range-0-65535 6 bytes MAC address

Default:32768

Election of the Root Switch

All switches in the Layer 2 network participating in STP gather information on other switches in the network through an exchange of data messages called Bridge Protocol Data Units (BPDUs). The exchange of messages results in the following actions:

» Election of a unique Root Switch for each spanning tree instance

» Election of a Designated switch for every switched LAN segment

» Removal of loops in the switched network by blocking Layer 2 interfaces connected to redundant links

The switch with the highest switch priority (the lowest numerical priority value) is elected as the Root Switch. If all switches are configured with the default priority (32768), then the switch with the lowest MAC address becomes the Root Switch. The switch priority value occupies the most significant bits of the bridge ID. The Root Switch is the logical center of the STP topology in a switched network. Redundant paths to the Root are put in STP blocking mode.

BPDUs contain information about the sending switch and its ports, including switch and port MAC addresses, switch priority, port priority, and path cost. The STP uses this information to elect the Root Switch and the root port for the switched network, and the root port and the designated port for each switched segment.

Default state

By default the STP is enabled on all ports.

Application ports Gi 0/3 and Gi 0/4 are set as edge ports.

STP Commands Hierarchy

+root

+config terminal

- shutdown spanning-tree

-[no] spanning-tree

-[no] spanning-tree mode (mst | rst | rapid-pvst)

-[no] spanning-tree (forward-time | hello-time | max-age)

-[no] spanning-tree [mst <instance-id>] priority <value(0-61440)>

-[no] spanning-tree portfast {bpdufilter default | bpduguard default | default}

-interface <port type> <port ID>

-[no] spanning-tree (cost <value(0-200000000)> | disable | link-type(point-topoint | shared) | portfast | port-priority <value(0-240)>)

-[no] spanning-tree disable

-[no] spanning-tree auto-edge

- spanning-tree bpduguard {disable | enable}

- spanning-tree mst configuration

    -[no] name <string>

    -[no] instance <instance-id (1-64)> vlan <vlan-range>

- show spanning-tree detail

- show spanning-tree interface <interface-id>

- show spanning-tree summary

STP Commands Descriptions

Command	Description
config terminal	Enters the Configuration mode
shutdown spanning-tree	This command shuts down spanning tree functionality in the switch. The switch does not execute any kind of STP to form a loop free topology in the Ethernet network and operates with the existing topology structure. Defaults: Spanning tree MSTP is started and enabled in the switch.
[no] spanning-tree	This command enables the spanning tree operation in the switch for the selected spanning tree mode. The no form of this command disables the spanning tree operation in the switch. The spanning tree operation is automatically enabled in the switch, once the spanning tree mode is changed. Defaults: Spanning tree MSTP is started and enabled in the switch.
[no]spanning-tree mode (mst | rst | rapid-pvst)	This command sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch. The current selected type of spanning tree is enabled and the existing spanning tree type is disabled in the switch. **Mst**: Configures the switch to execute MSTP for preventing undesirable loops. MSTP configures spanning tree on per VLAN basis or multiple VLANs per spanning tree. The mode cannot be set as mst, if the base bridge mode is configured as transparent bridging. **Rst**: Configures the switch to execute RSTP for preventing undesirable loops. RSTP provides rapid recovery of connectivity following the failure of a bridge/bridge port or a LAN. Defaults: mst
[no] spanning-tree (forward-time | hello-time | max-age)	This command sets the spanning tree timers such as hello time, that are used for controlling the transmission of BPDUs during the computation of loop free topology. The no form of this command resets the spanning tree timers to its default values. The spanning tree timers are reset to its default value, even if the spanning tree mode is changed. **forward-time**: Configures the number of seconds, a port waits before changing from the blocking state to the forwarding state. This value ranges between 4 and 30 seconds. In MSTP, this time configuration is applied for IST root (that is, MSTI 0). Defaults: forward-time - 15 seconds **hello-time**: Configures the time interval (in seconds) between two successive configuration BPDUs generated by the root switch. This value should be either 1 or 2 seconds. This value is configured on per-port basis for MSTP and is configured globally for RSTP. Defaults: hello-time - 2 seconds **max-age**: Configures the maximum expected arrival time (in seconds) of hello BPDUs. STP information learned from network on any port is discarded, once the configured arrival time expires. The spanning tree topology is re-computed after this time interval. This value ranges between 6 and 40 seconds. In MSTP, this time configuration is applied for IST root (that is, MSTI 0). Defaults: max-age - 20 seconds
[no]spanning-tree[mst <instance-id>] priority <value(0-61440)>	This command configures the priority value that is assigned to the switch. The no form of this command resets the priority to its default value. The priority value is changed to its default value even if the spanning tree mode is changed. **Mst**: Configures the ID of MSTP instance already created in the switch. This value ranges between 1 and 64. The special value 4094 can be used only in the switch that supports PBB-TE. This special value represents PTETID that identifies VID used by ESPs. This option is applicable, only if the spanning tree mode is set as mst. **Priority**: Configures the priority value for the switch and for the MSTI, in RSTP and MSTP respectively. This value ranges between 0 and 61440. The value should be set in steps of 4096, that is, you can set the value as 0, 4096, 8192, 12288 and so on. Defaults: priority = 32768

Command	Description
no spanning-tree portfast	This command1 configures the portfast of the non-trunk ports as bpdufilter default or bpduguard default or default. Default- Enables PortFast by default on all access ports. bpdufilter- Enables BPDU filtering on all PortFast ports. bpduguard default- Enables BPDU guard feature on all PortFast ports.
Interface <port type> <port ID>	Entering to the relevant interface to be configured
[no]spanning-tree(cost <value(0-200000000)>|disable |link-type(point-topoint| shared) | portfast | port-priority <value(0-240)>)	This command configures the port related spanning tree information for all kinds of STPs. This can be applied for any port, in RSTP/MSTP mode The no form of this command resets the port related spanning tree information to its default value. The port related spanning tree information is changed to its default value even if the spanning tree mode is changed. **Cost**: Configures the port's path cost value that contributes to the path cost of paths containing this particular port. The paths' path cost is used during calculation of shortest path to reach the root. The path cost represents the distance between the root port and designated port. This value ranges between 1 and 200000000. The configured path cost is used, even if the dynamic pathcost calculation feature or LAGG speed feature is enabled. This configuration is not supported for the spanning tree mode pvrst. Defaults: 200000 for all physical ports. 199999 for port channels **Disable**: Disables the spanning tree operation on the port. The port does not take part in the execution of spanning tree operation for preventing undesirable loops in the network. Defaults: Spanning tree operation is enabled in the port. **link-type**: Configures the link status of the LAN segment attached to the port. The options available are: 1. point-to-point – The port is treated as if it is connected to a point-to-point link. 2. shared - The port is treated as if it is using a shared media connection. Defaults: The port is considered to have a point-to-point link if: It is an aggregator and all of its members can be aggregated. The MAC entity is configured for full duplex operation, either manually or through auto negotiation process (that is, negotiation mode is set as Auto) Otherwise port is considered to have a shared media connection **Portfast**: Configures the portfast feature in the port. This feature specifies that the port is connected to only one hosts and hence can rapidly transit to forwarding. This feature can cause temporary bridging loops, if hubs, concentrators, switches, bridges and so on are connected to this port. This feature takes effect only when the interface is shutdown. **port-priority**: Configures the priority value assigned to the port. This value is used during port role selection process. This value ranges between 0 and 240. This value should be set in steps of 16, that is, you can set the value as 0, 16, 32, 48, and so on. This configuration is not supported for the spanning tree mode pvrst.
[no] spanning-tree auto-edge	This command enables automatic detection of Edge port parameter of an interface. The no form of this command disables automatic detection of Edge port parameter of an interface. The automatic detection of Edge port parameter is disabled, even if the spanning tree mode is changed. Once automatic detection is enabled, the Edge port parameter is automatically detected and set. The port is set as edge port, if no BPDU is received on the port. The port is set as non-edge port, if any BPDU is received. Defaults: Automatic detection of Edge port parameter of an interface is enabled.
spanning-tree mst configuration	This command enters into MSTP configuration mode, where instance specific and MST region configuration can be done.
spanning-tree bpduguard {disable | enable}	This command configures the status of BPDU guard. The BPDU guard feature disables the port and puts the port in error-disabled state on receiving BPDU, if the portfast feature is enabled on the port. This feature prevents the devices connected to the port from participating in STP operation. Once disabled, the port can be enabled only manually. feature in an interface.

Command	Description
[no] name <string>	This command configures the name for the MST region. The no form of this command resets the name to its default value. The name is unique and used to identify the specific MST region. Each MST region contains multiple spanning tree instances and runs special instance of spanning tree known as IST to dRLGE2FE16Reminate STP topology information for other STP instances. Defaults: Same as that of the base MAC address of the switch.
[no] instance <instance-id (1-64)> vlan <vlan-range>	This command creates an MST instance and maps it to VLANs. The no form of this command deletes the instance / un-maps specific VLANs from the MST instance. **instance-id (1-64)**: Configures the ID of MSTP instance to be created /deleted and mapped with / unmapped from VLAN. This value ranges between 1 to 64. The special value 4094 can be used in the switch that supports PBB-TE. Except vlan instance mapping, other commands for stp configurations will not be applicable in this mode. This special value represents PTETID that identifies VID used by ESPs. **Vlan**: Configures a VLAN ID or list of VLAN IDs that should be mapped with / unmapped from the specified MST instance. This value is a string whose maximum size is 9. For example, the value is provided as 4000-4010 to represent the list of VLANs IDs from 4000 to 4010. Defaults: Instance 0 is created and mapped with all VLANs (1-4094).
show spanning-tree active	This command displays spanning tree related information available in the switch for the current STP enabled in the switch. The information contains priority, address and timer details for root and bridge, status of dynamic path cost calculation feature, status of spanning tree function, STP compatibility version used, configured spanning tree mode, bridge and port level spanning tree statistics information, and details of ports enabled in the switch. The port details contain port ID, port role, port state, port cost, port priority and link type.
show spanning-tree detail	This command displays detailed spanning tree related information of the switch and all ports enabled in the switch. The information contains status of spanning tree operation, current selected spanning mode, current spanning tree compatibility version, bridge and root priority, bridge and root addresses, port path cost, port priority, port timers, bridge and port level spanning tree statistics information, transmit hold-count value, link-type, and status of L2GP, loop guard, BPDU receive, BPDU transmit, restricted TCN, restricted role and portfast features.
show spanning-tree interface <interface-id>	This command displays the port related spanning tree information for the specified interface. The information contains port ID, port role, port state, port cost, port priority and link type. The generic command cannot be executed without any option in the PVRST mode. **interface-id**: Displays the port related spanning tree information for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1. Only i-lan and port-channel ID is provided, for interface types i-lan and port-channel. For example: 1 represents i-lan and port-channel ID.
show spanning-tree summary	Displays a summary of port states or displays the total lines of the STP state section.

RSTP/MSTP

RSTP Description

The Rapid Spanning Tree Protocol Module is based on the IEEE 802.1w rapid reconfiguration. The existing spanning tree protocol, in particular takes significant time to re-configure and restore the service on link failure/restoration. RSTP avoids re-convergence delay by calculating an alternate root port and immediately switching over to the alternate port, if the root port becomes unavailable.

Port States

STP (802.1D) Port State	RSTP Port State	Is Port Included in active topology?	Is Port Learning MAC address?
Disabled	Discarding	No	No
Blocking	Discarding	No	No
Listening	Discarding	No	No
Learning	Learning	No	Yes
Forwarding	Forwarding	Yes	Yes

Port Roles

Port Role	Description
Root	Provides the best path to the root. This is the port that receives the best BPDU on a bridge.
Designated	A port is designated if it can send the best BPDU on a segment to which it is connected. Bridges connected to a given segment listen to the BPDUs of other bridges and agree on the bridge sending the best BPDU as the designated bridge for that segment and the port as designated port.
Alternate	A port blocked since another port on the bridge receives superior information from another bridge. This port corresponds to the blocking state of 802.1D.
Back-up	A port blocked since another port receives superior information from the same bridge. This port also corresponds to the blocking state of 802.1D.

A port with the root or a designated port role is included in the active topology. A port with the alternate or backup port is excluded from the active topology.

Rapid Convergence

Faster convergence compared to legacy spanning tree algorithm is the most important feature in RSTP. RSTP relies on two new variables for achieving this.

» Edge Port: Ports that are directly connected to end stations cannot create bridging loops and hence can rapidly transition to forwarding skipping the learning and listening states. When the link toggles on an edge-port then the topology-change is not triggered. Whenever a BPDU is received on an edge port, it loses its edge port status and becomes a normal spanning tree port. ComNet RSTP uses portfast keyword for edge port configuration.

» Link Types: RSTP can achieve rapid transition on point-to-point links. The link type is automatically derived from the duplex mode of a port. A port operating in full-duplex will be assumed to be point-to-point, while a half-duplex port will be considered as a shared port by default. This automatic link type setting can be overridden by explicit configuration.

Proposal Agreement Sequence

In Spanning tree algorithm, a port selected as a designated port waits for 2 x Fwd-delay (2 x 15) seconds before transitioning to forwarding state. In RSTP, this port corresponds to a designated role and blocking state. Figure 3-1 illustrates the rapid transition of a port to forwarding state.

P0: Designated port

P1: New root port

P2: Alternate port

P3: Designated port

P4: Edge Port

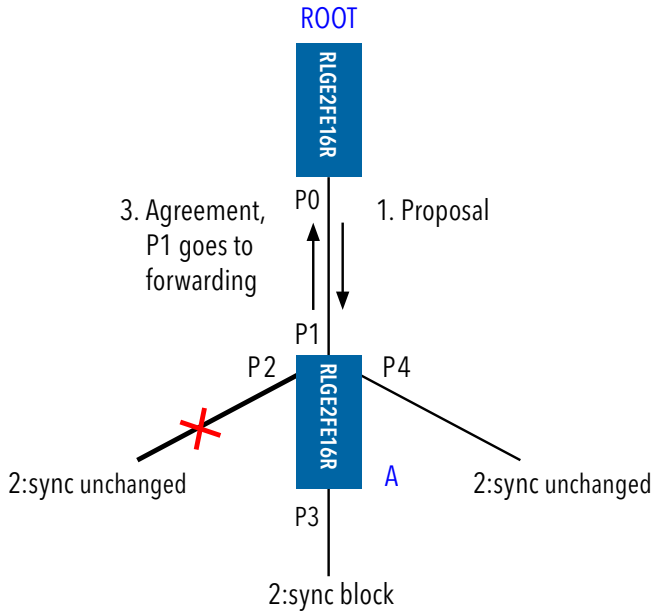


Figure 3-1: Proposal Agreement Handshake

If a new link is created between the Root and Switch A, then both the ports on this link are put in designated blocking state, until they receive a BPDU from their counterpart. When a designated port is in discarding or learning state (and only in this case), it sets the proposal bit on the BPDUs it sends out. This happens for port P0 of the root bridge, as shown in step 1 of Figure 3-1. Because switch A receives superior information, it immediately knows that P1 will be its new root port. Switch A then starts a sync operation to ensure that all of its ports are in-sync with this new information. A port is in-sync if it meets either of the following criteria:

» The port is in blocking state

» The port is an edge port

If there exists an alternate port P2, a designated forwarding port P3, and an edge port P4 on switch A. P2 and P4 already meet one of the listed criteria. To be in-sync (step 2 of the diagram above), switch A just needs to block port P3, assigning it the discarding state. If all ports are in-sync, switch A can unblock its newly selected root port P1 and reply to the Root by sending an agreement message (step 3). This message is a copy of the proposal BPDU, with the agreement bit set instead of the proposal bit. This ensures that port P0 knows exactly to which proposal, the agreement it receives corresponds.

When P0 receives that agreement, it can immediately transition to forwarding. Port P3 which was left in a designated discarding state after the sync, in the next Step, is exactly in the same state as port P0 was in Step 1. It then starts proposing to its neighbor, attempting to quickly transition to forwarding. This handshake mechanism propagates quickly towards the edge of the network, and quickly restores connectivity after a change in the topology.

Topology Change and Topology Change Detection

When an 802.1D Bridge detects a topology change, it first notifies the Root Bridge, using a reliable mechanism. Once the Root Bridge is aware of a change in the topology of the network, it sets the Topology Change (TC) flag on the BPDUs it sends out, which are then relayed to all the bridges in the network. When a bridge receives a BPDU with the TC flag bit set, it reduces its bridging-table aging time to forward delay seconds, ensuring a relatively quick flushing of stale information.

In RSTP, only non-edge ports moving to the forwarding state cause a topology change. This means that a loss of connectivity is not considered as a topology change any more, contrarily to 802.1D (that is, a port moving to blocking does no longer generates a TC). When a RSTP bridge detects a topology change, the following happens:

» It starts the TC While timer with a value equal to twice the hello time for all its non-edge designated ports and its root port, if necessary.

» It flushes the MAC addresses associated with all these Non-edge designated ports.

» As long as the TC While timer is running on a port, the BPDUs sent out of that port have the TC bit set. The BPDUs are also sent on the root port while the timer is active.

Default Configurations

Feature	Default Setting
Spanning Tree mode	MSTP
Spanning Tree Status	Enabled
Spanning tree timers	Hello time: 2 seconds Forward-delay time: 15 seconds. Maximum-aging time: 20 seconds.
Switch Priority	32768
Spanning-tree port priority (configurable on a per-interface basis)	128
Spanning-tree port cost (configurable on a per-interface basis)	200000 (For RSTP, the default value is 65535)

Setting Spanning Tree Compatibility to STP

When the switch comes up, spanning tree is enabled by default with MSTP operating in the switch.

1. Execute the following commands in the switch to set the spanning tree compatibility version for STP.

- Enter the Global Configuration mode.

```
RLGE2FE16R# configure terminal
```

- Set the priority for the spanning tree protocol.

```
RLGE2FE16R(config)# spanning-tree priority 4096
```

For priority, the range is 0 to 61440, in increments of 4096. The default is 32768. The lower the number, the more likely the switch will be chosen as the Root Switch. Valid priority values are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. All other values are rejected.

- Exit configuration mode.

```
RLGE2FE16R(config)#end
```

NOTE: Observation after configuring the Bridge priority for Switch C: Switch C has been detected as the Root and Port 1 of Switch B is the Alternate Port.

2. View the spanning tree information by executing the following show command.

```
RLGE2FE16R# show spanning-tree
```

In Switch A:

```
Root Id Priority 4096
Address 00:03:02:03:04:01
Cost 200000
Port 2 [Gi0/2]
Max age 20 Sec, forward delay 15 Sec
MST00
Spanning Tree Protocol Enabled.
MST000 is executing the mstp compatible Multiple Spanning Tree Protocol
Bridge Id Priority 32768
Address 00:01:02:03:04:01
Max age is 20 sec, forward delay is 15 sec
Name Role State Cost Prio Type
---- ---- ----- ---- ---- ------
Gi0/1 Designated Forwarding 200000 128 SharedLan
Gi0/2 Root Forwarding 200000 128 SharedLan
```

In Switch B

```
Root Id Priority 4096
Address 00:03:02:03:04:01
Cost 200000
Port 2 [Gi0/2]
Max age 20 Sec, forward delay 15 Sec
MST00
Spanning Tree Protocol Enabled.
MST000 is executing the mstp compatible Mutiple Spanning Tree Protocol
Bridge Id Priority 32768
Address 00:02:02:03:04:01
Max age is 20 sec, forward delay is 15 sec
Name Role State Cost Prio Type
---- ---- ----- ---- ---- ------
Gi0/1 Alternate Discarding 200000 128 SharedLan
Gi0/2 Root Forwarding 200000 128 SharedLan
```

In Switch C

```
Root Id Priority 4096
Address 00:03:02:03:04:01
Cost 0
Port 0 [0]
This bridge is the root
Max age 20 Sec, forward delay 15 Sec
MST00
Spanning Tree Protocol Enabled.
MST000 is executing the mstp compatible Mutiple Spanning Tree Protocol
Bridge Id Priority 4096
Address 00:03:02:03:04:01
Max age is 20 sec, forward delay is 15 sec
Name Role State Cost Prio Type
---- ---- ----- ---- ---- ------
Gi0/1 Designated Forwarding 200000 128 SharedLan
Gi0/2 Designated Forwarding 200000 128 SharedLan
```

Execute the no spanning-tree priority from the Global Configuration mode command to set the Priority to its default value.

```
RLGE2FE16R(config)# no spanning-tree priority
```

Configuring Spanning Tree Path Cost

When a loop occurs in the network topology, spanning tree protocol may use path cost to determine the spanning-tree states of the ports. Path cost is obtained from the speed of the interface. A user can configure lower path cost for an interface, if the port needs to be selected first or the user can configure higher path cost if the port needs to be selected last for putting it to forwarding state.

Path cost is used to determine the topology only if the loop in the network cannot be resolved using only the Bridge IDs. If all the ports have same path cost values, then the lowest numbered port is first put into forwarding state by spanning tree.

Refer Figure 2-1 for topology. All the switches are configured for STP compatible using spanning-tree compatibility STP in Global Configuration mode. After the topology stabilizes and switch A is elected as Root and the ports of all switches except Port 2 of switch C are in forwarding state. Port 2 of Switch C is an alternate port and is in discarding state.

1. Execute the following commands in the switch C

- Enter the Global Configuration mode.

```
RLGE2FE16R# configure terminal
```

- Specify the interface for which the path cost is to be configured.

```
RLGE2FE16R(config)# interface gigabitethernet 0/1
```

Valid interfaces include physical interfaces and port-channel logical interfaces (port-channel port-channel-number).

- Configure the cost for the interface.

```
RLGE2FE16R(config-if)# spanning-tree cost 2000
```

For cost, the range is 1 to 200000000; the default value is derived from the media speed of the interface.

NOTE: Observation after configuring the Path Cost for port 1 in Switch C: Port 2 of Switch B is the Alternate Port and Port 2 of Switch C is a Designated Port.

- Exit configuration mode.

```
RLGE2FE16R(config-if)# end
```

2. View the spanning tree properties of an interface.

```
In Switch A
RLGE2FE16R# show spanning-tree
Root Id Priority 32768
Address 00:01:02:03:04:01
Cost 0
Port 0 [0]
This bridge is the root
Max age 20 Sec, forward delay 15 Sec
MST00
Spanning Tree Protocol Enabled.
MST00 is executing the mstp compatible Multiple Spanning Tree Protocol
Bridge Id Priority 32768
Address 00:01:02:03:04:01
Max age is 20 sec, forward delay is 15 sec
Name Role State Cost Prio Type
---- ---- ----- ---- ---- ------
Gi0/1 Designated Forwarding 200000 128 SharedLan
Gi0/2 Designated Forwarding 200000 128 SharedLan
```

In Switch B

```
RLGE2FE16R# show spanning-tree
Root Id Priority 32768
Address 00:01:02:03:04:01
Cost 200000
Port 1 [Gi0/1]
Max age 20 Sec, forward delay 15 Sec
MST00
Spanning Tree Protocol Enabled.
MST00 is executing the mstp compatible Multiple Spanning Tree Protocol
Bridge Id Priority 32768
Address 00:02:02:03:04:01
Max age is 20 sec, forward delay is 15 sec
Name Role State Cost Prio Type
---- ---- ----- ---- ---- ------
Gi0/1 Root Forwarding 200000 128 SharedLan
Gi0/2 Alternate Discarding 200000 128 SharedLan
```

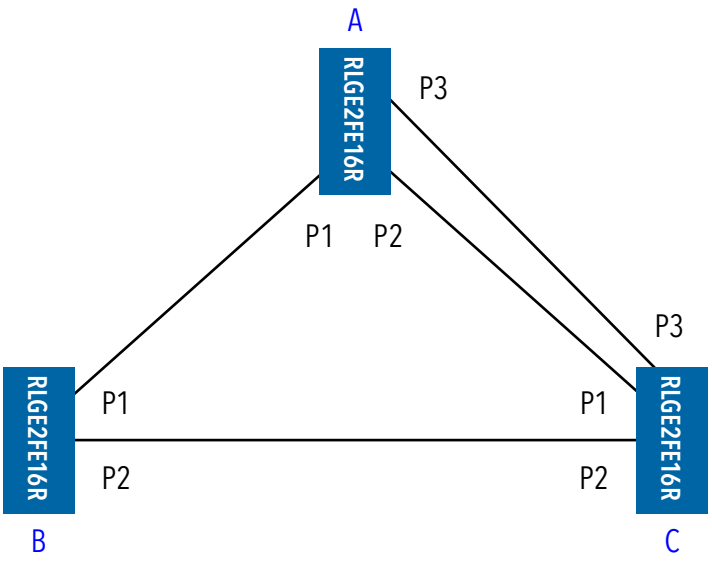
In Switch C

```
RLGE2FE16R# show spanning-tree
Root Id Priority 32768
Address 00:01:02:03:04:01
Cost 2000
Port 1 [Gi0/1]
Max age 20 Sec, forward delay 15 Sec
MST00
Spanning Tree Protocol Enabled.
MST00 is executing the mstp compatible Multiple Spanning Tree Protocol
Bridge Id Priority 32768
Address 00:03:02:03:04:01
Max age is 20 sec, forward delay is 15 sec
Name Role State Cost Prio Type
---- ---- ----- ---- ---- ------
Gi0/1 Root Forwarding 2000 128 SharedLan
Gi0/2 Designated Forwarding 200000 128 SharedLan
```

Execute the no spanning-tree cost Interface Configuration mode command to set the default value of the Spanning Tree Path Cost.

```
RLGE2FE16R(config-if)# no spanning-tree cost
```

Configuring Spanning Tree Port Priority



Switch A :VLAN 1 -10.0.0.1/255.0.0.0

Switch B :VLAN 1 – 10.0.0.2 /255.0.0.0

Switch C :VLAN 1 – 10.0.0.3/255.0.0.0

Figure 3-2: Spanning Tree Topology for Configuring Port Priority

When a loop occurs in a network topology, spanning tree may use the value of port-priority of the ports to decide the port that must be put in the forwarding state.

Port priority is used to determine the topology only if the loop in the network cannot be resolved using the Bridge IDs or path-cost.

If higher priority (lower numerical value) is assigned to a port, it goes to forwarding first and when lower priority (higher numerical value) is assigned to a port, it goes to forwarding last. If all ports have same priority values, spanning tree puts the lowest numbered interface to forwarding and blocks all the other interfaces.

Refer Figure 3-1 for setup. All the switches are configured for STP compatible using the spanning-tree compatibility stp Global Configuration mode command. After the topology stabilizes, switch A is elected as Root and all ports of all switches except Port 2 and 3 (alternate, discarding) of switch C are in forwarding.

1. Execute the following commands in the switch A.

- Enter the Global Configuration mode.

```
RLGE2FE16R# configure terminal
```

- Specify the interface for which the port priority is to be configured.

```
RLGE2FE16R(config)# interface gigabitethernet 0/3
```

Interfaces can be physical interfaces and port-channel logical interfaces (port-channel port-channel-number).

- Configure the port priority for spanning tree.

```
RLGE2FE16R(config-if) # spanning-tree port-priority 32
```

For priority, the range is 0 to 240 in increments of 16. The default is 128. The lower the number, the higher the priority.

Valid priority values are 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, and 240. All other values are rejected.

NOTE: Observation after configuring the Port Priority for Port 3 in Switch A: Ports 1, 2 of Switch B are the Alternate Ports and Port 3 is the root port.

- Exit configuration mode

```
RLGE2FE16R(config-if)# end
```

2. View the spanning tree properties of an interface

In Switch A

```
RLGE2FE16R# show spanning-tree
Root Id Priority 32768
Address 00:01:02:03:04:01
Cost 0
Port 0 [0]
This bridge is the root
Max age 20 Sec, forward delay 15 Sec
MST00
Spanning Tree Protocol Enabled.
MST00 is executing the mstp compatible Multiple Spanning Tree Protocol
Bridge Id Priority 32768
Address 00:01:02:03:04:01
Max age is 20 sec, forward delay is 15 sec
Name Role State Cost Prio Type
---- ---- ----- ---- ---- ------
Gi0/1 Designated Forwarding 200000 128 SharedLan
Gi0/2 Designated Forwarding 200000 128 SharedLan
Gi0/3 Designated Forwarding 200000 32 SharedLan
```

In Switch B

```
RLGE2FE16R# show spanning-tree
Root Id Priority 32768
Address 00:01:02:03:04:01
Cost 200000
Port 2 [Gi0/2]
Max age 20 Sec, forward delay 15 Sec
MST00
Spanning Tree Protocol Enabled.
MST00 is executing the mstp compatible Multiple Spanning Tree Protocol
Bridge Id Priority 32768
Address 00:02:02:03:04:01
Max age is 20 sec, forward delay is 15 sec
Name Role State Cost Prio Type
---- ---- ----- ---- ---- ------
Gi0/1 Root Forwarding 200000 128 SharedLan
Gi0/2 Designated Forwarding 200000 128 SharedLan
```

In Switch C

```
RLGE2FE16R# show spanning-tree
Root Id Priority 32768
Address 00:01:02:03:04:01
Cost 200000
Port 2 [Gi0/2]
Max age 20 Sec, forward delay 15 Sec
MST00
Spanning Tree Protocol Enabled.
MST00 is executing the mstp compatible Multiple Spanning Tree Protocol
Bridge Id Priority 32768
Address 00:03:02:03:04:01
Max age is 20 sec, forward delay is 15 sec
Name Role State Cost Prio Type
---- ---- ----- ---- ---- ------
Gi0/1 Alternate Discarding 200000 128 SharedLan
Gi0/2 Alternate Discarding 200000 128 SharedLan
Gi0/3 Root Forwarding 200000 128 SharedLan
```

Execute the no spanning-tree port-priority Interface configuration command to set the Spanning Tree Port Priority to its default value.

```
RLGE2FE16R(config-if) # no spanning-tree port-priority
```

Configuring Spanning Tree Link type

If a port is configured as point-to-point link and its port role is designated, then ComNet RSTP negotiates a rapid transition to forwarding with the other port by using proposal-handshake agreement mechanism to ensure that the topology is loop free. By default, if the interface is full-duplex, it is considered to have a point to point connection. If the interface is half duplex, then it is considered to have a shared connection. This default setting of link type can be overridden to enable rapid transition to forwarding.

1. Execute the following commands in the switch.

- Enter the Global Configuration mode.

```
RLGE2FE16R# configure terminal
```

- Specify the interface for which the link type is to be configured.

```
RLGE2FE16R(config)# interface gigabitethernet 0/1
```

Valid interfaces include physical interfaces and port-channel logical interfaces (port-channel port-channel-number).

- Configure link type of interface as point-to-point.

```
RLGE2FE16R(config-if) # spanning-tree link-type point-to-point
```

- Exit configuration mode.

```
RLGE2FE16R(config-if)# end
```

2. View the spanning tree properties of an interface.

```
RLGE2FE16R# show spanning-tree detail
Spanning tree Protocol Enabled.
MST00 is executing the mstp compatible Multiple Spanning Tree Protocol
Bridge Identifier has Priority 32768, Address 00:01:02:03:04:01
Configured Max age 20 sec, Forward delay 15 sec
Configured Hello Time 2 sec
We are root of the spanning tree
Current Root has priority 32768, address 00:01:02:03:04:01
cost of root path is 0
Number of Topology Changes 1, Time since topology Change 37 seconds ago
Transmit Hold-Count 3
Times : Max age 20 Sec,Forward delay 15 Sec
Port 1 [Gi0/1] of MST00 is Designated, Forwarding
Gi0/1 is operating in the MSTP Mode
Port path cost 200000, Port priority 128,
Port Identifier 128.1. Port HelloTime 2,
Timers:Hello - 0,Forward Delay - 0,Topology Change - 2
```

```
Designated root has priority 32768, address 00:01:02:03:04:01
Designated Bridge has priority 32768, address 00:01:02:03:04:01
Designated Port Id is 128.1, Designated pathcost is 0
Operational Forward delay 15, Max age 20
Number of Transitions to forwarding State : 1
PortFast is disabled
Link type is point to Point
BPDUs : sent 35, received 53
Restricted Role is disabled.
Restricted TCN is disabled.
```

Execute the no spanning-tree link-type Interface Configuration mode command to set the default link type for an Interface.

```
RLGE2FE16R(config-if) # no spanning-tree link-type
```

Configuring Spanning Tree Portfast

All ports that are directly connected to end stations cannot create bridging loops and hence can rapidly transition to forwarding, skipping the learning and listening states.

A switch can be configured to automatically detect the presence of another switch connected to one of its port. If a switch receives configuration BPDUs from other switch, it can detect the presence of the other switch connected to one of its ports. On configuring a port as portfast, if the switch does not receive any BPDUs for a certain interval then Spanning Tree puts the port to forwarding state rapidly.

1. Execute the following commands in the switch

- Enter the Global Configuration mode.

```
RLGE2FE16R# configure terminal
```

- Specify the interface for which the auto edge configuration is to be done.

```
RLGE2FE16R(config)# interface gigabitethernet 0/1
```

Valid interfaces include physical interfaces and port-channel logical interfaces (port-channel port-channel-number).

- Shutdown the interface

```
RLGE2FE16R(config-if)# shutdown
```

- Specify that the port has only hosts connected to it and hence can transition the port to forwarding rapidly.

```
RLGE2FE16R(config-if) # spanning-tree portfast
```

- Execute the no shutdown command to make the interface up.

```
RLGE2FE16R(config-if)# no shutdown
```

- Exit configuration mode.

```
RLGE2FE16R(config-if)# end
```

Configuring Spanning Tree Timers

The following table describes the timers.

Variable	Description
forward-time	Controls how fast a port changes its spanning tree state from Blocking state to Forwarding state.
hello-time	Determines how often the switch broadcasts its hello message to other switches, when it is the Root of the spanning tree.
max-age	The maximum time allowed for the Spanning Tree Protocol information learnt from the network on any port to be retained before it is discarded.

Example for Configuring Spanning Tree Timers:

```
RLGE2FE16R# configure terminal
RLGE2FE16R(config)# spanning-tree forward-time 11
RLGE2FE16R(config)# end
```

Enhanced RSTP

Enhanced RSTP is a rapid protection propriety mode of ComNet.

It allows protection time of 5msec per node hence significantly improving the protection time of standard RSTP.

This mode is supported on ring shape network (not tree) implemented over the RLGE2FE16R fiber sfp ports.

Enhanced RSTP is using the RSTP mechanism and port states but improves the protection time using fast diagnostic of the fiber link state.

A single failure is permitted.

NOTE: To make sure your hardware supports Enhanced RSTP please contact ComNet support team.

Method of operation

First, enabling rstp is required and will set the network switches and links to hold rstp known states (forwarding, learning and discarding). A ROOT switch will as well be selected. Standard rstp bpdu messages will be sent to publish the protocol states.

Once enhanced rstp is enabled at the switches, additional messages will be generated indicating the state of fiber links at the ring ports. These are broadcast messages sent from each of the ring switches to all ring members.

The enhanced-rstp protocol will determine the switches sharing the rstp alternate link as the ring LBS and NBS.

Once a link fault has occurred in the ring by a fiber signal loss on an SFP ring port, the enhanced rstp control messages will indicate this state to the LBS switch. The LBS and NBS switches will set their shared link (currently in alternate state) ports to the rstp “forwarding” stat, hence achieving protection.

When the link fault is recovered, the LBS and NBS switches will switch their shared link ports back to idle state, meaning will set the ports to achieve the rstp link alternate state.

The ERSTP refers to the ring ports as EAST and WEST whereas EAST refers to Gi 0/1 and WEST to Gi 0/2.

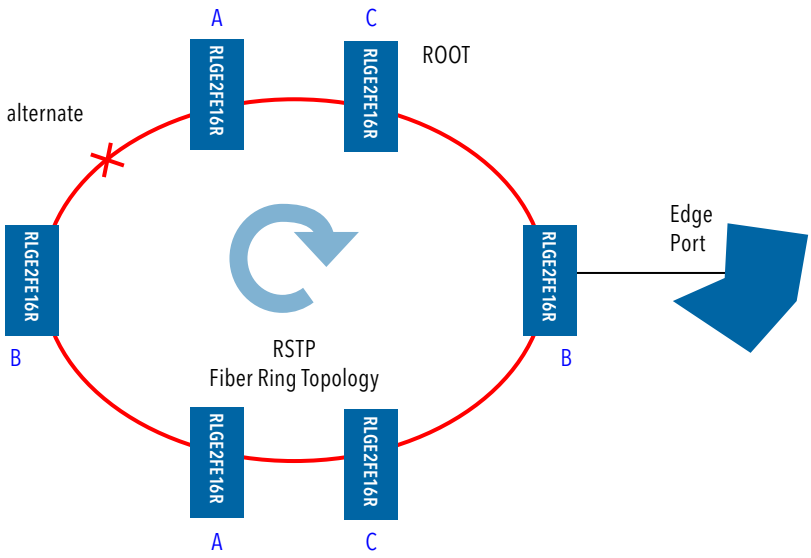


Figure 1 RSTP Ring

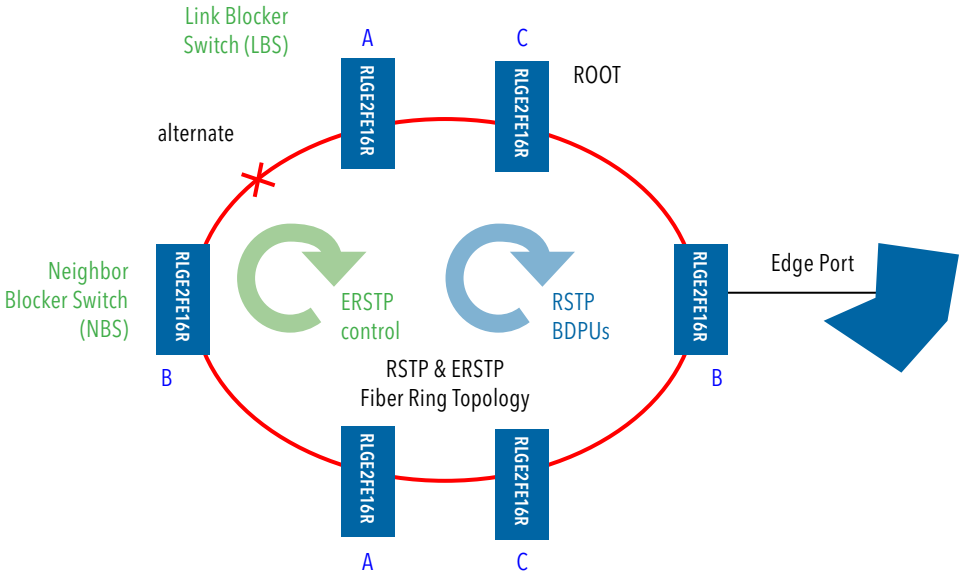


Figure 2: enhanced rstp typical network design

Example of status output

```
---------------Enhanced RSTP STATUS ---------------
Switch Status: Blocking Switch
West Link Status: Link In Forward State
East Link Status: Link In Blocked State
Switches In Ring: 4 Switches
Link Down Counter: 2
Link Up Counter: 2
Block Message Received: 0
```

Enhanced RSTP Command Hierarchy

+root

- enhanced RSTP { enable | disable | status }

+ config terminal

- shutdown spanning-tree

-[no] spanning-tree

-[no] spanning-tree mode rst

-[no] spanning-tree (forward-time | hello-time | max-age)

-[no] spanning-tree priority <value(0-61440)>

-interface <port type> <port ID>

-[no] spanning-tree (cost <value(0-200000000)> | disable | link-type(point-topoint | shared) | portfast | port-priority <value(0-240)>)

-[no] spanning-tree auto-edge

- show spanning-tree detail

- show spanning-tree interface <interface-id>

- show spanning-tree summary

Commands Descriptions

Command	Description
Root	
enhanced RSTP	Enable	disable: Activate/ deactivate the protocol. Status: show the current status

LLDP

LLDP (Link Layer Discovery Protocol) supports a set of attributes that it uses to discover the neighbor devices. These attributes contain type, length, and value descriptions and are referred to as TLVs. LLDP supported devices can use TLVs to receive and send information to their neighbors.

The switch supports these mandatory basic management TLVs.

» Port description TLV
» System name TLV
» System description
» System capabilities TLV
» Management address TLV
» Port VLAN ID TLV ((IEEE 802.1 organizationally specific TLVs)
» MAC/PHY configuration/status TLV(IEEE 802.3 organizationally specific TLVs)

ComNet LLDP is a portable software implementation of the Link Layer Discovery Protocol (LLDP). It provides complete management capabilities using SNMP and CLI. ComNet LLDP conforms to IEEE 802.1AB-2005 standard. The LLDP allows systems on an Ethernet LAN to advertise their key capabilities and also to learn about the key capabilities of other systems on the same Ethernet LAN. This, in turn, promotes a unified network management view of the LAN topology and connectivity to aid network administration and trouble-shooting.

ComNet LLDP provides the following features:

» Provides full conformance to the 802.1AB specification.
» Supports all mandatory TLVs (Chassis ID, Port ID and Time To Live).
» Supports optional TLVs - Port description, System name, System description, System capabilities and Management address.
» Supports organizationally specific optional TLVs - Port VLAN ID, Port and protocol VLAN ID, VLAN name, MAC or PHY configuration or status, Link Aggregation and Maximum frame size.
» Provides a generic set of APIs for easy integration into different platforms.
» Supports the basic MIB, as well as, the extension MIBs in Appendix F and Appendix G, defined in the 802.1AB specification and a proprietary MIB for management.
» Provides support for configuration and management by providing generic APIs usable from different management schemes like SNMP, CLI.
» Provides support for notifications through Traps.
» Conforms to Flexible Software Architecture for Portability (FSAP2), thus ensuring portable code, which uses flexible buffer and timer management libraries.

LLDP Commands Hierarchy

+root

+config terminal

-[no] shutdown lldp

-set lldp {enable | disable}

-[no] lldp transmit-interval <seconds(30,5-32768)>

-[no] lldp holdtime-multiplier <value(4,2-10)>

-[no] lldp reinitialization-delay <seconds(2,1-10)>

-[no] lldp tx-delay <seconds(2,1-8192)>

-[no] lldp notification-interval <seconds(5,5-3600)>

- lldp chassis-id-subtype { chassis-comp <string(255)> | if-alias | port-comp <string(255)> | mac-addr | nw-addr | if-name | local <string(255)> }

-clear lldp counters

-clear lldp table

+interface <port type> <port ID>

-[no] lldp {transmit | receive}

-[no] lldp notification [remote-table-chg][mis-configuration]

-[no] lldp tlv-select basic-tlv { [port-descr] [sys-name] [sys-descr] [sys-capab] [mgmt-addr {all | ipv4 <ucast_addr> }

-lldp port-id-subtype { if-alias | port-comp <string(255)> | mac-addr | if-name | local <string(255)> }

-[no] lldp tlv-select dot1tlv {[port-vlan-id] [protocol-vlan-id {all |<vlan-id>}] [vlan-name {all | <vlan-id>}]}

-[no] lldp tlv-select dot3tlv { [macphy-config] [link-aggregation] [max-framesize] }

- [no] debug lldp [{all | [init-shut] [mgmt] [data-path] [ctrl] [pkt-dump] [resource] [all-fail] [buf] [neigh-add] [neigh-del] [neigh-updt] [neigh-drop] [neighageout] [critical][tlv {all | [chassis-id] [port-id] [ttl] [port-descr] [sysname] [sys-descr] [sys-capab] [mgmt-addr] [port-vlan] [ppvlan] [vlan-name] [proto-id] [mac-phy] [pwr-mdi] [lagg] [max-frame]}] [redundancy]}]

-show lldp

-show lldp interface [<interface-type> <interface-id>]

-show lldp traffic [<iftype> <ifnum>]

- show lldp neighbors [chassis-id <string(255)> port-id <string(255)>] [<interface-type> <interface-id>][detail]

-show lldp local {[<interface-type> <interface-id>] | [mgmt-addr]}

-show lldp errors

-show lldp statistics

LLDP Commands Descriptions

Command	Description
config terminal	Enters the Configuration mode
[no] shutdown lldp	This command shuts down all the ports in the LLDP and releases all the allocated memory. The no form of the command enables all the ports by allocating the required resources in the LLDP Default: LLDP is not shutdown in the system
set lldp {enable | disable}	This command transmits or receives LLDP frames from the server to the LLDP module. **Enable**: Transmits/receives the LLDP packets between LLDP module and the server. **Disable**: Does not transmit/receive the LLDP packets between LLDP module and the server. Default: Disable
[no] lldp transmit-interval <seconds(5-32768)>	This command sets the transmission interval in which the server sends the LLDP frames to the LLDP module. The no form of the command sets the transmission interval to the default value. The value ranges between 5 and 32768 seconds. Default: 30 seconds
[no] lldp holdtime-multiplier <value(2-10)>	This command sets the holdtime-multiplier value, which is the amount of time, the server should hold the LLDP. The no form of the command sets the multiplier to the default value. The value ranges between 2 and 10 seconds. TLV (Time to Live) A value that tells the receiving agent, how long the information contained in the TLV Value field is valid. TTL = message transmission interval * hold time multiplier. For example, if the value of LLDP transmission interval is 30, and the value of the LLDP hold multiplier is 4, then the value 120 is encoded in the TTL field in the LLDP header Default: 4
[no] lldp reinitialization-delay <seconds(1-10)>	This command sets the re-initialization delay time which is the minimum time an LLDP port will wait before reinitializing LLDP transmission. The no form of the command sets the re-initialization delay time to the default value. The value ranges between 1 and 10 seconds. Default: 2 seconds
[no] lldp tx-delay <seconds(1-8192)>	This command sets the transmit delay which is the minimum amount of delay between successive LLDP frame transmissions. The no form of the command sets the transmit delay to the default value. The value ranges between 1 and 8192 seconds. NOTE: TxDelay should be less than or equal to (0.25 * Message Tx Interval) Default: 2 seconds
[no] lldp notification-interval <seconds(5-3600)>	This command sets the time interval in which the local system generates a notification-event. In the specific interval, generating more than one notification-event is not possible. The value ranges between 5 and 3600 seconds. The no form of the command sets the notification interval to the default value. Default: 5 seconds

Command	Description
lldp chassis-id-subtype { chassis-comp <string(255)> | if-alias | port-comp <string(255)> | mac-addr | nw-addr | if-name | local <string(255)> }	This command configures an ID for LLDP chassis subtype which is a unique address of any module. NOTE: Chassis id value can be set only for the chassis-component and local system subtypes. For all other subtypes, it takes the value from the system automatically. **chassis-comp**: Represents a chassis identifier based on the value of entPhysicalAlias object for a chassis component **if-alias**: Represents a chassis identifier based on the value of ifAlias for an interface on the containing chassis. **port-comp**: Represents a chassis identifier based on the value of entPhysicalAlias object for a port or backplane within the chassis. **mac-addr**: Represents a chassis identifier based on the value of a unicast source address, of a port on the chassis. **nw-addr**: Represents a chassis identifier based on a network address, associated with a particular chassis. The encoded address is actually composed of two fields. The first field is a single octet, representing the IANA AddressFamilyNumbers value for the specific address type, and the second field is the network address value. **if-name:** Represents a chassis identifier based on the value of ifName object for an interface on the containing chassis. **Local**: Represents a chassis identifier based on a locally defined value. Default: mac-addr
clear lldp counters	This command clears the inbuilt counter which has the total count of LLDP frames that are transmitted/received.
NOTE: This command does not clear the global statistics.	
clear lldp table	This command clears all the LLDP information about the neighbors.
interface <port type> <port ID>	Entering to the relevant interface to be configured
[no] lldp {transmit | receive}	This command transmits or receives LLDP frames from the one of the ports of the server to the LLDP module. The no form of the command resets LLDP admin status on an interface. **Transmit**: Enables transmission of LLDPDU from one of the ports of the server to the LLDP module. **Receive**: Enables reception of LLDPDU from one of the ports of the server to the LLDP module. Default: Transmission and Reception are enabled NOTE: This command can be executed only if lldp is not shutdown.
[no] lldp notification [remote-table-chg][mis-configuration]	This command controls the transmission of LLDP notifications. The no form of the command disables LLDP trap notification on an interface. **remote-table-chg**: Sends trap notification to NMS whenever remote table change occurs. **mis-configuration**: Sends trap notification to NMS whenever misconfiguration is identified. Default: mis-configuration
[no] lldp tlv-select basic-tlv { [port-descr] [sys-name] [sys-descr] [sys-capab] [mgmt-addr {all | ipv4 <ucast_addr>}	This command enables the basic settings while transmitting the LLDP frames on a given port. The no form of the command disables the basic TLV transmission on a given port. **port-descr**: Configures the port, which is a combination of interface type and interface ID. The interface ID is a combination of slot number and the port number (slot number/port number). **sys-name**: Configures the system name of the TLV **sys-descr**: Configures the system description of the TLV **sys-capab**: Configures the system capabilities of the TLV **mgmt-addr all**: Enables the transmission of all the available management address on the current interface. If no management address is present/configured in the system, switch mac-address will be taken for transmission. mgmt-addr ipv4 <ip addr>: Enables the transmission of a particular ipv4 address on the current interface. Default : no Tx Tlvs

Command	Description
lldp port-id-subtype { if-alias | port-comp <string(255)> | mac-addr | if-name | local <string(255)> }	This command configures an ID for LLDP port subtype. **if-alias**: Represents a chassis identifier based on the value of ifAlias for an interface on the containing chassis. **port-comp**: Represents a chassis identifier based on the value of entPhysicalAlias object for a port or backplane within the chassis. **mac-addr**: Represents a chassis identifier based on the value of a unicast source address, of a port on the containing chassis. **if-name:** Represents a chassis identifier based on the value of ifName object for an interface on the containing chassis. **Local**: Represents a chassis identifier based on a locally defined value. **Default**: if-alias
[no] lldp tlv-select dot1tlv {[port-vlan-id] [protocol-vlan-id {all |<vlan-id>}] [vlan-name {all | <vlan-id>}]}	This command performs dot1 TLV configuration while transmitting the LLDP frames to the particular port apart from the basic settings. The no form of the command disables the transmission of dot1 TLV types on a port. **port-vlan-id:** Specifies the VLAN ID of the port that uniquely identifies a specific VLAN. This VLAN ID is associated with a specific group of protocols for the specific port. **protocol-vlan-id:** Specifies the protocol ID that represents a specific group of protocols that are associated together when assigning a VID to a frame. This group ID is associated with the specific port. **vlan-name:** Specifies the administratively assigned string, which is used to identify the VLAN.
[no] lldp tlv-select dot3tlv { [macphy-config] [link-aggregation] [max-framesize] }	This command performs dot3 TLV configuration while transmitting the LLDP frames to the particular port apart from the basic settings. The no form of the command disables the transmission of dot3 TLV types on a port. **macphy-config:** Configures the physical MAC address of the TLV. **link-aggregation:** Configures the link aggregation protocol statistics for each port on the device. **max-framesize:** Configures the maximum frame size of the TLV.

Command	Description
[no] debug lldp [{all | [init-shut] [mgmt] [data-path] [ctrl] [pkt-dump] [resource] [all-fail] [buf] [neigh-add] [neigh-del] [neigh-updt] [neigh-drop] [neighageout] [critical][tlv {all | [chassis-id][port-id] [ttl] [port-descr] [sysname] [sys-descr] [sys-capab] [mgmt-addr] [port-vlan] [ppvlan] [vlan-name] [proto-id] [mac-phy] [pwr-mdi] [lagg] [max-frame]}] [redundancy]}]	This command specifies debug level for LLDP module. The no form of the command disables debug option for LLDP module. **All:** Generates debug statements for all traces **init-shut:** Generates debug statements for init and shutdown traces. This trace is generated on failed initialization and shutting down of LLDP related entries. **Mgmt**: Generates debug statements for management traces. This trace is generated during failure in configuration of any of the LLDP features. **data-path**: Generates debug statements for data path traces. This trace is generated during failure in packet processing. **Ctrl**: Generates debug statements for control path traces. This trace is generated during failure in modification or retrieving of LLDP entries pkt-dump - Generates debug statements for packet dump traces. This trace is currently not used in LLDP module. **Resource**: Generates debug statements for OS resource related traces. This trace is generated during failure in message queues. **all-fail**: Generates debug statements for all failure traces of the above mentioned traces **buf**: Generates debug statements for LLDP buffer related traces. This trace is currently not used in LLDP neigh-add - Generates debug statements for add SEM. **neigh-del**: Generates debug statements for delete SEM. **neigh-updt**: Generates debug statements for update SEM. **neigh-drop**: Generates debug statements for drop SEM. **neigh-ageout**: Generates debug statements for ageout SEM. **Critica**l: Generates debug statements for critical SEM. **tlv all**: Generates debug statements for all TLV traces **tlv chassis-id**: Generates debug statements for chassis-id TLV traces **tlv port-id**: Generates debug statements for port-id TLV trace **tlv ttl**: Generates debug statements for TTL TLV trace **tlv port-descr**: Generates debug statements for the port description TLV traces. **tlv sys-name**: Generates debug statements for the system name TLV traces **tlv sys-descr**: Generates debug statements for system description TLV traces **tlv sys-capab**: Generates debug statements for system capabilities TLV traces **tlv mgmt-addr**: Generates debug statements for management address TLV traces **tlv port-vlan**: Generates debug statements for port-vlan TLV traces **tlv ppvlan**: Generates debug statements for port-protocol-vlan TLV traces **tlv vlan-name**: Generates debug statements for vlan-name TLV traces **tlv proto-id**: Generates debug statements for protocol-id TLV traces **tlv mac-phy**: Generates debug statements for MAC or PHY TLV traces **tlv pwr-mdi**: Generates debug statements for power-through-MDI TLV traces **tlv lag**: Generates debug statements for link aggregation TLV traces **tlv max-frame**: Generates debug statements for maximum frame size TLV traces **redundancy**: Generates the debug statements for the LLDP redundancy module.
show lldp	This command displays LLDP global configuration details to initialize on an interface
show lldp interface [<interface-type> <interface-id>]	This command displays the information about interfaces where LLDP is enabled . **interface-type**: Displays the information about the specified type of interface. The interface can be: fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer upto 100 Megabits per second. gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second. extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links. i-lan / internal-lan – Internal LAN created on a bridge per IEEE 802.1ap. port-channel – Logical interface that represents an aggregator which contains several ports aggregated together. **interface-id**: Displays the information about the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1. Only i-lan or port-channel ID is provided, for interface types i-lan and port-channel. For example: 1 represents i-lan and port-channel ID.

Command	Description
show lldp neighbors [chassis-id <string(255)> port-id <string(255)>] [<interface-type> <interface-id>][detail]	This command displays information about neighbors on an interface or all interfaces. **chassis-id**: Configures the chassis identifier string. **port-id**: Configures the port number that represents the concerned aggregation port **interface-type**: Displays information about neighbors for the specified type of interface. The interface can be: fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer upto 100 Megabits per second. gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second. extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links. i-lan / internal-lan – Internal LAN created on a bridge per IEEE 802.1ap. port-channel – Logical interface that represents an aggregator which contains several ports aggregated together. **interface-id**: Displays information about neighbors for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1. Only i-lan or port-channel ID is provided, for interface types i-lan and port-channel. For example: 1 represents ilan and port-channel ID. **Detail**: Displays the information obtained from all the received TLVs.
show lldp traffic [<iftype> <ifnum>]	This command displays LLDP counters on all interfaces or on a specific interface. This includes the following: Total Frames Out Total Entries Aged Total Frames In Total Frames Received In Error Total Frames Discarded Total TLVS Unrecognized Total TLVs Discarded **Iftype**: Displays the LLDP counters for specified type of interface. The interface can be: fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer upto 100 Megabits per second. gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second. extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links. i-lan / internal-lan – Internal LAN created on a bridge per IEEE 802.1ap. port-channel – Logical interface that represents an aggregator which contains several ports aggregated together. **Ifnum**: Displays the LLDP counters for specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1. Only i-lan or port-channel ID is provided, for interface types i-lan and port-channel. For example: 1 represents ilan and port-channel ID

Command	Description
show lldp local {[<interface-type> <interface-id>] | [mgmt-addr]}	This command displays the current switch information that will be used to populate outbound LLDP advertisements for a specific interface or all interfaces. **Interfacetype**: Displays the current switch information for the specified type of interface. The interface can be: fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer upto 100 Megabits per second. gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second. extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links. i-lan / internal-lan – Internal LAN created on a bridge per IEE E 802.1ap. port-channel – Logical interface that represents an aggregator which contains several ports aggregated together **interface-id**: Displays the current switch information for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1. Only i-lan or port-channel ID is provided, for interface types i-lan and port-channel. For example: 1 represents ilan and port-channel ID. **mgmt-addr:** All the management addresses configured in the system and Tx enabled ports
show lldp errors	This command displays the information about the errors such as memory allocation failures, queue overflows and table overflow.
show lldp statistics	This command displays the LLDP remote table statistics information.

Example 1

Following setup will demonstrate configuration and show outputs of lldp signaling.



S1 configuration

1. set system hostname (not mandatory)

```
set hostname S1
```

2. Enable lldp . timer values are example only

```
no shutdown lldp
set lldp enable
lldp transmit-interval 5
lldp notification-interval 5
```

3. set the chassis id option to be the system own mac address

```
lldp chassis-id-subtype mac-addr
```

4. set lldp at the local interface fastethernet 0/3

```
interface fastethernet 0/3
lldp transmit
lldp receive
lldp notification remote-table-chg
lldp tlv-select basic-tlv port-descr sys-name sys-descr sys-capab mgmt-addr all
```

4b. set the port-id to be the port own local name

```
lldp port-id-subtype if-name
end
```

5. show local lldp state at the interface

```
S1# show lldp local fastethernet 0/3
Port Id SubType                : Interface Name
Port Id                         : Slot0/3
Port Description               : Ethernet Interface Port 03
Enabled Tx Tlvs                : Port Description, System Name,
                                    System Description, System Capability,
                                    Management Address, Port Vlan
Extended 802.1 TLV Info
-Port VLAN Id                  : 1
-Vlan Name
Vlan Id         Vlan Name                          TxStatus
-------         ---------                         --------
1                                                   Disabled
-------------------------------------------------------------
S1#
```

S2 configuration

1. set system hostname (not mandatory)

```
set hostname S2
```

2. enable lldp . timer values are example only

```
no shutdown lldp
set lldp enable
lldp transmit-interval 5
lldp notification-interval 5
```

3. set the chassis id option to be the system management IP address

```
lldp chassis-id-subtype nw-addr
```

4. set lldp at the local interface fastethernet 0/1

```
interface fastethernet 0/1
lldp transmit
lldp receive
lldp notification remote-table-chg
lldp tlv-select basic-tlv port-descr sys-name sys-descr sys-capab mgmt-addr all
```

4b. set the port-id to be the port alias

```
lldp port-id-subtype if-alias
alias S2P3
end
```

5. show local lldp state at the interface

```
S2# show lldp local fastethernet 0/1
Port Id SubType                : Interface Alias
Port Id                         : S2P3
Port Description               : Ethernet Interface Port 01
Enabled Tx Tlvs                : Port Description, System Name,
                                    System Description, System Capability,
                                    Management Address
Extended 802.1 TLV Info
-Port VLAN Id                  : 1
```

```
-Vlan Name
Vlan Id         Vlan Name                              TxStatus
-------         ---------                             --------
1                                                       Disabled
------------------------------------------------------------
```

Show LLDP

1. Following is the LLDP readings of switch 2 as received at switch 1

```
S1# show lldp neighbors

Capability Codes    :
(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device,
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Chassis ID            Local Intf     Hold-time   Capability       Port Id
----------            ----------     ---------   ----------       -------
172.18.212.51         Fa0/3          20          B,R              S2P3

Total Entries Displayed : 1
S1#
```

2. Following is the LLDP readings of switch 1 as received at switch 2

```
S2# show lldp neighbors

Capability Codes    :
(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device,
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Chassis ID            Local Intf     Hold-time   Capability       Port Id
----------            ----------     ---------   ----------       -------
00:22:3b:0e:09:08     Fa0/1          20          B,R              Slot0/3

Total Entries Displayed : 1
```

Example 2

Based on same setup, following changes in lldp configuration are made at switch 1 in order to show the updated state seen at switch 2.

S1 configuration

1. set the chassis id option to be a chosen text “S1”

```
lldp chassis-id-subtype local S1
```

2. Add the interface 0/3 to vlan id 5 (vlan name is www)

```
vlan 5
ports fastethernet 0/3 name www
end
```

3. set lldp at the local interface fastethernet 0/3

```
interface fastethernet 0/3
lldp transmit
lldp receive
lldp notification remote-table-chg
lldp tlv-select basic-tlv port-descr sys-name sys-descr sys-capab mgmt-addr all
```

3.b set the port-id to be the port alias

```
lldp port-id-subtype if-alias
alias S1P1
```

3.c activate lldp for vlan id

```
lldp tlv-select dot1tlv port-vlan-id
lldp tlv-select dot1tlv vlan-name 5
end
```

4. show local lldp state at the interface

```
S1# show lldp local fastethernet 0/3
Port Id SubType                 : Interface Alias
Port Id                          : S1P1
Port Description                : Ethernet Interface Port 03
Enabled Tx Tlvs                 : Port Description, System Name,
                                    System Description, System Capability,
                                    Management Address, Port VlanExtended 802.1 TLV Info
-Port VLAN Id                   : 1
Vlan Id         Vlan Name                          TxStatus
-------         ---------                          --------
1                                                    Disabled
5                www                                 Enabled
```

Show LLDP

1. Following is the updated LLDP readings of switch 1 as received at switch 2

```
S2# show lldp neighbors

Capability Codes    :
(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device,
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Chassis ID            Local Intf     Hold-time    Capability       Port Id
----------            ----------     ---------    ----------       -------
S1                     Fa0/1          20            B,R              S1P1

Total Entries Displayed : 1
```

2. Detailed readings

```
S2# show lldp neighbors detail

Capability Codes   :
(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device,
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Chassis Id SubType             : Local
Chassis Id                      : S1
Port Id SubType                : Interface Alias
Port Id                         : S1P1
Port Description               : Ethernet Interface Port 03
System Name                     : Linux Router Ver 1.0
System Desc                     : Switch software version 3.2
Local Intf                      : Fa0/1
Time Remaining                  : 18 Seconds
System Capabilities Supported : B,R
System Capabilities Enabled   : B,R
Management Addresses           :
IfId SubType Address                          OID
---- ------- -------                         ---
49   IPv4    172.18.212.53                   1 3 6 1 2 1 2 2 1 1

Extended 802.1 TLV Info
-Vlan Name
Vlan Id         Vlan Name
-------         ---------
5               www
------------------------------------------------------------

Total Entries Displayed : 1
S2#
```

1588v2 Precision Time Protocol

IEEE 1588 protocol is designated to synchronize real-time clocks in a distributed Ethernet network.

The RLGE2FE16R support the 1588v2 protocol with following implementation.

- » End to end mode Transparent clock (TC), aka Telecom profile. The switch stamps the sync message at ingress and egress and computes the residence time
- » One step (the sync timestamp is carried in the sync message and no follow-up message is sent)
- » Hardware time stamping
- » No PPS limitation of 1588 sync messages
- » No limitation of number of domains
- » Supported at the 10/100 RJ45 copper ports only

1588 Commands Hierarchy

+root

+config terminal

- set ptp enable

- set ptp disable

- set ptp default-params

- set ptp e2e local-port fastethernet <ifnum>

- set ptp e2e remote-port fastethernet <ifnum>

- set ptp switch-count ge-ge (0,<0-100>)

- set ptp switch-count ge-fe (0,<0-100>)

- set ptp switch-count fe-fe (0,<0-100>)

- set ptp switch-count fe-ge (0,<0-100>)

- set ptp switch-count rf-fe-fe (1,<0-100>)

- set ptp network-load (30%,<0-100>)

- set ptp avg-packet-size (200 bytes,<64-1500>)

- set ptp fix-local {positive | negative} (0 microsec,<0-5000>)

- show ptp e2e ports

- show ptp details

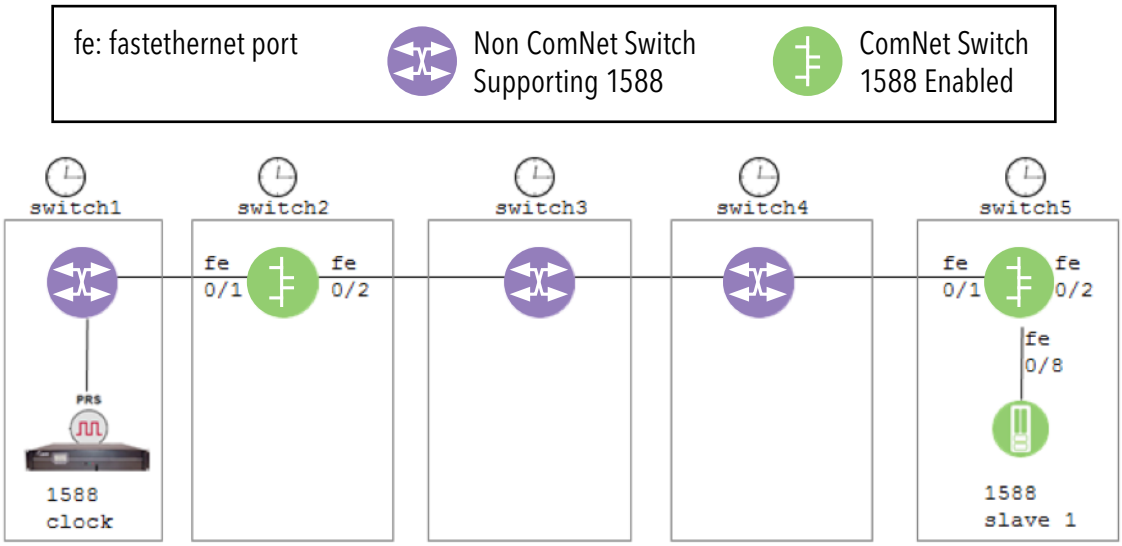
1588 Commands Descriptions

Command	Description
config terminal	Enters the Configuration mode
set ptp enable	Enable time stamp correction
set ptp disable	disable time stamp correction
set ptp default-params	Set the ptp properties to their default state
set ptp e2e local-port	Define via which physical port of the unit the local traffic is coming through. The port may be one of the fastethernet ports.
set ptp e2e remote-port	Define at which physical port of the unit the remote 1588 device is connected at. The port may be one of the fastethernet ports.
set ptp switch-count	These parameters describe the Ethernet physical topology between the local and remote. The objective of these is to determine the total amount of Ethernet switches (which do not support 1588) and calculate the correction needed for the time stamp for the RLGE2FE16R to make. The calculation takes into account the number of switches and their respective Ethernet port types used for the interconnection. **ge-ge <0-100>**: the number of switches (non RLGE2FE16R), which are: connected between the local and remote do not support 1588 at which the connection towards the local is with a gigabit port at which the connection towards the remote is with a gigabit port. default: 0 **ge-fe <0-100>**: the number of switches (non RLGE2FE16R), which are: connected between the local and remote do not support 1588 at which the connection towards the local is with a gigabit port at which the connection towards the remote is with a fastethernet port. default: 0 **fe-fe <0-100>**: the number of switches (non RLGE2FE16R), which are: connected between the local and remote do not support 1588 at which the connection towards the local is with a fastethernet port at which the connection towards the remote is with a fastethernet port. default: 0 **fe-ge <0-100>**: the number of switches (non RLGE2FE16R), which are: connected between the local and remote do not support 1588 at which the connection towards the local is with a fastethernet gigabit port at which the connection towards the remote is with a gigabit port. default: 0 **rf-fe-fe <1-100>**: the number of RLGE2FE16R switches which are: connected between the local and remote at which the connection towards the local is with a fastethernet port at which the connection towards the remote is with a fastethernet port. default: 1
set ptp network-load	The network typical load may influence the time correction calculation. Enter here the network typical load in %. Default: 30.
set ptp avg-packet-size	The size of the Ethernet packets may influence the time correction calculation. Enter here the network typical mtu <64-1500>. Default: 200.
set ptp fix-local	This field allow an additional time correction coefficient of plus/minus 0-5000 micro seconds.
show ptp e2e ports	Show output of the local/remote port assignment
show ptp details	Show output of the detailed ptp settings

Example 1

Following setup will demonstrate configuration of 1588 at the RLGE2FE16R switches. The setup shows an Ethernet network at which all the switches are supporting 1588.

Setup drawing



Configuration

Switch2 configuration

1. set system hostname (not mandatory)

```
set host-name switch2
```

2. Enable 1588 ptp

```
config
set ptp enable
```

3. Determine the local port and remote port

```
set ptp e2e local-port fastethernet 0/1
set ptp e2e remote-port fastethernet 0/2
```

4. Calculate the switch count from the local

```
set ptp switch-count rf-fe-fe 1 ;note- calculate its own time correction
end
write startup-cfg
switch2# show ptp e2e ports
-------------------
  PTP Master Ports
-------------------
Fa0/1

-------------------
  PTP Slave Ports
-------------------
Fa0/2
Fa0/8

switch2# show ptp details
---------------------------------
           PTP Details
            Disabled
---------------------------------
Switch count GE-GE     :    0
Switch count GE-FE     :    0
Switch count FE-FE     :    0
Switch count FE-GE     :    0
Switch count RF-FE-FE :    1
Network load           :    30
Average packet size    :    200

Fix for local         :    0
Total offset local    :    200
Total offset remote     :    200
switch2#
```

Switch5 configuration

1. set system hostname (not mandatory)

```
set host-name switch5
```

2. Enable 1588 ptp

```
config
set ptp enable
```

3. Determine the local port and remote port

```
set ptp e2e local-port fastethernet 0/1
set ptp e2e remote-port fastethernet 0/2
set ptp e2e remote-port fastethernet 0/8
```

4. Calculate the switch count from the local

```
set ptp switch-count rf-fe-fe 1 ;note- calculate its own time correction
end
write startup-cfg
```

```
switch5# show ptp e2e ports
-------------------
  PTP Master Ports
-------------------
Fa0/1

-------------------
  PTP Slave Ports
-------------------
Fa0/2
Fa0/8

switch5# show ptp details
--------------------------------
           PTP Details
            Disabled
--------------------------------
Switch count GE-GE    :    0
Switch count GE-FE    :    0
```

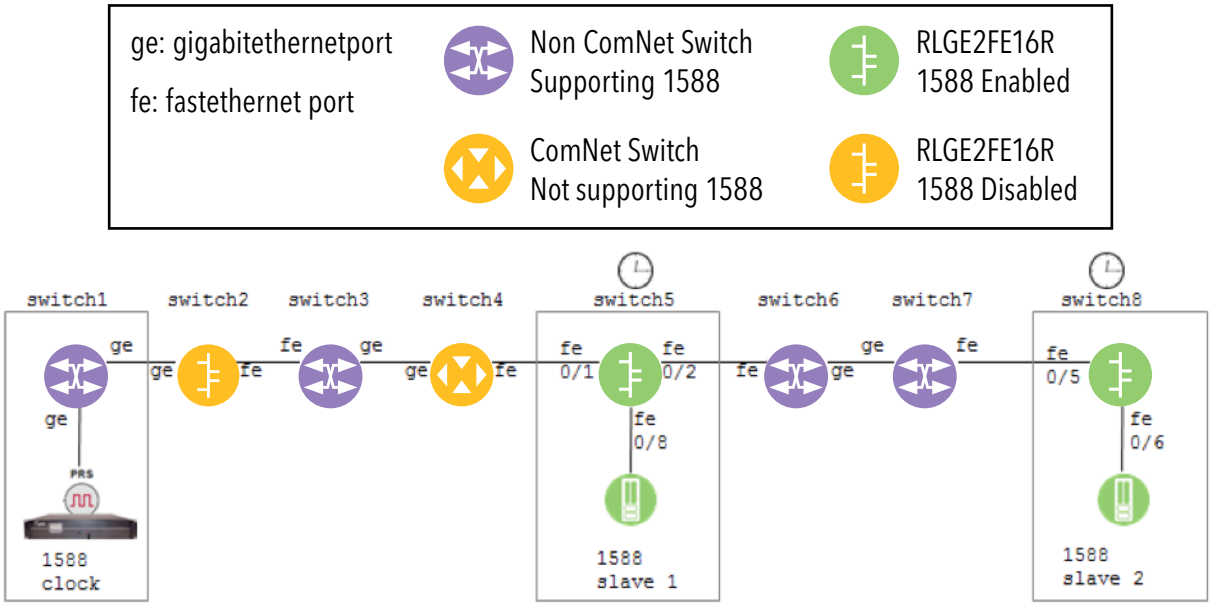
```
Switch count FE-FE     :    0
Switch count FE-GE     :    0
Switch count RF-FE-FE  :    1
Network load           :    30
Average packet size    :    200
Fix for local          :    0
Total offset local     :    200
Total offset remote    :    200
switch5#
```

Example 2

Following setup will demonstrate configuration of 1588 at the RLGE2FE16R switches.

The setup shows an Ethernet network at which some of the switches are supporting 1588 and some are not. Switch5 is a RLGE2FE16R at which 1588 is enabled and has a local remote connected to it. Switch5 will calculate a time correction compensating the time drift which occurred to the local signal over switch1-switch4. Switch8 is as well a RLGE2FE16R at which 1588 is enabled and a local remote is connected.Switch8 needs to correct the time drift accumulated between switch5 (port 0/2) and switch8 (port 0/6).

Setup drawing



switch1: the local is connected at a gigabitethernet port (ge) and the remotes are available as well via a ge port (connected via 'switch2'). This condition is described as ge-ge.

switch2: the local is connected at a ge port (connected with ge port to 'switch1') and the remotes are available via a fe port (connected via 'switch3'). This condition is described as ge-fe.

switch3: the local is connected at a fe port (connected with fe port to 'switch2') and the remotes are available via a ge port (connected via 'switch4'). This condition is described as fe-ge.

switch4: ge-fe.

switch5: is a RLGE2FE16R at which 1588 is enabled. The RLGE2FE16R supports 1588 only at its copper (fe) ports and thus this switch settings are rf-fe-fe where 'rf' represents ComNet RLGE2FE16R.

switch6: fe-ge.

switch7: ge-fe.

switch8: is a RLGE2FE16R at which 1588 is enabled. The RLGE2FE16R supports 1588 only at its copper (fe) ports and thus this switch settings are rf-fe-fe where 'rf' represents ComNet RLGE2FE16R.

Configuration

Switch5 configuration

5. set system hostname (not mandatory)

```
set host-name switch5
```

6. Enable 1588 ptp

```
config
set ptp enable
```

7. Determine the local port and remote port

```
set ptp e2e local-port fastethernet 0/1
set ptp e2e remote-port fastethernet 0/2
set ptp e2e remote-port fastethernet 0/8
```

8. Calculate the switch count from the local

```
set ptp switch-count ge-ge 1    ;note- calculate 'switch1'
set ptp switch-count ge-fe 2    ;note- calculate 'switch2' & 'switch2'
set ptp switch-count fe-ge 1    ;note- calculate 'switch3'
set ptp switch-count rf-fe-fe 1 ;note- calculate 'switch5'
end
write startup-cfg
switch5# show ptp e2e ports
-------------------
  PTP Master Ports
-------------------
Fa0/1
-------------------
```

```
  PTP Slave Ports
-------------------
Fa0/2
Fa0/8
switch5# show ptp details
--------------------------------
           PTP Details
            Enabled
--------------------------------
Switch count GE-GE     :    1
Switch count GE-FE     :    2
Switch count FE-FE     :    0
Switch count FE-GE     :    1
Switch count RF-FE-FE :    1
Network load           :    30
Average packet size    :    200
Fix for local          :    0
Total offset local    :    34957
Total offset remote     :    3
```

Switch8 configuration

1. set system hostname (not mandatory)

```
set host-name switch8
```

2. Enable 1588 ptp

```
config
set ptp enable
```

3. Determine the local port and remote port

```
set ptp e2e local-port fastethernet 0/5
set ptp e2e remote-port fastethernet 0/6
```

4. Calculate the switch count from the switch5 as the local clock is corrected by it.

```
set ptp switch-count fe-ge 1    ;note- calculate 'switch6'
set ptp switch-count ge-fe 1    ;note- calculate 'switch7'
set ptp switch-count rf-fe-fe 1 ;note- calculate 'switch8'
end
write startup-cfg
```

OAM CFM

The Connectivity Fault Management provides the capabilities useful for detecting, verifying and isolating connectivity failures in Virtual Bridged Local Area Networks. These capabilities are used in network operated by multiple independent organizations, each with restricted access to each other's equipment. In general, the Network Administrator is informed about the failure in the connection based on the Continuity Check Messages reception or by the User It initiates the Loop Back or Link Trace, to quickly determine and isolate the fault condition.

The following is the order in which the Ethernet Connectivity Fault Management elements must be configured:

» Domain at the same level as the MEP to be configured.

» Service within the domain (Maintenance Association).

» If a Service (Maintenance Association) is to be associated with more than one

» Vlan-id, then its Primary VLAN ID must be mapped to all the associated VLAN

» Ids with the command Ethernet cfm associate vlan-id

» primary-vlan-id

» Ma Mep List with MepId of the MEP

CFM Command Hierarchy

+root

+ config terminal

+ ethernet cfm domain name <name> level <level-id> [format {}]

- service name <name> [format] [icc <code> [{vlan <vlan-id> | service-instance <instance>] [mip-creationcriteria{}] [sender-id permission {}]

- set mip-creation-criteria {none | default | explicit}

- set sender-id-permission {}

- ethernet cfm mep { domain <name> | level <0-7>} [inward] mpid <id> [{service <name>| vlan <id> | service-instance <integer>}][active]

- ethernet cfm mip {domain <domain-name> | level <level-id (0-7)>} vlan <vlan-id (1-4094)> [active]

- [no] ethernet cfm start

- [no] ethernet cfm enable

- [no] ethernet cfm cc {domain <name> | level <>} [vlan{<id> | vlan-list} | [interval {}] [role{}]

- [no] ethernet cfm cc enable {domain <domain-name> | level <a,b,c-d>} [vlan <a,b,c-d> | service-instance <integer(<>]

- [no] ethernet cfm associate vlan-id <a.b,c-d> primary-vlan-id <id>

- [no] mep crosscheck mpid <id> [{vlan <id> | service-instance <id>}]

- [no] ethernet cfm traceroute cache

- [no] ethernet cfm mip ccm-database

- traceroute ethernet {mpid <id> | mac <>} {domain <name>| level <id>} [service <name> | vlan <id>] | service-instance <id>] [interface <type> <number>] [direction {}] [time-tolive <ttl>] [timeout <msec>] [use-mip-ccm-db]

- show ethernet cfm domain [brief]

- show ethernet cfm service [brief]

- show ethernet cfm maintenance-point local [mep | mip] [interface [<type> <number>] |[domain <name>] | [level <id>]

- show ethernet cfm maintenance-points remote detail {mpid <id>|mac<> }[domain <name> | level <id> [{service <name> | unaware | vlan <id> | service-instance <id>}]]

- show ethernet cfm traceroute-cache

CFM Commands Descriptions

Command	Description
config terminal	Enters the Configuration mode
ethernet cfm	
domain	
format	Sets the format of the CFM maintenance domain. The options are: dns-like-name – Configures the domain name like string. Globally unique text string derived from a DNS name. this option of format should be chosen only along with Y.1731. mac-addr – Configures the MAC address plus 2- octet (unsigned) integer. char-string – Configures the RFC2579 display string. The character codes 0-31 (decimal) are not used.
Name	Creates a domain with a specified name. Character string has a maximum limit of 20 characters.
Level	Sets a level for the created domain.at which the maintenance domain is defined. This integer value ranges between 0 and 7.
service	This command configures the service (Maintenance Association) at the specified service-instance or VLAN.
name	Identifies the association. Maximum limit of the Character string is up to 20 characters
Format	Configures the format of the service. The options are: **primary-vid** - Specifies Primary VLAN ID. 1 to 4096. The vlan must be created beforehand. **char-string** - Specifies RFC2579 DisplayString, except that the character codes 0-31 (decimal) are not used. String with maximum size 39. **unsigned-int16** - 0 to 65535. **icc** – Specifies ITU-Carrier Code

Command	Description
Icc	Configures the ITU-Carrier Code. String with maximum size 40. User can configure ICC only when Y.1731 is enabled.
Umc	Configures the Unique Maintenance Entity Group Identifier Code. User can configure UMC only when Y.1731 is enabled.
vlan	Configures the primary VLAN ID which the Maintenance Association must be associated This is a unique value that represents the specific VLAN created / to be created. Value ranges between 1 and 4094. when the service vlan command is executed: Maintenance Association Name must be unique within a Maintenance Domain. More than one VLAN can be associated with the Maintenance Association through the command ethernet cfm associate vlan-id primary-vlan-id. Primary VLAN ID associated with a Maintenance association is not assigned to any other Maintenance Association at the same level. The same Maintenance Association Name can be used, if the Maintenance Association exists in different domain. All the MEPs related to the Maintenance Association must be removed,before removing that Maintenance Association.
Service instance	Indicates a service-instance for the configuration. This value ranges between 256 and 16777214
mip-creationcriteria	Indicates, whether the management entity is able to create MHF for this Maintenance Association. The options are: none | default | explicit | defer
sender-id-permission	Sets the value to control the Sender ID TLV, to be transmitted in CFM PDUs by MHFs associated with this Maintenance Association. The options are: none | chassis | manage | chassis-mgt-address | defer
mep	This command configures the MEP (Maintenance End Point) for an service-instance . Sets an interface as a domain boundary (edge), defines it as a MEP (Maintenance End Point), sets direction for the MEP and sets the operational status of the MEP. The no form of the command removes the MEP configuration from the interface. An active keyword is provided to enable or disable the MEP, if it is already configured. By default, MEP is disabled. For Vlan unaware MEP, Vlan is not to be specified. **domain** : Identifies the Maintenance Domain. The maximum length of the domain-name is 20. **level** : Maintenance Domain level for the MEP. This integer value ranges between zero and seven. **inward** : Specifies the direction. By default, outward is created, that is, down MEP. **mpid** : MEP identifier. This integer value ranges between 1 and 8191. **Service** : Indicates the service name. The maximum length of the service-name is 20. **Vlan** : VLAN ID. This value ranges between 1 and 4094. Following restrictions apply : - On a particular interface, only one MEP can be configured at particular level, VlanId and direction. - MPID has to be unique in a Maintenance Association. **Service instance** : Service instance identifier for which the MEP is defined. This is required only for the ISID aware MEP. This is applicable only for ports in PBB bridge mode. This value ranges between 256 and 16777214 (2^24-1). **Active** : Operational status of the MEP. By default, MEP will not be active.

Command	Description
mip	This command configures a Maintenance Intermediate Point (MIP) at the specified maintenance level and VLAN on an interface. An active keyword is provided to enable or disable the MIP, if it is already configured. **domain** : Identifies the Maintenance Domain. The maximum length of the domain-name is 20. **level** : Specifies the maintenance level at which the MIPs are defined. This integer value ranges between zero and seven. **Service** : Indicates the service name. The maximum length of the service-name is 20. **Vlan** : VLAN ID. This value ranges between 1 and 4094. Following restrictions apply : - There must not be any MP configured at an equal or higher MD Level at the same VLAN than the MIP to be configured. - Level with which MIP is to be created must be set corresponding to the - If the service (Maintenance Association) associated with the specified VLAN and level is configured in the system, with at least an up (inward) MEP then its MHF creation parameter must not be “none”. - If the above MA exists and its MHF criteria is “defer”, then its enclosing domain’s MHF creation parameter must be either “default or explicit”. It can be modified using the command set mip-creation-criteria. - If service (Maintenance Association) associated with the specified VLAN and level is not configured in the system, then the default MHF creation parameter must not be “none”. **Service instance** : Service instance for which the MIP is being defined. This value ranges between 256 and 16777214. **Active** : Specifies the MIP’s operational status. By default, MIP will be active.
set mip-creation-criteria	This command sets MIP creation criteria for a particular Maintenance Domain. MIP creation criteria is applicable only if Maintenance Domain’s underlying Maintenance Association ’s MIP creation criteria is “defer”.
set sender-id-permission	This command sets Sender ID permission for a particular Maintenance Domain. Sender ID permission criteria is applicable only if Maintenance Domain’s underlying Maintenance Association’s SenderID permission is “defer”. The following values are allowed: 1. none 2. chassis 3. manage 4. chassis-mgt-address
ethernet cfm start	This command starts an Ethernet connectivity fault Management (CFM), processing globally on the switch. The no form of the command shutdown an Ethernet CFM processing on the switch
ethernet cfm enable	This command enables a Connectivity Fault Management (CFM) processing globally on a device or on an interface. The no form of the command disables the CFM processing globally on a device or on an interface.

Command	Description
ethernet cfm cc	This command sets the parameters (that is, Interval and Role) for CCMs (Continuity Check Messages). The level and vlan identifies the service (Maintenance Association) to which the configuration applies. This command is used to set the parameters for CC transmission for a Maintenance Association, that is, for a particular level and for a particular VLAN. **domain** : Identifies the Maintenance Domain. The maximum length of the domain-name is 20. **level** : Specifies the maintenance level at which the MIPs are defined. This integer value ranges between zero and seven. **Service** : Indicates the service name. The maximum length of the service-name is 20. **Vlan id**: VLAN ID. This value ranges between 1 and 4094. **Vlan list**: Indicates a list of VLANs. **Service instance** : Indicates a service-instance for the configuration. This value ranges between 256 and 16777214. **interval** : The time between CCM transmissions. Options are: hundred-ms – 100 milliseconds one-sec – one second ten-sec – 10 seconds one-min – one minute ten-min – 10 minutes **role**: ETH-CC role to be performed. Options are: fault-management – ETH-CC is used for Fault Management. performance-monitoring – ETH-CC is used for Performance Monitoring. protection-switching – ETH-CC is used for Protection Switching. Default : fault management
ethernet cfm cc enable	This command enables the transmission of Continuity Check Messages (CCMs). The level and vlan identifies the Maintenance End Points (MEPs) to which the configuration applies. The no form of the command disables the transmission of CCMs. For the transmission of CCMs by the Vlan unaware MEPs, vlan is not to be specified.
ethernet cfm associate vlan-id	This command associates a VLAN ID or a list of VLAN IDs to a Primary VLAN. The no form of the command deletes the mapping of a VLAN ID or a list of VLAN IDs with a Primary VLAN. **Vlan id**: Identifies the VLAN to which the Primary VLAN ID must be associated. This value ranges between 1 and 4094. vlan-id <a,b,c-d> **Primary-Vlan-id**: Identifies the Primary VLAN ID. The range of the integer value is from 1 to 4094. Restrictions : * VLAN ID and Primary VLAN ID cannot be the same. * One VLAN cannot be associated with more than one Primary VLAN.
mep crosscheck mpid	This command statically defines an MEP (Maintenance End Point) in a Crosscheck List (MA-MEP List) within a Maintenance Association. The no form of the command deletes statically defined MEP from the Crosscheck List. Vlan/Service-Instance unaware MEP can be statically defined by not providing vlan/service-Instance. **mpid** : Identifies MEP. The mep-id value ranges from 1 to 8191. Service : Indicates the service name. The maximum length of the service-name is 20. **Vlan**: Identifies the Primary VLAN ID of service (Maintenance Association) with which remote MEP must be associated. Restrictions : - MEP Identifier must be unique within the service (Maintenance Association). **Service instance** : Identifies a service-instance in a Provider backbone bridge mode. This value ranges between 256 and 16777214.
ethernet cfm traceroute cache	This command enables caching of Ethernet Connectivity Fault Management (CFM) data learned through traceroute (Linktrace Replies) messages. The no form of the command disables caching.
ethernet cfm mip ccm-database	This command enables caching of Ethernet Connectivity Fault Management (CFM) data learned through the Continuity Check Messages (CCM). The no form of the command disables caching.

Command	Description
ethernet cfm loopback cache	This command enables loopback cache. The no form of the command disables loopback caching.
traceroute Ethernet	This command initiates Linktrace message by providing MEP identifier of the destination MEP (Maintenance End Point) or the MAC Address of the MEP or MIP. **Direction** : Specifies the direction of the MEP. inward – MEP faces in up direction on the bridge port. outward – MEP faces in down direction on the bridge port **Time-to-live** : 1-255 **timeout** : Deadline timeout(in milliseconds),before which the trace route reply must come. The value ranges from 10 to 10000 milliseconds.
show ethernet cfm domain	This command displays the information about all the CFM Maintenance Domains configured on a device.
show ethernet cfm service	This command displays the information about all the CFM Maintenance Associations configured on a device.
show ethernet cfm maintenance-point	This command displays the details of all the maintenance points (Maintenance End Point (MEP) or Maintenance Intermediate Point (MIP)) configured on a device.
show ethernet cfm maintenance-points remote detail	This command displays the information about the remote maintenance points in continuity check database.
show ethernet cfm traceroute-cache	This command displays the contents of the traceroute cache.

ERPS

ERPS (Ethernet Ring Protection Switching) is a portable software implementation that conforms to the ITU-T Standard G.8032/Y.1344 (06/2008) and its amendment ITU-T Standard G.8032/Y.1344 Amendment 1 (04/2009). The ERPS module ensures that there are no loops formed at the Ethernet layer.

ERPS modules provides support for the following:

» Forced switch and Manual switch

» Revertive and Non-revertive mode of operation

» Multi-board environment

ERPS provides highly reliable and stable protection mechanism in ring networks; and provides mechanism to avoid formation of loops, which would fatally affect network operation and service availability. Each ring node is connected to adjacent nodes participating in the same ring, using two independent links. A ring link is bounded by two adjacent nodes and a port for a ring link is called a ring port. The minimum number of nodes on a ring is two.

The fundamentals of this ring protection switching architecture are:

» Principle of loop avoidance

» Utilization of learning, forwarding, and address table mechanisms of Ethernet technology

Loop avoidance in the ring is achieved by guaranteeing that, at any time, traffic may flow on all but one of the ring links. This particular link is called the ring protection link (RPL), and under normal conditions this link is blocked, i.e., not used for traffic. One designated node, the RPL owner, is responsible to block traffic over the RPL.

ERPS Commands Hierarchy

+root

+config terminal

+switch [default]

-[no] shutdown aps ring [switch]

-[no] aps ring enable

+[no] aps ring group <group-id>

- [no] aps group active

- aps group name <group_name> ring group <group_id>

- aps working <interface_type> <interface_id> [<interface_type> <interface_id>] vlan <vlan_id>

-[no] aps protect <interface_type> <interface_id>

-[no] aps blockport-on-virtualchannel-recovery

- aps watchdog id <0,3-255> {enable| disable}

- aps working meg <meg-id(1-4294967295)> me <me-id(1-4294967295)> mep <mep-id(1-8191)> meg <meg-id(1-4294967295)> me <me-id(1-4294967295)> mep <mep-id(1-8191)>

-[no] aps {force | manual} <interface-type> <interface-id>

-[no] aps revert [wtr] <timer_value> [{milliseconds | seconds | minutes | hours}]

- aps timers [periodic <integer> {milliseconds | seconds | minutes | hours}][hold-off <integer> {milliseconds | seconds | minutes | hours}] [guard <integer> {milliseconds | seconds | minutes | hours}]

-[no] aps propagate-tc {[status {enable | disable}]} [ring-ids < ringid-range>]

-aps map vlan-group <short(0-64)>

-aps mac-id {<integer(1-255)>}

-aps protection-type{port-based|service-based}

-aps main ring id <main-ring-id>

-aps virtual channel recovery periodic time <timer_value> [{milliseconds |seconds | minutes | hours}]

-aps compatible version {v1 | v2}

-[no] aps neighbor <interface_type> <interface_id>

-aps wtb <integer> [{milliseconds | seconds | minutes | hours}]

-aps clear

-[no] aps next-neighbor <interface_type> <interface_id>

-aps subring-without-virtualchannel {enable | disable}

-aps multiple-failure {disabled | primary | secondary}

-aps interconnection-node {none | primary | secondary}

-aps ring {[port1 {local | remote}] [port2 {local | remote}]}

-[no]aps distribute <interface_type> <interface_id>

- [no] aps ring map vlan-group <short(0-64)> [{add|remove}] <port_list>

- aps ring vlan-group-manager {erps | mstp}

- [no] aps ring notification enable

-clear aps ring statistics [ring group <group-id>]

- [no] debug aps ring {[all] [critical] [start-shut] [mgmt] [ctrl] [pkt-dump][resource] [all-fail] [buff] [switch <string (32)>]}

-show aps ring global info [switch <context_name>]

- show aps ring [group <group_id>] [{configuration | statistics | timers }] [switch <context_ name>]

-show aps ring vlan-group [<short(0-64)>]

- show running-config erps

- show running-config ecfm

ERPS Commands Descriptions

Command	Description
config terminal	Enters the Configuration mode
Switch [default]	Creates a virtual context.
[no] shutdown aps ring [switch]	This command shuts down the ERPS functionality in the virtual switch. The no form of the command starts the ERPS functionality in the virtual switch. When the ERPS functionality is started, ERPS module is started in the context and the module status is initialized to disable. When the ERPS functionality is shutdown (without the switch string), ERPS module is shutdown in the context and all the ring configurations in the context are deleted. When the command is used with the switch string, then the ERPS context information in the switch is also deleted. Default: ERPS functionality is shutdown.
[no] aps ring enable	This command enables the ERPS functionality. The no form of the command disables the ERPS functionality. When the ERPS functionality is enabled, ERPS module is enabled in the context and ERPS protocol starts running on all the rings configured in the context. When the ERPS functionality is disabled, ERPS module is disabled in the context and all the rings configured in the context become non-operational, that is, ERPS protocol does not run on the rings in the context. Defaults: ERPS functionality is disabled for all virtual contexts.
[no] aps ring group <group-id>	This command creates a ring entry in the ERPS and enters into the ring group configuration mode. The newly created ring entries are in inactive state. If the ring entry is already created, this command enters into the ring group configuration mode for that ring entry. All the ring group specific configurations are done in the ring group mode. These configurations include making the ring active, configuring the ring ports and R-APS VLAN ID for the ring and so on. The no form of the command deletes an already created ring entry. If the ring entry is not present, an error message Ring Entry is not present is displayed. **<group-id>**: Configures the unique numeric identifier of a ring within the context. This value ranges between 0 and 4294967295.
[no] aps group active	This command activates the given ring group. The no form of the command de-activates the given ring group. The ring group is created using the commands aps ring group or aps group name. Defaults: The ring group is inactive

Command	Description
aps group name <group_name> ring group <group_id>	This command creates the ring entry, configures the ring name for the given ring ID and enters into the ring group configuration mode. The newly created ring entries are in inactive state. If the ring entry is already created, this command configures the ring name and enters into the ring group configuration mode for that ring entry. All the ring group specific configurations are done in the ring group mode. These configurations include making the ring active, configuring the ring ports and R-APS VLAN ID for the ring and so on. **<group_name>**: Indicates the name of the ring. The maximum string size is 35.The group name is created by appending ring ID to the string ring. For example, group name for a ring with ID as 1 is ring1. **<group-id>**: Configures the unique numeric identifier of a ring within the context. This value ranges between 0 and 4294967295. Defaults: The group name will be constructed by appending ring ID to the string ring. For example, group name for a ring with ID as 1 will be ring1.
aps working <interface_type> <interface_id> [<interface_type> <interface_id>] vlan <vlan_id>	This command configures the ring ports and R-APS (Ring-Automatic Protection Switching) VLAN ID for the ring. **<interface_type>**: Sets the type of interface for ring ports of the ring. The interface type can be: fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second. gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links internal-lan – Internal LAN created on a bridge per IEEE 802.1ap. port-channel – Logical interface that represents an aggregator which contains several ports aggregated together. **<interface_id>**: Sets the ring ports of the ring. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than internal-lan and port-channel. Only i-lan or port-channel ID is provided, for interface types internal-lan and port-channel. **vlan <vlan_id>**: Configures the R-APS vlan for the ring. This is a unique value that represents the specific VLAN created. This value ranges from 1 to 4094. The configured VLAN should have been already activated. Defaults: Ring Ports - 0, 0 R-APS VLAN ID - 0
[no] aps protect <interface_type> <interface_id>	This command configures the given port as RPL (Ring Protection Link) port for the ring group and the ring node becomes the RPL owner. The no form of the command configures the given port as non-RPL port from the ring. If the given port is configured earlier as RPL port, then the node becomes non-RPL owner for this ring. **<interface_type>**: Sets the port as RPL port for the specified type of interface. The interface type can be: fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second. gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links. internal-lan – Internal LAN created on a bridge per IEEE 802.1ap. port-channel – Logical interface that represents an aggregator which contains several ports aggregated together. **<interface_id>**: Sets the specified port as RPL port for the ring. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than internal-lan and port-channel. Only i-lan or port-channel ID is provided, for interface types internal-lan and portchannel. Defaults: RPL Port - 0

Command	Description
[no] aps blockport-on-virtualchannel-recovery	This command allows blocking of sub-ring port to avoid temporary loop in the sub-ring, when the virtual channel of sub-ring recovers. The no form of the command disables blocking of sub-ring port, when virtual channel of sub-ring recovers. The blocking of subring port should be enabled only on one of the interconnected nodes of a subring. The subring will be temporarily cutoff from the rest of network, if blocking is allowed on both of the interconnected nodes. Defaults: Blocking of sub-ring port is disabled.
aps watchdog id	Applicable only when the unit is in a subring. Enables a watchdog mechanism to improve recovery from 'pending' state to idle state. The unit is to be given an id (numeric value 3-255) which represents its physical position in the subring. The first unit in the subring will given id 3, its directly connected unit in the subring will be 4 and such until the last unit in the subring which is connected to the main ring. The id influences a watchdog timer which initiates a shut/no-shut function (re-enable) at the ring ports. The RLGE2FE16R unit in the subring, which is the RPL-Owner of the subring should have this field set to 0. id: a value in a range of 3-255 indicating the unit position in the subring. Rpl-owner node should be set to 0. Enable | disable: enable/disable the watchdog.
aps working meg <meg-id(1-4294967295)> me <me-id(1-4294967295)> mep <mep-id(1-8191)> meg <meg-id(1-4294967295)> me <me-id(1-4294967295)> mep <mep-id(1-8191)>	This command associates the fault monitoring entities (Y.1731 specific) for each of the ring ports. **<meg-id(1-4294967295)>**: Configures the unique identifier of the Maintenance Entity Group for the working entity of the ring group. This value ranges between 1 and 4294967295. **<me-id(1-4294967295)>**: Configures the unique identifier of the Maintenance Entity for the working entity of the ring group. This value ranges between 1 and 4294967295. **<mep-id(1-4294967295)>**: Configures the unique identifier of the Maintenance Entity Group End Point that monitors the working entity of the ring group. This value ranges between 1 and 8191. Defaults: meg-id - 0 me-id - 0 mep-id - 0
[no] aps {force | manual} <interface-type> <interface-id>	This command applies the force/manual switch for the ring on the given ring port. The no form of the command clears the force / manual switch for the given ring. Force switch is of higher priority than the manual switch. Force switch will overwrite the manual switch configuration. Similarly, manual switch cannot be configured, when force switch is configured. Manual switch cannot be configured, if a link failure is present in the ring. Failure of the link in the ring clears the manual switch. **Force:** Applies the force switch for the ring and blocks on the port. **Manual**: Applies the manual switch for the ring and blocks on the port. **<interface_type>**: Sets the type of interface. The interface can be: fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second. gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links. internal-lan – Internal LAN created on a bridge per IEEE 802.1ap. port-channel – Logical interface that represents an aggregator which contains several ports aggregated together. **<interface_id>**: Sets the interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than internal-lan and port-channel. Only i-lan or port-channel ID is provided, for interface types internal-lan and port-channel. Defaults: None

Command	Description
[no] aps revert [wtr] <timer_value> [{milliseconds | seconds | minutes | hours}]	This command sets the operating mode of the ring group to revertive and sets the timer duration of wait-to-restore timer. The no form of the command resets the operating mode of the ring to non-revertive mode. When the manual option is given, then manual recovery method is configured. **wtr <timer_value>**: Configures the period for the Wait to restore timer. This configuration can be done, only if this ring is operating in the revertive mode of operation. In the revertive mode of operation, if it is configured with a value of '0', then the traffic is switched back to the working entity from the protection entity immediately upon recovery of the working entity from failure. The configured value of this timer is applicable only from the next start/re-start of the timer. The units of wait to restore time interval are: milliseconds – Configures the time interval in milliseconds. seconds – Configures the time interval in seconds. minutes – Configures the time interval in minutes. hours – Configures the time interval in hours. This value ranges between 0 and 86400000 milliseconds. **Manual:** Applies the manual recovery method of operation. When the link recovers, link ports remains in the blocked state until manual method is changed to auto by the administrator. Defaults: Operating mode of the protection group is set as revertive. wtr - 300000 milliseconds
aps timers [periodic <integer> {milliseconds | seconds | minutes | hours}] [hold-off <integer> {milliseconds | seconds | minutes | hours}] [guard <integer> {milliseconds | seconds | minutes | hours}]	This command configures the interval of the periodic timer, the hold-off timer and the guard timer. **periodic <integer>**: Configures time interval for the periodic transmission of Ring Automatic Protection Switching Protocol Data Units. Periodic timer is not valid for the first 3 R-APS PDU transmission, that is sent on any change of R-APS information. The configured value of this timer is applicable only from the next start/ re-start of the timer. The units of periodic time interval are: milliseconds – Configures the time interval in milliseconds. seconds – Configures the time interval in seconds. minutes – Configures the time interval in minutes. hours – Configures the time interval in hours. This value ranges between 1 and 3600000. **hold-off <integer>**: Configures the period for the hold-off timer of the ring. Hold-Off timer is started when a new defect is received for the ring. This defect will not be given as local SF to ERP control process until Hold-Off timer expires. When the Hold-Off timer expires and if a local defect still exists, it is given as local SF to the ERPS control process of this ring. The configured value of this timer is applicable only from the next start/re-start of the timer. The units of hold-off time interval are: milliseconds – Configures the time interval in milliseconds. seconds – Configures the time interval in seconds. minutes – Configures the time interval in minutes. hours – Configures the time interval in hours. This value ranges between 1 and 3600000. **guard <integer>**: Configures the period for the guard timer of the ring. This timer is required to prevent the reception of outdated R-APS messages. Guard timer is started on reception of local clear SF event. R-APS messages (except R-APS event messages) received during the running of the guard timer will be discarded. The configured value of this timer is applicable only from the next start/re-start of the timer. The units of guard time interval are: milliseconds – Configures the time interval in milliseconds. seconds – Configures the time interval in seconds. minutes – Configures the time interval in minutes. hours – Configures the time interval in hours. This value ranges between 1 and Defaults: periodic - 5000 milliseconds hold-off - 0 millisecond guard - 500 milliseconds3600000.

Command	Description
[no] aps propagate-tc {[status {enable | disable}]} [ring-ids < ringid-range>]	This command configures the propagate TC (Topology Change) flag for the ring and configures the IDs of rings, for which the TC should be propagated. The no form of the command removes the configured TC list for the rings. Ring ID of the ring (self ring ID) should not be configured in the TC ring ID list. **Status**: Specifies the status of the propagation of TC in the associated rings, whenever the flush FDB (Filtering Database) is triggered for the sub-ring. The options are: enable - Enables the propagation of TC in the associated rings, whenever the flush FDB is triggered for the sub-ring. disable - Disables the propagation of TC in the associated rings, whenever the flush FDB is triggered for the sub-ring. **ring-ids <ringid-range>**: Identifies the ring ID to which the TC should to be propagated upon FDB flush condition in the subring. Defaults: status - disable ring-ids - None
aps map vlan-group <short(0-64)>	This command associates a group of vlans to a ring. This value ranges between 0 and 64.
aps mac-id {<integer(1-255)>}	This command configures an id to be sent as last octet in the destination mac address of R-APS packets of the ring. This value ranges between 1 and 255.
aps protection-type{port-based | service-based}	This command configures the protection type for the ring. The type of protection being provided by this ring instance can be port-based or service-based. In a single virtual context one ring can run in port based protection mode and another ring can run in service based protection mode.
aps main ring id <main-ring-id>	This command configures the ID of the main Ring to which the sub-ring is connected. Upon configuration, the sub-ring gets added to the sub-ring list maintained by the Main Ring. Main ring gives the virtual channel status change indication to all the sub-rings present in its sub-ring list. This value must be configured on both the inter-connected nodes of the main ring. The main ring ID value ranges between 0 and 4294967295. When a main ring id of zero is configured, the sub-ring gets removed from the sub-ring list of the main ring. NOTE: ERPS functionality should be started and enabled in the virtual context, before executing this command.
aps virtual channel recovery periodic time <timer_value> [{milliseconds |seconds | minutes | hours}]	This command configures the time interval for which the periodic timer needs to be restarted for the subring, when the corresponding main ring indicates the virtual channel status change to this sub-ring and when the virtual channel of this sub-ring is in failed state. When one of the ring port of the main ring is in failed state, main ring indicates virtual channel status change indication to sub-ring. On getting this virtual channel status indication from the main ring, this subring restarts the periodic timer for this value. This is applicable only if the virtual channel is in failed state. Once the periodic timer expires, it gets restarted only for the normal periodic time. **periodic time <timer_value>**: Sets the time interval for the periodic timer. This value ranges between 0 and 3600000. **Milliseconds**: Configures the time interval in milliseconds. **Seconds**: Configures the time interval in seconds. **Minutes**: Configures the time interval in minutes. **Hours**: Configures the time interval in hours. Defaults: 5560 milliseconds
aps compatible version {v1 | v2}	This command configures the ring version for the ring entry in the ERPS. v1: Sets the ring version as v1. v2: Sets the ring version as v2. Defaults: V1

Command	Description
[no] aps neighbor <interface_type> <interface_id>	This command configures the given port as RPL neighbor port for the ring group so that the ring node becomes the RPL neighbor. This port should be one of the ring ports and adjacent to the RPL. The no form of this command is used to remove the RPL neighbor configuration from the ring. **<interface_type>**: Configures a port for the specified type of interface. The interface can be: fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer upto 100 Megabits per second. gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second. extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links. internal-lan – Internal LAN created on a bridge per IEEE 802.1ap. port-channel – Logical interface that represents an aggregator which contains several ports aggregated together. **<interface_id>**: Configures a port for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1. Only i-lan or port-channel ID is provided, for interface types i-lan and port-channel. For example: 1 represents i-lan and port-channel ID. NOTE: This command executes only if ERPS functionality is started and enabled in the virtual context.
aps wtb <integer> [{milliseconds | seconds | minutes | hours}]	This commans sets the timer duration of wait-to-block timer. The WTB timer is defined to be 5 seconds longer than the guard timer. **<integer>**: Configures the wtb timer value. The value ranges between 0 and 24 hours. **Milliseconds**: Sets the wtb timer in milliseconds. **Seconds**: Sets the wtb timer in seconds. **Minutes**: Sets the wtb timer in minutes. **Hours**: Sets the wtb timer in hours. Defaults: 5500 milliseconds
aps clear	This command uses to trigger clear operation to remove the switch commands (Force Switch/Manual Switch) or trigger reversion in revertive mode before the WTR or WTB timer expires or trigger reversion in non-revertive mode when the ERPS compatible version number is configured as 2.
[no] aps next-neighbor <interface_type> <interface_id>	This command configures the port as RPL next neighbor port for the ring group so that the ring node becomes the RPL next neighbor. This port should be one of the ring ports and adjacent to either RPL owner node or RPL neighbor node. The no form of this command removes the RPL next neighbor configuration from the ring. **<interface_type>**: Configures a port for the specified type of interface. The interface can be: fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer upto 100 Megabits per second. gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second. extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links. internal-lan – Internal LAN created on a bridge per IEEE 802.1ap. port-channel – Logical interface that represents an aggregator which contains several ports aggregated together. **<interface_id>**: Configures a port for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1. Only i-lan or port-channel ID is provided, for interface types i-lan and port-channel. For example: 1 represents i-lan and port-channel ID.

Command	Description
aps subring-without-virtualchannel {enable | disable}	This command allows blocking/ unblocking of ring R-APS channel in the sub-ring. **Enable**: Configures sub-ring to run without R-APS Virtual Channel and the traffic channel is blocked. **Disable**: Configures sub-ring to run with R-APS Virtual Channel and both the traffic channel and the R-APS channels are blocked. Default: Disable
aps multiple-failure {disabled | primary | secondary}	This command configures the multiple failure in interconnection node of the sub-ring. **Disabled**: Disables minimizing segmentation feature in Ring Node. Primary: Sets the multiple-failure in interconnection node as primary which is used by minimizing segmentation in interconnected rings feature. On detection of loss of connectivity between the two interconnection nodes, manual switch command will be applied in the interconnection node sub-ring port. On recovery of loss of connectivity between the two interconnection nodes, manual switch command is cleared in the interconnection node sub-ring port. **secondary**: Sets the multiple-failure in interconnection node as secondary which minimizes segmentation in interconnected rings. On detection of loss of connectivity between the two interconnection nodes, manual switch command will be applied in the interconnection node sub-ring port. On recovery of loss of connectivity between the two interconnection nodes, manual switch is cleared command in the interconnection node sub-ring port. Default: Disabled
aps interconnection-node {none | primary | secondary}	This command configures the interconnection node of the sub-ring to minimize segmentation in interconnected rings. **None**: Disables minimizing segmentation feature in the Ring Node. **Primary**: Sets the interconnection node of the sub-ring as primary which minimizes segmentation in interconnected rings. On detection of loss of connectivity between the two interconnection nodes, Manual switch command will be applied in the interconnection node sub-ring port. On recovery of loss of connectivity between the two interconnection nodes manual switch is cleared command in the interconnection node sub-ring port. **Secondary**: Sets the interconnection node of the sub-ring as secondary which minimizes segmentation in interconnected rings. On detection of loss of connectivity between the two interconnection nodes, Manual switch command will be applied in the interconnection node sub-ring port. On recovery of loss of connectivity between the two interconnection nodes, manual switch is cleared command in the interconnection node sub-ring port. Default: none
aps ring {[port1 {local | remote}] [port2 {local | remote}]}	This command configures the ring port1 or/and port2 as local or remote. **port1**: Configures the first ring port. The port type can be: local- Configures port 1 as local when port 1 is present in the local line card. remote- Configures port 1 as remote when port 1 is present in the remote line card. port2 - Configures the second ring port. The port type can be: local- Configures port 2 as local when port 2 is present in the local line card. remote- Configures port 2 as remote when port 2 is present in the remote line card. Defaults: Port1 – local Port2 – local

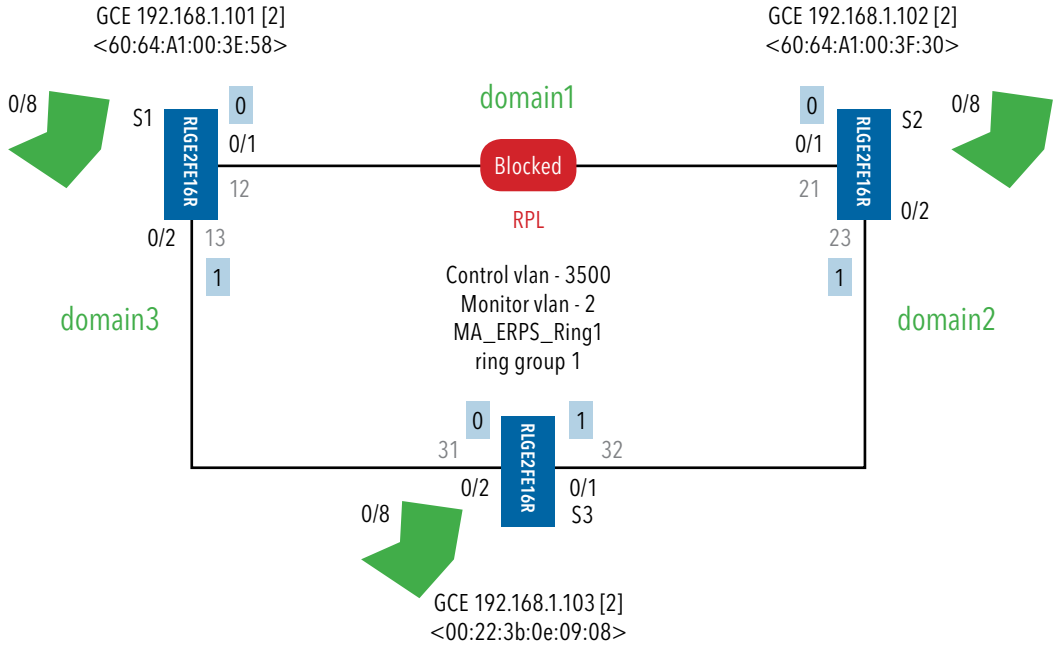
Command	Description
[no]aps distribute <interface_type> <interface_id>	This command configures the ring port as distributing port. The fault monitoring entities (Y.1731 specific) will be associated with this ring port. The no-form of the command removes the distributing port configuration from the ring. **<interface_type>**: Configures the port as distributing port for the specified type of interface. The interface type can be: fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second. gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links. internal-lan – Internal LAN created on a bridge per IEEE 802.1ap. port-channel – Logical interface that represents an aggregator which contains several ports aggregated together. **<interface_id>**: Configures the port as distributing port for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than internal-lan and port-channel. Only i-lan or port-channel ID is provided, for interface types internal-lan and port-channel. Default: 0
[no] aps ring map vlan-group <short(0-64)> [{add|remove}] <port_list>	This command adds or removes a set of VLANs to a VLAN group. If add/remove option is not given, then the given list overwrites the existing vlan list for the group. The no form of the command deletes the entire VLAN grouping information that belongs to a particular VLAN group. **vlan-group <short(0-64)>**: Configures the vlan group identifier. **Add**: Adds a list of vlans to the vlan group **Remove**: Removes a list of vlans from the vlan group **<port_list>**: Configures the list of vlans that are mapped to the vlan group.
aps ring vlan-group-manager {erps | mstp}	This command configures the module that manages the grouping of VLANs in the virtual context. **Erps**: ERPS module manages the grouping of vlans. **Mstp**: MSTP module manages the grouping of vlans. Defaults: mstp
[no] aps ring notification enable	This command enables the sending of trap notification messages from ERPS to a remote management entity upon specific events. The no form of the command disables the sending of trap notification messages from ERPS to a remote management entity upon specific events. Defaults: Trap notification is disabled.
clear aps ring statistics [ring group <group-id>]	This command clears the statistics counters for the given ring. If the ring ID is not given, this command clears the statistics for all the rings in the context. **ring group <group-id>**: Clears the unique numeric identifier of a ring within the context.

Command	Description
[no] debug aps ring {[all] [critical] [start-shut] [mgmt] [ctrl] [pkt-dump] [resource] [all-fail] [buff] [switch <string (32)>]}	This command enables the tracing of the ERPS module as per the configured debug levels. The trace statements are generated for the configured trace levels. The no form of the command disables the tracing of the ERPS module as per the configured debug levels. The trace statements are not generated for the configured trace levels. This command allows the combination of debug levels to be configured (that is, more than one level of trace can be enabled or disabled). The debug levels are configured one after the other and not in single execution of the command. When the commands debug aps ring or no debug aps ring are executed without any of the optional parameters, it displays the traces enabled in the switches. **All**: Generates debug statements for all kinds of traces. **Critical**: Generates debug statements for critical traces. These traces are generated for cases such as failure of RBTree addition, failure to program the hardware and so on. **start-shut**: Generates debug statements for start and shutdown traces. This trace is generated on failed initialization and shutting down of ERPS related entries. **mgmt**: Generates debug statements for management traces. This trace is generated during failure in configuration of any of the ERPS features. **ctrl**: Generates debug statements for control plane traces. These traces are generated for cases such as MBSM card removal, failure of state change and so on. **pkt-dump**: Generates debug statements for packet dump traces. These traces are generated during the reception and transmission of packets. **Resource**: Generates debug statements for traces related to all resources such as memory, data structure and the like. These traces are generated for failure of memory allocation and so on. **all-fail**: Generates debug statements for all kinds of failure traces. These traces are generated for all valid and invalid failures. **Buff**: Generates debug statements for buffer allocation / release traces. **Switch**: Configures the tracing of the ERPS module for the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature. Defaults: critical
show aps ring global info [switch <context_name>]	This command displays the ERPS global information for a context.
show aps ring [group <group_id>] [{configuration | statistics | timers }] [switch <context_name>]	This command displays the protection ring group related information. **group <group_id>**: Displays the unique identifier for the protection group. **Configuration**: Displays configuration (such as R-APS VLAN ID, ring ports, node type, and so on) of the protection ring groups in the virtual contexts. **Statistics**: Displays statistics information (such as count of RAPS PDUs sent, R-APS PDUs received, R-APS PDUs discarded and so on) for each of the protection ring groups. **Timers**: Displays timer related information (such as intervals of hold-off, wait-to-restore, guard and periodic timers) for each of the protection ring groups. **switch<context_name>**: Displays the protection ring group related information for the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.
show aps ring vlan-group [<short(0-64)>]	This command displays the Vlan to group mapping information. NOTE: ERPS functionality should be started and enabled in the virtual context, before executing this command.

ERP setup example

Below setup example and configuration will allow protection over vlan 2 running the PCs traffic and switch management.

The link between S1 and S2 is chosen as the RPL.



NOTE: Values in blue are CFM MEPs:
Values 0,1 are the Ring Ports BPR

Common Configuration for all switches

Disable RSTP on all interfaces before enabling ERP

```
Config
shutdown spanning-tree
no spanning-tree
end
write startup-cfg
```

S1 configuration

1. Set switch host-name (not mandatory)

```
set host-name S1
```

2. Create the control vlan .tag the ring ports

```
config
vlan 3500
port  gigabitethernet 0/1-2
exit
```

3. Create the monitored user vlan .tag the ring ports and user port

```
vlan 2
port  gigabitethernet 0/1-2 fastethernet 0/8 untagged fastethernet 0/8
exit
```

4. Assign the default vlan for the user ports

```
interface fast 0/8
switchport pvid 2
exit
```

5. Assign the management IP to the switch over the monitored vlan

```
interface vlan 2
ip address 192.168.1.101 255.255.255.0
no shutdown
exit
```

6. Remove the ring ports from the default vlan 1

```
vlan 1
no ports gigabitethernet 0/1-2 fast 0/8 untagged all
exit
```

7. CFM configuration

```
ethernet cfm start
ethernet cfm enable
ethernet cfm y1731 enable
ethernet cfm traceroute cache
```

8. Create CFM domain, name 'domain1' for the S1-S2 link. The system will generate this domain with index 1. An ME named 'MA_ERPS_Ring1' is created, common for all domains, at all 3 ring switches. At each domain assign the mep crosscheck, first assign the local MEP of the domain, then the opposite MEP at the link (local MEP at the switch sharing the link).

```
ethernet cfm domain format none name domain1 level 6
service format char-string name MA _ ERPS _ Ring1 vlan 3500
mep crosscheck mpid 12 vlan 3500  ! local mep in the domain
mep crosscheck mpid 21 vlan 3500  ! neighbor mep in the domain
exit
```

9. Create CFM domain, name 'domain3' for the S1-S3 link. The system will generate this domain with index 2. An ME named 'MA_ERPS_Ring1' is created, common for all domains, at all 3 ring switches. At each domain assign the mep crosscheck, first assign the local MEP of the domain, then the opposite MEP at the link (local MEP at the switch sharing the link).

```
ethernet cfm domain format none name domain3 level 6
service format char-string name MA _ ERPS _ Ring1 vlan 3500
mep crosscheck mpid 13 vlan 3500
mep crosscheck mpid 31 vlan 3500
exit
```

10. Control vlan enable and CCM interval

```
ethernet cfm cc level 6 vlan 3500 interval hundred-ms
ethernet cfm cc enable level 6 vlan 3500
```

11. Ring ports CFM assignment. As per the setup drawing, Gi 0/1 holds MEP 12 at CFM domain1. Gi 0/2 holds MEP 13 at CFM domain3.

```
interface Gi 0/1
ethernet cfm mep level 6 mpid 12 vlan 3500 active
exit
exit
interface Gi 0/2
ethernet cfm mep level 6 mpid 13 vlan 3500 active
exit
exit
```

12. Enable ERP

```
no shutdown aps ring
aps ring enable
```

13. Create Ring group, set Ring Port1 (BPR 0) and Port2 (BPR 1). In below example, Port1 is Gi 0/1, Port2 is Gi 0/2. The order of assignment is important, Port1 should relate to the interface member in CFM Domain index 1 ('domain1'). Port2 should relate to the interface member in CFM Domain index 2 ('domain3')

```
aps ring group 1
aps working Gi 0/1 Gi 0/2 vlan 3500
```

14. At the Ring group, set MGE1 and MGE2. In below example, MEG1 defines 'meg 1 me 1 mep 12 and MEG2 defines 'meg 2 me 1 meg 13'. The order of assignment is important, MEG1 should relate to the MEP (12) member in CFM Domain index 1 ('domain1'). MEG2 should relate to the MEP (13) member in CFM Domain index 2 ('domain3')

```
aps working meg 1 me 1 mep 12 meg 2 me 1 mep 13
```

15. Set the Switch as the ring owner by assigning the RPL port as 'protect'. At our setup, Gi 0/1 is the RPL owner

```
aps protect Gi 0/1
aps revert wtr 500 milliseconds
aps group active
end
```

16. Commit

```
write startup-cfg
```

S2 configuration

1. Set switch host-name (not mandatory)

```
set host-name S2
```

2. Create the control vlan .tag the ring ports

```
config
vlan 3500
port  gigabitethernet 0/1-2
exit
```

3. Create the monitored user vlan .tag the ring ports and user port

```
vlan 2
port  gigabitethernet 0/1-2 fastethernet 0/8 untagged fastethernet 0/8
exit
```

4. Assign the default vlan for the user ports

```
interface fast 0/8
switchport pvid 2
exit
```

5. Assign the management IP to the switch over the monitored vlan

```
interface vlan 2
ip address 192.168.1.102 255.255.255.0
no shutdown
exit
```

6. Remove the ring ports from the default vlan 1

```
vlan 1
no ports gigabitethernet 0/1-2 fast 0/8 untagged all
exit
```

7. CFM configuration

```
ethernet cfm start
ethernet cfm enable
ethernet cfm y1731 enable
ethernet cfm traceroute cache
```

8. Create CFM domain, name 'domain1' for the S1-S2 link. The system will generate this domain with index 1. An ME named 'MA_ERPS_Ring1' is created, common for all domains, at all 3 ring switches. At each domain assign the mep crosscheck, first assign the local MEP of the domain, then the opposite MEP at the link (local MEP at the switch sharing the link).

```
ethernet cfm domain format none name domain1 level 6
service format char-string name MA _ ERPS _ Ring1 vlan 3500
mep crosscheck mpid 21 vlan 3500
mep crosscheck mpid 12 vlan 3500
exit
```

9. Create CFM domain, name 'domain2' for the S2-S3 link. The system will generate this domain with index 2. An ME named 'MA_ERPS_Ring1' is created, common for all domains, at all 3 ring switches. At each domain assign the mep crosscheck, first assign the local MEP of the domain, then the opposite MEP at the link (local MEP at the switch sharing the link).

```
ethernet cfm domain format none name domain2 level 6
service format char-string name MA _ ERPS _ Ring1 vlan 3500
mep crosscheck mpid 23 vlan 3500
mep crosscheck mpid 32 vlan 3500
exit
```

10. Control vlan enable and CCM interval

```
ethernet cfm cc level 6 vlan 3500 interval hundred-ms
ethernet cfm cc enable level 6 vlan 3500
```

11. Ring ports CFM assignment. As per the setup drawing, Gi 0/1 holds MEP 21 at CFM domain1. Gi 0/2 holds MEP 23 at CFM domain2.

```
interface Gi 0/1
ethernet cfm mep level 6 mpid 21 vlan 3500 active
exit
exit
interface Gi 0/2
ethernet cfm mep level 6 mpid 23 vlan 3500 active
exit
exit
```

12. Enable ERP

```
no shutdown aps ring
aps ring enable
```

13. Create Ring group, set Ring Port1 (BPR 0) and Port2 (BPR 1). In below example, Port1 is Gi 0/1, Port2 is Gi 0/2. The order of assignment is important, Port1 should relate to the interface member in CFM Domain index 1 ('domain1'). Port2 should relate to the interface member in CFM Domain index 2 ('domain2')

```
aps ring group 1
aps working Gi 0/1 Gi 0/2 vlan 3500
```

14. At the Ring group, set MGE1 and MGE2. In below example, MEG1 defines 'meg 1 me 1 mep 21 and MEG2 defines 'meg 2 me 1 meg 23'. The order of assignment is important, MEG1 should relate to the MEP (21) member in CFM Domain index 1 ('domain1'). MEG2 should relate to the MEP (23) member in CFM Domain index 2 ('domain2')

```
aps working meg 1 me 1 mep 21 meg 2 me 1 mep 23
```

15. Set the Switch as the ring neighbor by assigning the RPL port as 'neighbor'. At our setup, Gi 0/1 is the RPL neighbor

```
aps neighbor Gi 0/1
aps revert wtr 500 milliseconds
aps group active
end
```

16. Commit

```
write startup-cfg
```

S3 configuration

1. Set switch host-name (not mandatory)

```
set host-name S3
```

2. Create the control vlan .tag the ring ports

```
config
vlan 3500
port  gigabitethernet 0/1-2
exit
```

3. Create the monitored user vlan .tag the ring ports and user port

```
vlan 2
port  gigabitethernet 0/1-2 fastethernet 0/8 untagged fastethernet 0/8
exit
```

4. Assign the default vlan for the user ports

```
interface fast 0/8
switchport pvid 2
exit
```

5. Assign the management IP to the switch over the monitored vlan

```
interface vlan 2
ip address 192.168.1.103 255.255.255.0
no shutdown
exit
```

6. Remove the ring ports from the default vlan 1

```
vlan 1
no ports gigabitethernet 0/1-2 fast 0/8 untagged all
exit
```

7. CFM configuration

```
ethernet cfm start
ethernet cfm enable
ethernet cfm y1731 enable
ethernet cfm traceroute cache
```

8. Create CFM domain, name 'domain3' for the S1-S3 link. The system will generate this domain with index 1. An ME named 'MA_ERPS_Ring1' is created, common for all domains, at all 3 ring switches. At each domain assign the mep crosscheck, first assign the local MEP of the domain, then the opposite MEP at the link (local MEP at the switch sharing the link).

```
ethernet cfm domain format none name domain3 level 6
service format char-string name MA _ ERPS _ Ring1 vlan 3500
mep crosscheck mpid 31 vlan 3500
mep crosscheck mpid 13 vlan 3500
exit
```

9. Create CFM domain, name 'domain2' for the S2-S3 link. The system will generate this domain with index 2. An ME named 'MA_ERPS_Ring1' is created, common for all domains, at all 3 ring switches. At each domain assign the mep crosscheck, first assign the local MEP of the domain, then the opposite MEP at the link (local MEP at the switch sharing the link).

```
ethernet cfm domain format none name domain2 level 6
service format char-string name MA _ ERPS _ Ring1 vlan 3500
mep crosscheck mpid 32 vlan 3500
mep crosscheck mpid 23 vlan 3500
exit
```

10. Control vlan enable and CCM interval

```
ethernet cfm cc level 6 vlan 3500 interval hundred-ms
ethernet cfm cc enable level 6 vlan 3500
```

11. Ring ports CFM assignment. As per the setup drawing, Gi 0/2 holds MEP 31 at CFM domain1. Gi 0/1 holds MEP 32 at CFM domain2.

```
interface Gi 0/2
ethernet cfm mep level 6 mpid 31 vlan 3500 active
exit
exit
interface Gi 0/1
ethernet cfm mep level 6 mpid 32 vlan 3500 active
exit
exit
```

12. Enable ERP

```
no shutdown aps ring
aps ring enable
```

13. Create Ring group, set Ring Port1 (BPR 0) and Port2 (BPR 1). In below example, Port1 is Gi 0/2, Port2 is Gi 0/1. The order of assignment is important, Port1 should relate to the interface member in CFM Domain index 1 (‘domain1’). Port2 should relate to the interface member in CFM Domain index 2 (‘domain2’)

```
aps ring group 1
aps working Gi 0/2 Gi 0/1 vlan 3500
```

14. At the Ring group, set MGE1 and MGE2.In below example, MEG1 defines ‘meg 1 me 1 mep 31’ and MEG2 defines ‘meg 2 me 1 meg 32’. The order of assignment is important, MEG1 should relate to the MEP (31) member in CFM Domain index 1 (‘domain1’). MEG2 should relate to the MEP (32) member in CFM Domain index 2 (‘domain2’)

```
aps working meg 1 me 1 mep 31 meg 2 me 1 mep 32
```

15. Activate the group

```
aps group active
end
```

16. Commit

```
write startup-cfg
```

Configuration validation

Following is a show output example for S1.

A validation of configuration will include verifying the proper co-relation between the CFM configuration and the APS.

1. Show the CFM domain configuration and state. In ring idle state, all MEPs should be 'Up'. In below example, 'domain1' is set with index 1 and domain2 with index 2.

```
S1# show ethernet cfm domain

Domain Name : domain1
Index : 1
Level : 6
Vlan Priority : 7
Drop Eligibility : Disabled
MHF Creation Criteria : none
Sender Id Permission : none
Total Services : 1

Vlan Crosscheck ServiceID
3500 Enabled    MA _ ERPS _ Ring1
Crosscheck:
MPID VLAN ISID       Type            Mep-Up
12   3500 -          Local           Yes
21   3500 -          Remote          Yes

Domain Name : domain3
Index : 2
Level : 6
Vlan Priority : 7
Drop Eligibility : Disabled
MHF Creation Criteria : none
Sender Id Permission : none
Total Services : 1

Vlan Crosscheck ServiceID
```

```
3500 Enabled    MA _ ERPS _ Ring1
Crosscheck:
MPID VLAN ISID       Type            Mep-Up
13   3500 -          Local           Yes
31   3500 -          Remote          Yes
```

2. Show the ERP configuration. Notice the coloring indication representing the domain index relation to the APS port configuration and MEG. CFM domain1 has index 1 (in yellow). It defines MEP 12 on interface Gi 0/1. Thus, the APS configuration should have Gi 0/1 as Port1. As well, the APS assignment of mep 12, which belongs to domain1, should be in MEG1.

```
S1# show running-config erps
no shutdown aps ring
aps ring enable
!
switch default
aps ring group 1
aps working gigabitethernet 0/1 gigabitethernet 0/2 vlan 3500
aps protect gigabitethernet 0/1

aps working meg 1 me 1 mep 12 meg 2 me 1 mep 13
aps revert wtr 500 milliseconds
aps group active
```

Verifying setup state

Following is a show output example for S1

1. Show the ring state using the command “show aps ring”. If no fault is present at the ring, an indication of ‘Idle’ is expected and the link status of both ring ports should be ‘Not Failed’. In Idle state, the RPL port status should be ‘blocked’.

```
S1# show aps ring

 Ring Id 1
-------------------------------------------------------
Ring Name                          : Ring1
RAPS Vlan Id                       : 3500
Operating Mode                     : Revertive
Recovery Method                    : Auto
ERPS Compatible Version            : Version2
```

```
Ring State                              : Idle
Status                                  : Active
Wait-to-restore timer                  : Not Running
Wait-to-block timer                    : Not Running
Hold timer                              : Not Running
Guard timer                             : Not Running
TC Propagation Status                  : Disable
TC Propagation Ring List               : None
Inter Connection Node                  : none
Multiple Failure                        : Disabled
Monitoring Mechanism                   : Cfm


Node ID, BPR bit Pair
=====================
Ring Port 1 - (00:00:00:00:00:00    , 0)
Ring Port 2 - (00:00:00:00:00:00    , 0)


This node is RPL Owner. RPL Port is Gi0/1

Ring node is configured with virtual channel

 Ring Port          Link Status       Command         Port Status
-----------------------------------------------------------------
 Gi0/1              Not Failed         None            Blocked
 Gi0/2              Not Failed         None            UnBlocked

Line Card Information
----------------------
Ring Port 1 (Gi0/1): Local
Ring Port 2 (Gi0/2): Local
```

2. Show the state of CFM local and remote points. In Idle state, all MEPs should be ‘Up’ and the MAC addresses should be learned.

```
S1# show ethernet cfm service


----------------------------------------
Service Name : MA _ ERPS _ Ring1
```

```
Domain Name  : domain1
Index        : 1
Primary Vid  : 3500
Level        : 6

MHF Creation Criteria : defer
Sender Id Permission  : defer
CC Role    : fault management
ICC Code   : MA _ ERP
UMC Code   : domain
Total MEPs : 2
Primary Vlan Associations :
None
Crosscheck status : Enabled
Crosscheck:
MPID VLAN ISID      Type           Mep-Up Mac Address
12   3500 -         Local          Yes    60:64:a1:00:3e:60
21   3500 -         Remote         Yes    60:64:a1:00:3f:38

----------------------------------------
Service Name : MA _ ERPS _ Ring1
Domain Name  : domain3
Index        : 1
Primary Vid  : 3500
Level        : 6

MHF Creation Criteria : defer
Sender Id Permission  : defer
CC Role    : fault management
ICC Code   : MA _ ERP
UMC Code   : domain
Total MEPs : 2
Primary Vlan Associations :
None
Crosscheck status : Enabled
Crosscheck:
MPID VLAN ISID      Type           Mep-Up Mac Address
13   3500 -         Local          Yes    60:64:a1:00:3e:61
31   3500 -         Remote         Yes    00:22:3b:0e:09:08
```

Removing ERP and CFM configuration

Example given for S1

1. Remove the ERP APS configuration

```
config
no aps ring group 1
no aps ring enable
shutdown aps ring
```

2. Remove the MEP assignment from the ring ports

```
interface fastethernet 0/1
no ethernet cfm mep level 6 mpid 12 vlan 3500
exit
interface fastethernet 0/2
no ethernet cfm mep level 6 mpid 13 vlan 3500
exit
```

3. Remove the MEPs and MA service from each domain

```
ethernet cfm domain format none name domain1 level 6
no mep crosscheck mpid 12 vlan 3500
no mep crosscheck mpid 21 vlan 3500
no service name MA _ ERPS _ Ring1
exit
ethernet cfm domain format none name domain3 level 6
no mep crosscheck mpid 13 vlan 3500
no mep crosscheck mpid 31 vlan 3500
no service name MA _ ERPS _ Ring1 exit
```

4. Remove the CFM Domains

```
no ethernet cfm domain format none name domain1 level 6
no ethernet cfm domain format none name domain3 level 6
```

5. Disable CFM

```
no ethernet cfm y1731 enable
no ethernet cfm enable
```

Discrete IO Channels

Discrete signals are very common in industrial application to monitor alarms and indications from the field side.

The ComNet switch allows the most effective feature of monitoring and controlling these channels over the IP network.

The ComNet switch basically acts as a Modbus gateway, expecting connections from Modbus tcp clients at port tcp 502.

Discrete channel interfaces

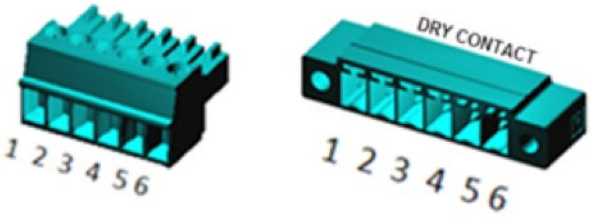
The status of the digital inputs can be read via CLI and using Modbus TCP.

The digital output can be set using Modbus TCP. The state can be read via cli and Modbus TCP.

NOTE: The physical interface DO1 used for this feature can be utilized as well for the purpose of manifesting system alarms acting as "Alarm-Relay". The physical interface cannot be assigned simultaneously to both feature types.
For the use of discrete channels please make sure the interface is not occupied by the Alarm-Relay service.

Connection terminal are as shown in below figure.

1. Digital Output 1
2. N/A
3. Digital Output Common
4. Digital Input Common
5. Digital Input 1 (12-48vDC)
6. Digital Input 2 (12-48vDC)



Hardware

Please contact ComNet support to verify if your hardware supports this interface.

Modbus/TCP

The discrete channels are controllable via Modbus/TCP commands.

An ACE interface is required to accept incoming connections at TCP port 502.

Channel	Terminal	Default state	Modbus address	Modbus Function Code
Discrete In #1	5,4	Low [0], no external PS voltage is connected.	10001	[2] read discrete input contacts
Discrete In #2	6,4	Low [0], no external PS voltage is connected.	10002	[2] read discrete input contacts
Discrete Out #1	1,3	Low [0], contact is open.	0001	[5] write single discrete output coil
			10011	[1] read discrete output coil

NOTE: The state of the OUT channel is always set to 0 after system boot.

Electric data

» At the digital Input points please connect a DC source in the nominal range 12-48v at terminals 6,4 for channel 2; or 5,4 for channel 1. Maximum limits of 9-58vDC should not be exceeded.

» Maximum power to be implemented at the contacts :
AC: Max 250v , 37.5vA.
DC: Max 220v ,30 watt.

Above mentioned power limitations should not be exceeded. Maximum current allowed at the contacts is 1A.

Discrete IO Channels Commands Hierarchy

+ root

+ application connect

    + discrete-channels

        + admin-status <enable| disable>

+ mapping

- add modbus-gw {address-prefix <A.B.C.D/M>}

- remove modbus-gw {address-prefix <A.B.C.D/M>}

+ connection

    - show

    - clear

+ show

- discrete-values

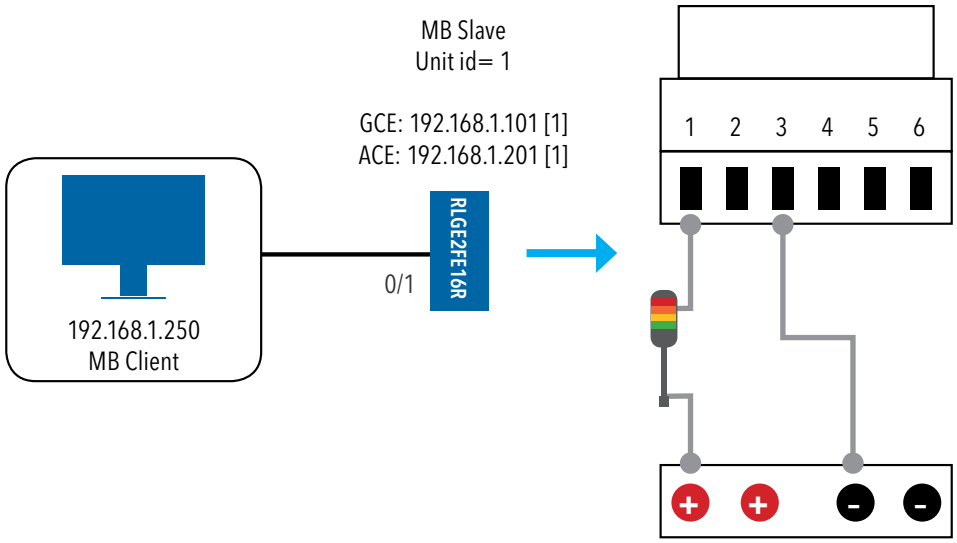
- mb_gw

Discrete Interfaces Commands

Command	Description
Application connect	Enter the industrial application menu
discrete-channels	Enter the configuration mode for a specific physical serial ports
admin-status	Enable/disable listening to Modbus TCP connections
mapping	Assign an IP interface
add modbus-gw	IP address and subnet of the local ACE interface used to listen to incoming Modbus connections.
remove modbus-gw	IP address and subnet of the local ACE interface used to listen to incoming Modbus connections.
Connection show	Show connected Modbus clients
Show	History- history events. discrete-values- the state of the discrete channels. Mb_gw- the properties and state of the gateway.

Example

Following setup demonstrates DNP3 gateway configuration.



1. set switch host name (optional)

```
set host-name Gateway
```

2. Set service vlan. Gigabitethernet 0/3 must be a tagged member.

```
config
vlan 1
ports fastethernet 0/1  gigabitethernet 0/3 untagged fastethernet 0/1
exit
interface fastethernet 0/1
alias CLIENT
switchport pvid 1
exit
```

3. assign management IP (optional)

```
interface vlan 1
ip address 192.168.1.101 255.255.255.0
no shut
end
```

4. access the ACE mode

```
application connect
```

5. assign IP interface for the gateway

```
router interface create address-prefix 192.168.1.201/24 vlan 1 purpose application-host
```

6. assign the ACE interface to be used for the Modbus gateway

```
discrete-channels mapping add modbus-gw address-prefix 192.168.1.201/24
```

7. Enable the feature

```
discrete-channels admin-status enable
exit
write startup-cfg
```

Establish a Modbus connection from the client to the server.

Sent a command from the client to the server, using function code 5 an address 0001 to activate the discrete output contact.

```
[/]discrete-channels connection show
+-------+-----------------+---------------+----------+
| Index |    GW IP/Subnet | client ip addr| src port |
+=======+=================+===============+==========+
|    1    | 192.168.1.250/24 | 192.168.1.250   |   55218    |
+-------+-----------------+---------------+----------+

[/]discrete-channels show discrete-values
+---------------+---------------+---------------+
| Input#1 10001 | Input#2 10002 | Output#1 0001 |
+===============+===============+===============+
|        0      |        0       |        1       |
+---------------+---------------+---------------+
[/]
```

NAT

The RLGE2FE16R router supports Static and Dynamic settings of Network Address Translation.

Dynamic NAT settings allow LAN members to initiate sessions with targets located at the WAN. The NAT router (RLGE2FE16R) will use its WAN IP interface as the new source ip of the session request, hiding the original private IP of the initiating LAN device. The NAT router can use a single WAN ip interface to traverse multiple private IP addresses of its lan, thus limiting the required public ip addresses to a single one.

Static NAT settings, direct incoming WAN traffic to a particular target LAN client. As the WAN stations usually will not have a route to the private LAN, but only to the WAN ip address of the router, the static Nat settings are mandatory to allow them to initiate sessions towards LAN targets.

The NAT router serves both a routing function and security layer, allowing provisioning of WAN traffic access to the LAN.

The NAT functionality is supported at the ACE.

Networking

Following picture will suggest NAT networking results per configuration option of dynamic/ static NAT set at the RLGE2FE16R.

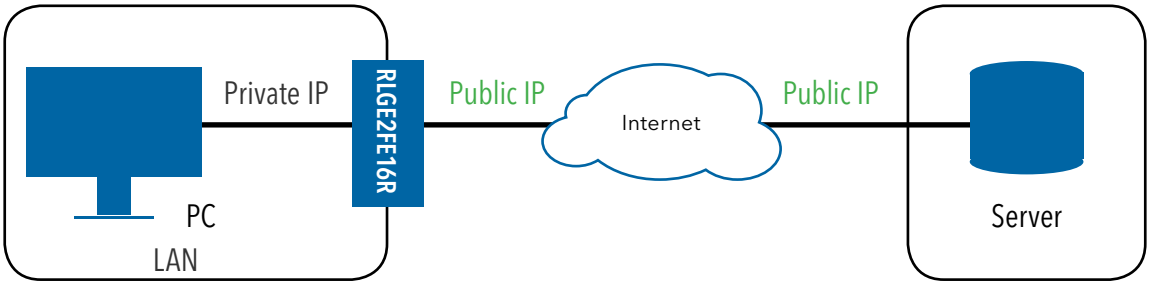


Figure 1 NAT networking 1

Looking at picture 'NAT networking 1', PC communication towards the server is dependent on the NAT configuration set at the RLGE2FE16R NAT router.

» Static NAT only

The PC will not be able to initiate sessions towards the Server. Sessions initiated by the Server towards the PC will be received by the PC and replies of the PC will be received at the Server.

» Dynamic NAT only

The PC will be able to initiate sessions towards the Server and replies of the Server will be received at the PC. Sessions initiated by the Server towards the PC will not be received by the PC.

» Dynamic and Static NAT together

Both the Server and the PC can initiate sessions and receive replies.

NAT Commands Hierarchy

+ Application connect

+ router

+ nat

+ Dynamic

- Create {interface-name {eth1.<vlan-id>| ppp0}} [description <text>]

- remove interface-name {eth1.<vlan-id>|ppp0}

- show

+ static

- Create {original-ip <A.B.C.D>} {modified-ip <>}

[original-port <1-65535>] [modified-port <1-65535>]

[protocol <tcp |udp| all>] [description <text>]

- remove {[rule-id <>] | [{original-ip < A.B.C.D >}

{modified-ip < A.B.C.D >} {protocol <tcp |udp| all>}]}

- show

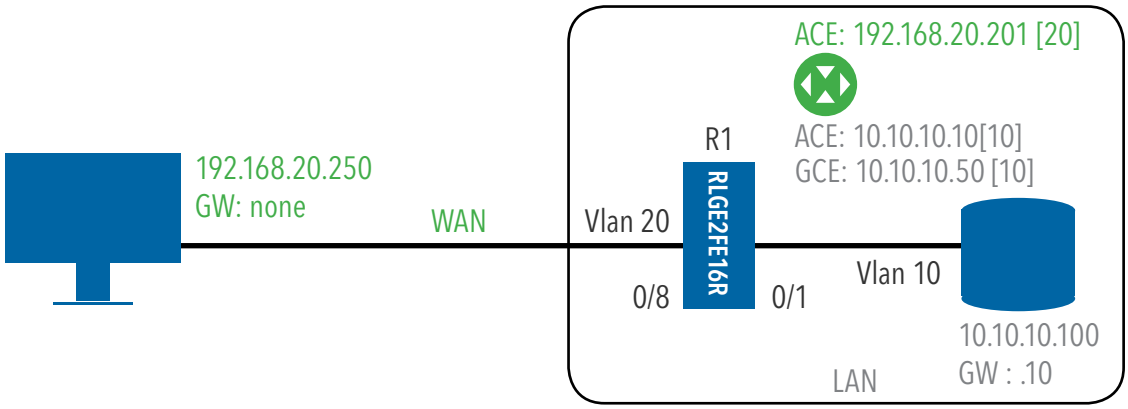
NAT Commands Description

Command	Description
Application connect	Access the ACE
nat	Access the NAT configuration mode
Dynamic	Create | remove | show interface for dynamic nat. Interface name: the IP interface on which to enable the dynamic nat. LAN packets egressing the route rover this interface will have their 'source ip' replaced with the interface IP. The interface may be one which is associated with a VLAN or the cellular ppp0 interface. Description: text describing the interface. Optional.
static	Create | remove | show static nat entries. Original-ip: the original 'destination ip' at the incoming packet ip header. Modified-ip: the ip to which the nat should traverse the original-ip to. Original-port: the original protocol 'destination port' at the incoming packet ip header. Modified-port: the protocol port to which the nat should traverse the original-port to. Protocol: define the protocol, which the incoming packet uses, for which the nat should traverse. Packets which do not meet this condition will not traverse. Rule-id: an identifier given automatically by the system for each static nat entry. The rule-id is a sufficient parameter to remove an entry.

Example, Fixed Network

Following setup example will explain how to use NAT to allow the PC, residing outside the LAN and with no routing to the LAN, connectivity to the LAN.

The PC is set to achieve management to the switch using the switch private interface and as well telnet to a server located at the LAN.



1. Set host name (optional)

```
set host-name R1
```

2. Set vlans and port assignment

```
config
vlan 20
ports fa 0/8 gigabitethernet 0/3  untagged fast 0/8 name wan
exit
vlan 10
ports fa 0/1 gigabitethernet 0/3 untagged fast 0/1
exit

interface fastethernet 0/1
alias CE
switchport pvid 10
exit

interface fastethernet 0/8
alias wan
switchport pvid 20
exit
```

3. Set a GCE interface for management. Add static route to the ACE NAT interface

```
interface vlan 10
ip address 10.10.10.50 255.255.255.0
no shut
exit
ip route 0.0.0.0 0.0.0.0 10.10.10.10
exit
write startup-cfg
```

4. Set ACE interfaces. Interface eth1.20 will be the NAT interface, eth1.10 will be used to route towards the lan

```
application connect
router interface create address-prefix 192.168.20.201/24 vlan 20 purpose application-host description wan
router interface create address-prefix 10.10.10.10/24 vlan 10 purpose general description lan
```

5. Set Static NAT settings, directing WAN traffic targeted to 192.168.20.201 with port SSH (22) towards the GCE interface 10.10.10.50. This will allow the PC to achieve management to the RLGE2FE16R.

```
router nat static create original-ip 192.168.20.201 modified-ip 10.10.10.50 original-port 22 modified-port 22 protocol tcp
```

6. Set Static NAT settings, directing WAN traffic targeted to 192.168.20.201 towards 10.10.10.100 with port 20000 (DNP3). This will allow the PC to establish DNP3 session with the server.

```
router nat static create original-ip 192.168.20.201 modified-ip 10.10.10.100 original-port 20000 modified-port 20000 protocol tcp
```

7. Set dynamic NAT settings, allowing lan devices to initiate connection to the PC residing at the WAN

8. Commit

```
exit
Write startup-cfg
```

9. Show output example

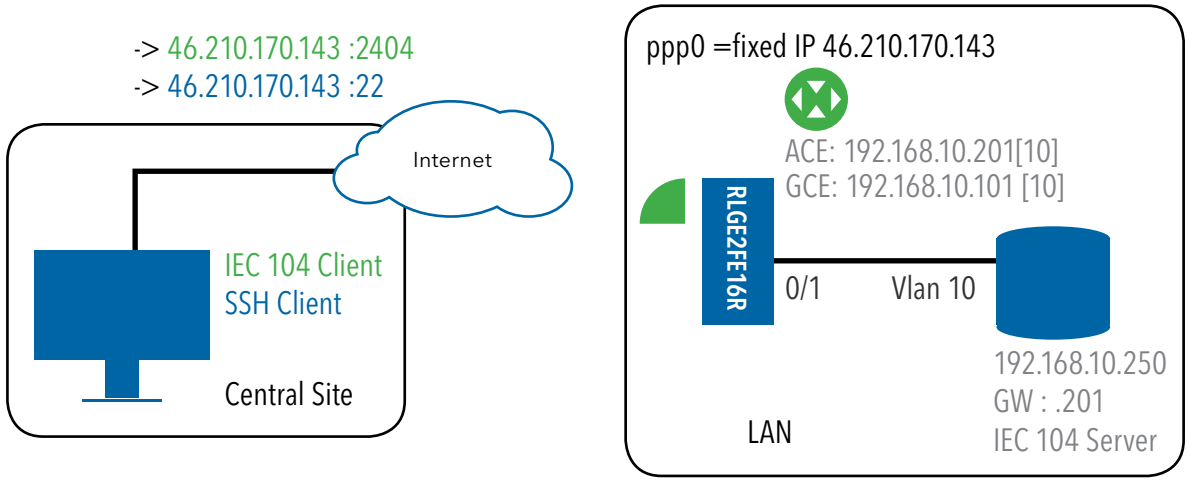
```
RLGE2FE16R#router interface show
+----+------+--------+-----------------+------+---------+-------------+-------------+
| Id | VLAN |  Name  |    IP/Subnet     | Mtu  | Purpose | Admin status | Description |
+====+======+========+=================+======+=========+=============+=============+
| 1  | N/A  | eth1:1 |  10.10.10.10/24  | 1500 | general |    enable    |     LAN     |
+----+------+--------+-----------------+------+---------+-------------+-------------+
| 2  | N/A  | eth2:2 | 192.168.10.11/24 | 1500 | general |    enable    |     WAN     |
+----+------+--------+-----------------+------+---------+-------------+-------------+
[router/]nat dynamic show
+---------+---------+-------------+
| Rule-Id | If-Name | Description |
+=========+=========+=============+
|    1    | eth2:2  |     wan     |
+---------+---------+-------------+
RLGE2FE16R#router nat static show
+---------+-----------------+-------------------+----------+-----------------+----------------
---+
| Rule-Id | Original-Dst-IP | Original-Dst-Port | Protocol | Modified-Dst-IP | Modified-
Dst-Port |
+=========+=================+===================+==========+=================+==========
=========+
|    1    |  192.168.10.11  |         23        |   tcp    |   10.10.10.10   |         23
|
+---------+-----------------+-------------------+----------+-----------------+----------------
---+
|    2    |  192.168.10.11  |       20000       |   tcp    |  10.10.10.100   |
20000       |
+---------+-----------------+-------------------+----------+-----------------+----------------
---+
```

Example, Cellular Network

Following setup example will explain how to use NAT over the cellular connection so to allow the PC, residing outside the LAN and with no routing to the LAN, connectivity to the LAN.

The PC is set to achieve management to the switch using the switch private interface and as well IEC104 (TCP connection with port 2404) to an IEC 104 server located at the LAN.

The cellular modem must hold a static IP address for this scenario. At below example the cellular modem retrieved IP 46.210.170.143 from the ISP. The PC will open the connections towards this address.



1. Set host name (optional)

```
set host-name R1
```

2. Set vlans and port assignment

```
config
vlan 10
ports fa 0/1 gigabitethernet 0/3 untagged fast 0/1
exit
interface fastethernet 0/1
alias CE
switchport pvid 10
exit
```

3. Set a GCE interface for management. Add static route to the ACE NAT interface

```
interface vlan 10
ip address 192.168.10.101 255.255.255.0
no shut
```

```
exit
ip route 0.0.0.0 0.0.0.0 192.168.10.201
exit
write startup-cfg
```

4. Set ACE interfaces eth1.10 to route towards the lan

```
application connect
router interface create address-prefix 192.168.10.201/24 vlan 10 purpose application-host
description wan
```

5. Set the celllar modem per the SIM properties

```
cellular wan update admin-status enable apn-name internetg sim-slot 1 operator-name
cellcom user-name guest password guest
cellular settings update  default-route yes
cellular enable
```

6. Set Static NAT settings, directing WAN traffic targeted to the cellular public IP 46.210.170.143 (EXAMPLE) with port SSH (22) towards the GCE interface 192.168.10.101. This will allow the PC to achieve management to the RLGE2FE16R.

```
router nat static create original-ip 46.210.170.143 modified-ip 192.168.10.101 original-port
22  modified-port 22 protocol tcp
```

7. Set Static NAT settings, directing WAN traffic targeted to 46.210.170.143 (EXAMPLE) towards 192.168.10.250 with port 2404 (IEC104). This will allow the PC to establish DNP3 session with the server.

```
router nat static create original-ip 46.210.170.143 modified-ip 192.168.10.250 original-port
2404 modified-port 2404 protocol tcp
```

8. Set dynamic NAT settings, allowing lan devices to initiate connection to the PC residing at the WAN

```
router nat dynamic create interface-name ppp0 description wan
```

9. Commit

```
exit
Write startup-cfg
```

OSPF

OSPF (Open Shortest Path First) protocol is an Interior Gateway Protocol used to distribute routing information within a single Autonomous System. Routers use link-state algorithms to send routing information to all nodes in an inter-network by calculating the shortest path to each node based on topography of the Internet constructed by each node. Each router sends that portion of the routing table (keeps track of routes to particular network destinations), which describes the state of its own links, and it also sends the complete routing structure (topography).

The advantage of shortest path first algorithms is that they result in smaller more frequent update everywhere. They converge quickly, thus preventing such problems as routing loops and Count-to-Infinity (when routers continuously increment the hop count to a particular network). This makes for a stable network.

OSPF is available both in the central switch unit and in the ACE layer. Configuration is thus available in both GCE mode and ACE modes.

Routing of VPNs can be done only in the application layer.

NOTE: Total limit of 64 subnets is supported at the routing table. Customer static and dynamic entries in total should not exceed a total of 60 entries. A syslog message with severity ERROR will indicate exceeding this limit "Number of routes [%d] exceeded max of 60!"

OSPF GCE Commands Hierarchy

+root

+config terminal

+[no] router ospf

-router-id <a.b.c.d>

-[no] network <ip address> <mask> area <a.b.c.d>

-[no] passive-interface vlan <vlan-id>

-[no] area <area-id> stability-interval <Interval-Value (0 - 0x7fffffff)>

-[no] area <area-id> translation-role { always | candidate }

-[no] compatible rfc1583

-abr-type { standard | cisco}

-[no] neighbor <neighbor-id> [priority <priority value (0-255)>]

-[no] area <area-id> default-cost <cost> [tos <tos value(0-30)>]

- area <area-id> nssa [{ no-summary | default-information-originate [metric <value>] [metric-type <Type(1-3)>] [tos <tos value (0-30)>] }]
- [no] area <area-id> stub [no-summary]
- [no] default-information originate always [metric <metric-value (0-0xffffff)>][metric-type <type (1-2)>]
- area <area-id> virtual-link <router-id> [authentication { simple |message-digest | null}] [hello-interval <value (1-65535)>] [retransmit-interval <value (0-3600)>] [transmit-delay <value (0-3600)>] [dead-interval <value>] [{authentication-key <key (8)> | message-digest-key <Key-id (0-255)> md5 <key (16)>}]
- [no] ASBR Router
- [no] area <AreaId> range <Network> <Mask> {summary | Type7} [{advertise | not-advertise}] [tag <value>]
- [no] summary-address <Network> <Mask> <AreaId> [{allowAll | denyAll | advertise | not-advertise}] [Translation {enabled | disabled}]
- [no] redistribute {static | connected | all}
- [no] distribute-list route-map <name(1-20)> in
- [no] redist-config <Network> <Mask> [metric-value <metric (1 - 16777215)>] [metrictype {asExttype1 | asExttype2}] [tag <tag-value>}
- [no] capability opaque
- [no] nsf ietf restart-interval <grace period(1-1800)>
- [no] nsf ietf helper-support [{unknown | softwareRestart | swReloadUpgrade | switchToRedundant}]
- nsf ietf helper gracetimelimit <gracelimit period(0-1800)>
- [no] nsf ietf helper strict-lsa-checking
- [no] nsf ietf grace lsa ack required
- nsf ietf grlsa retrans count <grlsacout (0-180)>
- nsf ietf restart-reason [{unknown | softwareRestart | swReloadUpgrade |switchToRedundant}]
- [no] distance <1-255> [route-map <name(1-20)>]
- [no] route-calculation staggering
- route-calculation staggering-interval <milli-seconds (1000-0x7fffffff)>
- [no] network <Network number> area <area-id> [unnum Vlan <PortNumber> [switch <switch-name>]]

- set nssa asbr-default-route translator { enable | disable }

- [no] passive-interface default

+interface vlan <vlan ID>

-[no] ip ospf demand-circuit

-[no] ip ospf transmit-delay <seconds (0 - 3600)>

-[no] ip ospf priority <value 0 - 255)>

-[no] ip ospf hello-interval <seconds (1 - 65535)>

-[no] ip ospf dead-interval <seconds (0-0x7fffffff)>

-[no] ip ospf cost <cost (1-65535)> [tos <tos value (0-30)>]

-[no] ip ospf network {broadcast | non-broadcast | point-to-multipoint | point-to-point}

-[no] ip ospf authentication-key <password (8)>

-[no] ip ospf authentication [{message-digest | null}]

-[no] debug ip ospf [vrf <name>] { pkt { hp | ddp |lrq | lsu | lsa } | module { adj_formation | ism | nsm | config | interface | restarting-router | helper }}

- show ip ospf [vrf <name>] interface [{ vlan <vlan-id (1-4094)> [switch <switch-name>] | <interface-type> <interface-id> }]

- show ip ospf [vrf <name>] neighbor [{ vlan <vlan-id (1-4094)> [switch <switchname>] | <interface-type> <interface-id> }] [Neighbor ID] [detail]

- show ip ospf [vrf <name>] request-list [<neighbor-id>] [{ vlan <vlan-id (1- 4094)> [switch <switch-name>] | <interface-type> <interface-id> }]

- show ip ospf [vrf <name>] retransmission-list [<neighbor-id>] [{ vlan <vlan-id (1-4094)> [switch <switch-name>] | <interface-type> <interface-id> }]

- show ip ospf [vrf <name>] virtual-links

- show ip ospf [vrf <name>] border-routers

- show ip ospf [vrf <name>]

- show ip ospf [vrf <name>] route

- show ip ospf [vrf <name>] [area-id] database [{database-summary | self- originate | adv-router <ip-address>}]

- show ip ospf [vrf <name>] [area-id] database { asbr-summary | external | network | nssa-external | opaque-area | opaque-as | opaque-link | router | summary } [link-state-id] [{adv-router <ip-address> | self-originate}]

-show ip ospf redundancy

OSPF GCE Commands Descriptions

Command	Description
config terminal	Enters the Configuration mode
[no] router ospf [vrf <name>]	This command enables OSPF routing process and the no form of the command disables OSPF routing process. **vrf vrf <name>**: Name of the VRF instance. This value is a string of size 32. Defaults: vrf - default
router-id <router ip address>	This command sets the router-id for the OSPF process. **router ip address**: Specifies the OSPF router ID as an IP address NOTE: An arbitrary value for the ip-address for each router can be configured; however, each router ID must be unique. To ensure uniqueness, the router-id must match with one of the router's IP interface addresses.
[no] area <area-id> stability-interval <Interval-Value (0 - 0x7fffffff)>	Configures the Stability interval for NSSA and the no form of the command configures default Stability interval for NSSA. **area-id**: Area associated with the OSPF address range. It is specified as an IP address **stability-interval**: The number of seconds after an elected translator determines its services are no longer required, that it must continue to perform its translation duties Defaults: 40
[no] area <area-id> translation-role { always | candidate }	Configures the translation role for the NSSA and the no form of the command configures the default translation role for the NSSA. **area-id:** Area associated with the OSPF address range. It is specified as an IP address **translation-role**: An NSSA Border router's ability to perform NSSA Translation of Type-7 LSAs to Type-5 LSAs. **Always**: Translator role where the Type-7 LSAs are always translated into Type-5 LSAs **Candidate**: Translator role where an NSSA border router participates in the translator election process Defaults: candidate
[no] compatible rfc1583	Sets OSPF compatibility list compatible with RFC 1583 and the no form of the command disables RFC 1583 compatibility. Defaults: Enabled
abr-type {standard | cisco | ibm}	Sets the Alternative ABR Type. **Standard**: Standard ABR type as defined in RFC 2328 **Cisco**: CISCO ABR type as defined in RFC 3509 **Ibm**: IBM ABR type as defined in RFC 3509 Defaults: standard
[no] neighbor <neighbor-id> [priority <priority value (0-255)>]	Specifies a neighbor router and its priority. The no form of the command removes the neighbour /Set default value for the Neighbor Priority. **neighbor-id**: Neighbor router ID **priority**: A number value that specifies the router priority Defaults: priority - 1
[no] area <area-id> default-cost <cost> [tos <tos value(0-30)>]	Specifies a cost for the default summary route sent into a stub or NSSA and the no form of the command removes the assigned default route cost. **area-id**: Area associated with the OSPF address range. It is specified as an IP address **default-cost**: Cost for the default summary route used for a stub area **tos**: Type of Service of the route being configured Defaults: default-cost - 10 tos - 0

Command	Description
area <area-id> nssa [{ no-summary | default-information-originate [metric <value>] [metric-type <Type(1-3)>] [tos <tos value (0-30)>]}]	Configures an area as a NSSA and other parameters related to that area. **area-id**: Area associated with the OSPF address range. It is specified as an IP address **nssa**: Configures an area as a not-so-stubby area (NSSA) **no-summary**: Allows an area to be a not-so-stubby area but not have summary routes injected into it **default-information-originate**: Default route into OSPF **metric**: The Metric value applied to the route before it is advertised into the OSPF domain. **metric-type**: The Metric Type applied to the route before it is advertised into the OSPF domain. **tos**: Type of Service of the route being configured Defaults: metric - 10 metric-type - 1 tos - 0
[no] area <area-id> stub [no-summary]	Specifies an area as a stub area and other parameters related to that area and the no form of the command removes an area or converts stub/nssa to normal area. **area-id**: Area associated with the OSPF address range. It is specified as an IP address **stub**: Configures an area as a stub area. **Nssa**: Configures an area as a Not-So-Stubby Area (NSSA).
[no] default-information originate always [metric <metric-value (0-0xffffff)>] [metric-type <type (1-2)>]	Enables generation of a default external route into an OSPF routing domain and other parameters related to that area. The no form of the command disables generation of a default external route into an OSPF routing domain. **Metric**: The Metric value applied to the route before it is advertised into the OSPF Domain **metric-type**: The Metric Type applied to the route before it is advertised into the OSPF Domain Defaults: metric - 10 metric-type - 2
[no] area <area-id> virtual-link <router-id>[authentication { simple |message-digest | null}] [hello-interval <value (1-65535)>][retransmit-interval <value(0-3600)>] [transmit-delay <value (0-3600)>] [dead-interval <value>] [{authentication-key <key (8)> | message-digest-key <Key-id (0-255)> md5 <key(16)>}]	Defines an OSPF virtual link and its related parameters. The no form of removes an OSPF virtual link. **area-id**: The Transit Area that the Virtual Link traverses. It is specified as an IP address **virtual-link**: The Router ID of the Virtual Neighbor **authentication**: The authentication type for an interface **hello-interval**: The interval between hello packets that the software sends on the OSPF virtual link interface **retransmit-interval**: The time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the OSPF virtual link interface **transmit-delay**: The time the router will stop using this key for packets generation **dead-interval**: The interval at which hello packets must not be seen before its neighbors declare the router down (the range of values for the dead interval is 0–0x7fffffff) **authentication-key**: Identifies the secret key used to create the message digest appended to the OSPF packet **message-digest-key**: OSPF MD5 authentication. Enables Message Digest 5 (MD5) authentication on the area specified by the area-id **md5**: The secret key which is used to create the message digest appended to the OSPF packet Defaults: Authentication - null hello-interval - 10 retransmit-interval - 5 transmit-delay - 1 dead-interval - 40
[no] ASBR Router	Specifies this router as ASBR. The no form of the command disables this router as ASBR.

Command	Description
[no] area <AreaId> range<Network> <Mask> {summary | Type7} [{advertise | not-advertise}] [tag <value>]	Consolidates and summarizes routes at an area boundary. The no form of the command deletes the Summary Address. **Area-id**: Area associated with the OSPF address range. It is specified as an IP address **Range**: OSPF address range **Network**: The IP address of the Net indicated by the range **Mask**: The subnet mask that pertains to the range **Summary**: Summary LSAs **Type7**: Type-7 LSA **Advertise**: When associated areaId is 0.0.0.0, aggregated Type-5 are generated. Otherwise if associated areaId is x.x.x.x (other than 0.0.0.0) aggregated Type-7 is generated in NSSA x.x.x.x Defaults: tag - 2
[no] summary-address <Network> <Mask> <AreaId> [{allowAll | denyAll | advertise | not-advertise}] [Translation {enabled | disabled}]	Creates aggregate addresses for OSPF and the no form of the command deletes the External Summary Address. **Network**: The IP address of the Net indicated by the range **Mask**: The subnet mask that pertains to the range **AreaId**: Area associated with the OSPF address range. It is specified as an IP address **allowAll**: When set to allowAll and associated areaId is 0.0.0.0 aggregated Type-5 are generated for the specified range. In addition aggregated Type-7 are generated in all attached NSSA, for the specified range **denyAll**: When set to denyAll neither Type-5 nor Type-7 will be generated for the specified range **advertise**: When associated areaId is 0.0.0.0, aggregated Type-5 are generated. Otherwise if associated areaId is x.x.x.x(other than 0.0.0.0) aggregated Type-7 is generated in NSSA x.x.x.x **not-advertise**: When associated areaId is 0.0.0.0, Type-5 is not generated for the specified range, while aggregated Type-7 are generated in all attached NSSA. While associated areaId is x.x.x.x(other than 0.0.0.0), Type-7 are not generated in NSSA x.x.x.x for the specified range **Translation**: Indicates how an NSSA Border router is performing NSSA translation of Type-7 to into Type-5 LSAs. When set to enabled, P Bit is set in the generated Type-7 LSA. When set to disabled P Bit is cleared in the generated Type-7 LSA for the range Defaults: summary-address - advertise translation - disabled
[no] redistribute {static | connected | rip | bgp | all} [route-map <name(1-20)>]	Configures the protocol from which the routes have to be redistributed into OSPF and the no form of the command disables redistribution of routes from the given protocol into OSPF. **Static**: Redistributes routes, configured statically, to the OSPF routing protocol **Connected**: Redistributes directly connected network routes, to the OSPF routing protocol **Rip**: Redistributes routes, that are learnt by the RIP process, to the OSPF routing protocol **Bgp**: Redistributes routes, that are learnt by the BGP process, to the OSPF routing protocol **All**: Redistributes all routes to the OSPF routing protocol **route-map**: Identifies the specified route-map in the list of route-maps. The length of the name ranges from 1 to 20.
[no] distribute-list route-map <name(1-20)> in	Enables inbound filtering for routes. The no form of the command disables inbound filtering for the routes. **Name**: Name of the Route Map for which inbound filtering should be enabled. This value is a string of size 20.
[no] redist-config <Network> <Mask> [metric-value <metric (1 - 16777215)>] [metric-type {asExttype1 | asExttype2}] [tag <tag-value>}	Configures the information to be applied to routes learnt from RTM and the no form of the command deletes the information applied to routes learnt from RTM. **Network**: IP Address of the Destination route **Mask**: Mask of the Destination route **metric-value**: The Metric value applied to the route before it is advertised into the OSPF Domain **metric-type**: The Metric Type applied to the route before it is advertised into the OSPF Domain **tag**: The Tag Type describes whether Tags will be automatically generated or will be manually configured Defaults: metric-value - 10 metric-type - asExttype2 tag - manual

Command	Description
[no] capability opaque	Enables the capability of storing opaque LSAs. The no form of the command disables the opaque capability. Defaults: Opaque capability is disabled
[no] nsf ietf restart-support [plannedOnly]	Enables the graceful restart support. Graceful restart support is provided for both unplanned and planned restart, if the command is executed without any option. The no form of the command disables the graceful restart support. **plannedOnly**: Supports only the planned restarts (such as restarting a control plane after a planned downtime). Defaults: Graceful restart support is disabled.
[no] nsf ietf restart-interval <grace period(1-1800)>	Configures the OSPF graceful restart timeout interval. This value specifies the graceful restart interval, in seconds, during which the restarting router has to reacquire OSPF neighbors that are fully operational prior to the graceful restart. The value ranges between 1 and 1800 seconds. The value is provided as an intimation of the grace period to all neighbors. The no form of the command resets the interval to default value. Defaults: 120
[no] nsf ietf helper-support [{unknown | softwareRestart | swReloadUpgrade | switchToRedundant}]	Enables the helper support. The helper support is enabled for all the options, if the command is executed without any option. The helper support can be enabled for more than one option, one after the other. The no form of the command disables the helper support. The helper support is disabled for all the options, if the command is executed without any option. **Unknown**: Enables / disables helper support for restarting of system due to unplanned events (such as restarting after a crash). **softwareRestart**: Enables / disables helper support for restarting of system due to restart of software. **swReloadUpgrade**: Enables / disables helper support for restarting of system due to reload or upgrade of software. **switchToRedundant**: Enables / disables helper support for restarting of system due to switchover to a redundant support processor. Defaults: Helper support is enabled
nsf ietf helper gracetimelimit <gracelimit period(0-1800)>	Configures the grace period till which the router acts as Helper. During this period, the router advertises that the restarting router is active and is in FULL state. The value ranges between 0 and 1800 seconds. Defaults: 0
[no] nsf ietf helper strict-lsa-checking	Enables the strict LSA check option in helper. The strict LSA check option allows the helper to terminate the graceful restart, once a changed LSA that causes flooding during the restart process is detected. The no form of the command disables the strict LSA check option in helper. Defaults: Strict LSA check option is disabled in helper.
[no] nsf ietf grace lsa ack required	Enables Grace Ack Required state in restarter. The GraceLSAs sent by the router are expected to be acknowledged by peers, if the Grace Ack Required state is enabled. The no form of the command disables the Grace Ack Required state in restarter. Defaults: Grace Ack Required state is enabled in restarter.
nsf ietf grlsa retrans count <grlsacout (0-180)>	Configures the maximum number of retransmissions for unacknowledged GraceLSA. This value ranges between 0 and 180. Defaults: 2
nsf ietf restart-reason [{unknown | softwareRestart | swReloadUpgrade | switchToRedundant}]	Configures the reason for graceful restart. **Unknown**: System restarts due to unplanned events (such as restarting after a crash). **softwareRestart**: System restarts due to software restart. **swReloadUpgrade**: System restarts due to reloading / upgrading of software. **switchToRedundant**: System restarts due to switchover to a switchover to a redundant support processor. Defaults: unknown

Command	Description
[no] distance <1-255> [route-map <name(1-20)>]	Enables the administrative distance (that is, the metric to reach destination) of the routing protocol and sets the administrative distance value. The distance value ranges between 1 and 255. The administrative distance can be enabled for only one route map. The distance should be disassociated for the already associated route map, if distance needs to be associated for another route map. The no form of the command disables the administrative distance. **Name**: Name of the Route Map for which the distance value should be enabled and set. This value is a string of size 20. Defaults: 0 (Represents directly connected route)
[no] route-calculation staggering	Enables OSPF route calculation staggering feature and also sets the staggering interval to the last configured value. This feature staggers the OSPF route calculation at regular intervals for processing neighbor keep alive and other OSPF operations. The no form of the command disables OSPF route calculation staggering and removes the staggering interval. Defaults: OSPF route calculation staggering is enabled
route-calculation staggering-interval <milli-seconds (1000-0x7fffffff)>	Configures the OSPF route calculation staggering interval (in milliseconds). This value represents the time after which the route calculation is suspended for doing other OSPF operations. Defaults: 10000 (OSPF route calculation staggering interval is equal to Hello interval)
[no] network <Network number> area <area-id> [unnum Vlan <PortNumber> [switch <switch-name>]]	Defines the interfaces on which OSPF runs and the area ID for those interfaces. The no form of the command disables OSPF routing for interfaces defined and to remove the area ID of that interface. **Network number**: Network type **Area**: Area associated with the OSPF address range. It is specified as an IP address **unnum Vlan**: VLAN id for which no ip address is configured **switch<switch-nam**: Switch instance / Virtual switch. This value is a string of size 32.
set nssa asbr-default-route translator { enable| disable}	Enables/disables setting of P bit in the default Type-7 LSA generated by NSSA internal ASBR. **Enable**: When set to enabled, P-Bit is set in the generated Type-7 default LSA **Disable**: When set disabled, P-Bit is clear in the generated default LSA Defaults: disable
[no] passive-interface {vlan <vlan-id(1-4094)> [switch <switch-name>] | <interface-type> <interface-id>}	Suppresses routing updates on an interface and the no form of the command enables routing updates on an interface. **vlan-id**: LSA retransmissions for adjacencies belonging to the VLAN interface. This value ranges between 1 and 4094. **switch<switch-name>**: Switch instance / Virtual switch. This value is a string of size 32. **interface-type**: Interface Type **interface-id:** Interface Identifier
[no] passive-interface default	Suppresses routing updates on all interfaces and the no form of the command enables routing updates on all interfaces.
interface vlan <vlan ID>	Entering to the relevant vlan to be configured
[no] ip ospf demand-circuit	Configures OSPF to treat the interface as an OSPF demand circuit and the no form of the command removes the demand circuit designation from the interface.
[no] ip ospf transmit-delay <seconds (0 - 3600)>	Sets the estimated time it takes to transmit a link state update packet on the interface and the no form of the command sets the default estimated time it takes to transmit a link state update packet on the interface. Defaults: 1
[no] ip ospf priority <value 0 - 255)>	Sets the router priority and the no form of the command sets default value for router priority. NOTE: When two routers attached to a network attempt to become the designated router, the one with the higher router priority takes precedence. If there is a tie, the router with the higher router ID takes precedence. Defaults: 1
[no] ip ospf hello-interval <seconds (1 - 65535)>	Specifies the interval between hello packets sent on the interface and the no form of the command sets default value for, interval between hello packets sent on the interface. NOTE: This value must be the same for all routers attached to a common network. Defaults: 10

Command	Description
[no] ip ospf dead-interval <seconds (0-0x7fffffff)>	Sets the interval at which hello packets must not be seen before neighbors declare the router down and the no form of the command sets default value for the interval at which hello packets must not be seen before neighbors declare the router down. NOTE: This value must be the same for all routers and access servers on a specific network. Defaults: 40
[no] ip ospf cost <cost (1-65535)> [tos <tos value (0-30)>]	Explicitly specifies the cost of sending a packet on an interface and the no form of the command resets the path cost to the default value. **Cost**: Type 1 external metrics which is expressed in the same units as OSPF interface cost, that is in terms of the OSPF link state metric **Tos**: Type of Service of the route being configured Defaults: 0
[no] ip ospf network {broadcast | non-broadcast | point-to-multipoint | point-to-point}	Configures the OSPF network type to a type other than the default for a given media and the no form of the command sets the OSPF network type to the default type. **Broadcast**: Networks supporting many (more than two) attached routers, together with the capability to address a single physical message to all of the attached routers (broadcast) **non-broadcast**: Networks supporting many (more than two) routers, but having no broadcast capability **point-to-multipoint**: Treats the non-broadcast network as a collection of point-to-point links **point-to-point**: A network that joins a single pair of routers Default: broadcast
[no]ip ospf authentication-key <password (8)>	Specifies a password to be used by neighboring routers that are using the OSPF simple password authentication. The no form of the command removes a previously assigned OSPF password.
[no] ip ospf authentication [{message-digest | null}]	Specifies the authentication type for an interface and the no form of the command removes the authentication type for an interface and set it to NULL authentication. **message-digest**: Message Digest authentication **null**: NULL authentication Defaults: null
[no] ip ospf message-digest-key <Key-ID (0-255)> md5 <md5-Key (16)>	Enables OSPF MD5 authentication and the no form of the command removes an old MD5 key. **Key-ID**: Identifies the secret key, which is used to create the message digest appended to the OSPF packet **md5**: Secret key, which is used to create the message digest appended to the OSPF packet
[no] debug ip ospf [vrf <name>] { pkt { hp | ddp | lrq | lsu | lsa } | module { adj_formation | ism | nsm | config | interface | restarting-router | helper }}	Sets the OSPF debug level. and the no form of the command removes an old MD5 key. **vrf<name>]**: Name of the VRF instance. This value is a string of size 32. **Pkt**: Packet High Level Dump debug messages **Hp**: Hello packet debug messages **Ddp**: DDP packet debug messages **Lrq**: Link State Request Packet debug messages **Lsu**: Link State Update Packet debug messages lsa Link State Acknowledge Packet debug messages **Module**: RTM Module debug messages **adj_formation**: Adjacency formation debug messages **ism**: Interface State Machine debug messages **nsm**: Neighbor State Machine debug messages **config**: Configuration debug messages **interface**: Interface **restarting-router**: Debug messages related to restarting router **helper**: Debug messages related to router in helper mode **all**: All debug messages Defaults: vrf - default
show ip ospf [vrf <name>] interface [{ vlan <vlan-id (1-4094)> [switch <switch-name>] | <interface-type> <interface-id> }]	Displays OSPF interface information. **vrf<name>**: Name of the VRF instance. This value is a string of size 32. **Vlan**: LSA retransmissions for adjacencies belonging to the VLAN interface. This value ranges between 1 and 4094. **switch<switch-name>**: Switch instance / Virtual switch. This value is a string of size 32. **interface-type**: Interface Type **interface-id**: Interface Identifier Defaults: vrf - default

Command	Description
show ip ospf [vrf <name>] neighbor [{ vlan <vlan-id (1-4094)> [switch <switch-name>] | <interface-type> <interface-id> }] [Neighbor ID] [detail]	Displays OSPF neighbor information list. **vrf<name>**: Name of the VRF instance. This value is a string of size 32. **Vlan**: LSA retransmissions for adjacencies belonging to the VLAN interface. This value ranges between 1 and 4094. **Switch <switch-name>]**: Switch instance / Virtual switch. This value is a string of size 32. **Neighbor ID**: Neighbor router ID **Detail**: OSPF Neighbor information in detail **interface-type**: Interface Type **interface-id**: Interface Identifier Defaults: vrf - default
show ip ospf [vrf <name>] request-list [<neighbor-id>] [{ vlan <vlan-id (1- 4094)> [switch <switch-name>] | <interface-type> <interface-id> }]	Displays OSPF Link state request list information. **vrf<name>]**: Name of the VRF instance. This value is a string of size 32. **neighbor-id**: Neighbor router ID **vlan**: LSA retransmissions for adjacencies belonging to the VLAN interface. This value ranges between 1 and 4094. **switch<switch-name>]**: Switch instance / Virtual switch. This value is a string of size 32. **interface-type**: Interface Type **interface-id**: Interface Identifier Defaults: vrf - default
show ip ospf [vrf <name>] retransmission-list [<neighbor-id>] [{ vlan <vlan-id (1-4094)> [switch <switch-name>] | <interface-type> <interface-id> }]	Displays OSPF Link state retransmission list information. **Vrf<name>]**: Name of the VRF instance. This value is a string of size 32. **neighbor-id**: Neighbor router ID **vlan**: LSA retransmissions for adjacencies belonging to the VLAN interface. This value ranges between 1 and 4094. **switch<switch-name>]**: Switch instance / Virtual switch. This value is a string of size 32. **interface-type**: Interface Type **interface-id:** Interface Identifier Defaults: vrf - default
show ip ospf [vrf <name>] virtual-links	Displays OSPF Virtual link information. **vrf< name>]**: Name of the VRF instance. This value is a string of size 32. Defaults: vrf - default
show ip ospf [vrf <name>] border-routers	Displays OSPF Border and Boundary Router Information. **vrf<name>]**: Name of the VRF instance. This value is a string of size 32. Defaults: vrf - default
show ip ospf [vrf <name>] {area-range | summary-address}	Displays OSPF summary-address redistribution Information. **vrf< name>]**: Name of the VRF instance. This value is a string of size 32. **area-range**: Area associated with the OSPF address range. It is specified as an IP address **summary-address**: Aggregate addresses for OSPF Defaults: vrf - default
show ip ospf [vrf <name>]	Displays general information about the OSPF routing process. **vrf< name>]**: Name of the VRF instance. This value is a string of size 32. Defaults: vrf - default
show ip ospf [vrf <name>] route	Displays routes learnt by OSPF process. **vrf< name>]**: Name of the VRF instance. This value is a string of size 32. Defaults: vrf - default
show ip ospf [vrf <name>] [area-id] database [{database-summary | self-originate | adv-router <ip-address>}]	Displays OSPF LSA Database summary. **vrf< name>]**: Name of the VRF instance. This value is a string of size 32. **area-id**: Area associated with the OSPF address range. It is specified as an IP address. **Database**: Displays how many of each type of LSA for each area there are in the database **database-summary**: Displays how many of each type of LSA for each area there are in the database, and the total number of LSA types **self-originate**: Displays only self-originated LSAs (from the local router) **adv-router**: Displays all the specified router link-state advertisements (LSAs). If no IP address is included, the information is about the local router itself Defaults: vrf - default

Command	Description
show ip ospf [vrf <name>] [area-id] database { asbr-summary | external | network | nssa-external | opaque-area | opaque-as | opaque-link | router | summary } [link-state-id] [{adv-router <ip-address> | self-originate}]	Displays OSPF Database summary for the LSA type. **vrf< name>]**: Name of the VRF instance. This value is a string of size 32. **area-id**: Area associated with the OSPF address range. It is specified as an IP address **database**: Displays how many of each type of LSA for each area there are in the database **asbr-summary**: Displays information only about the Autonomous System Boundary Router (ASBR) summary LSAs **external**: Displays information only about the external LSAs **network**: Displays information only about the network LSAs **nssa-external**: Displays information about the NSSA external LSAs **opaque-area**: Displays information about the Type-10 LSAs **opaque-as**: Displays information about the Type-11 LSAs **opaque-link**: Displays information about the Type-9 LSAs **router**: Displays information only about the router LSAs **summary**: Displays information only about the summary LSAs **link-state-id**: Portion of the Internet environment that is being described by the advertisement. The value entered depends on the type of the LSA. The value must be entered in the form of an IP address **adv-router**: Displays all the specified router link-state advertisements (LSAs). If no IP address is included, the information is about the local router itself **self-originate**: Displays only self-originated LSAs (from the local router) Defaults: vrf - default
show ip ospf redundancy	Displays OSPFv2 redundancy information.

OSPF ACE Commands Hierarchy

+ application connect

- router interface {create | remove} <IP address> [netmask] [vlan id]

+ router ospf

- enable

+ configure terminal

+ router ospf

- [no] area { A.B.C.D | < metric id ,(0-4294967295)> }

- [no] router-id < A.B.C.D >

- [no] network { A.B.C.D/M | <interface name ,eth1.(id)> }

- [no] passive-interface <interface name,eth1.(id)>

- [no] redistribute {connected | static}

- [no] neighbor A.B.C.D

- write

- exit

- exit

    - show running-config

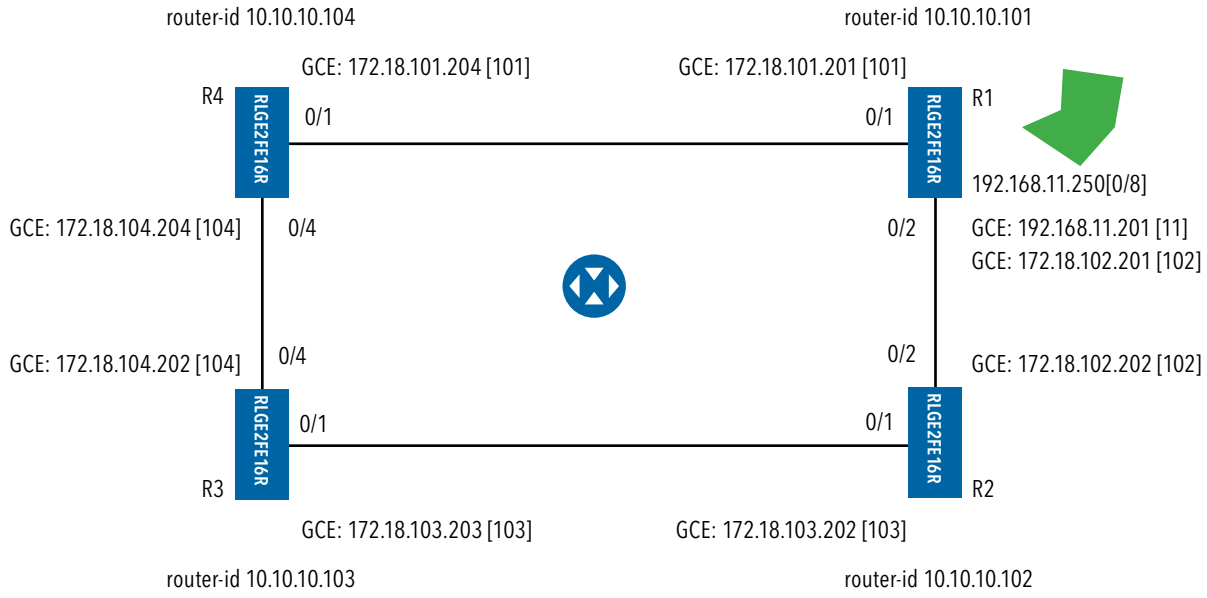
- show ip ospf [border-routers| database| interface| neighbor|route]

OSPF ACE Commands Descriptions

Command	Description
Application connect	Enters the Configuration mode
router interface	
create | remove	Add or Remove an IP interface for the application engine. The configuration should include: Address-prefix : IP address in the format aa.bb.cc.dd/xx VLAN : vlan ID that the application engine will use for this IP interface The interface will be name eth1.<vlan id>
Router ospf	enable
Configure terminal	Enter configuration mode
Router ospf	area – OSPF area parameters given in A.B.C.D format or as a metric id (0-4294967295). router-id – router-id for the OSPF process given in A.B.C.D format. network – Enable routing on an IP network . Network can be given as A.B.C.D/M or as a name of a preconfigured interface eth1.<vlan id>. passive-interface – Suppress routing updates on an interface, given as a name of a preconfigured interface eth1.<vlan id>. redistribute – Redistribute information from another routing protocol. neighbor – Specify a neighbor router. given as A.B.C.D/M . write – commit and preserve configuration

OSPF setup example

Below setup example and configuration will allow L3 OSPF based protection over the closed network. The PC should be set with default gateway to be R1 interface 192.168.1.201 and will then be available to all other subnets.



R1 configuration

1. Set host name (optional)

```
set host-name R1
```

2. disable spanning tree

```
config
no spanning-tree
exit
```

3. remove network ports from default vlan 1

```
vlan 1
no ports fa 0/1-2 untagged fa 0/1-2
exit
```

4. assign vlans and corresponding IP interfaces

```
vlan 101
ports fastethernet 0/1
exit
vlan 102
ports fastethernet 0/2
exit
vlan 11
port fastethernet 0/8 untagged fastethernet 0/8 name lan
exit
interface vlan 101
shutdown
ip address 172.18.101.201 255.255.255.0
no shutdown
exit
interface vlan 102
shutdown
ip address 172.18.102.201 255.255.255.0
no shutdown
exit
interface vlan 11
shutdown
ip address 192.168.11.201 255.255.255.0
```

```
no shutdown
exit
```

5. Set PVID to the lan PC (untagged access device)

```
interface fastethernet 0/8
switchport pvid 11
exit
```

6. configure OSPF

```
router ospf
router-id 10.10.10.101
network 172.18.101.201 255.255.255.0 area 0.0.0.0
network 172.18.102.201 255.255.255.0 area 0.0.0.0
network 192.168.11.201 255.255.255.0 area 0.0.0.0
passive-interface vlan 11
end
write startup-cfg
```

R2 configuration

1. Set host name (optional)

```
set host-name R2
```

2. disable spanning tree

```
config
no spanning-tree
exit
```

3. remove network ports from default vlan 1

```
config
vlan 1
no ports fa 0/2,0/3 untagged fa 0/2-3
exit
```

4. assign vlans and corresponding IP interfaces

```
vlan 102
ports fastethernet 0/2
exit
vlan 103
ports fastethernet 0/3
exit
interface vlan 102
shutdown
ip address 172.18.102.202 255.255.255.0
no shutdown
exit
interface vlan 103
shutdown
ip address 172.18.103.202 255.255.255.0
no shutdown
exit
```

5. configure OSPF

```
router ospf
router-id 10.10.10.102
network 172.18.102.202 255.255.255.0 area 0.0.0.0
network 172.18.103.202 255.255.255.0 area 0.0.0.0
end
write startup-cfg
```

R3 configuration

1. Set host name (optional

```
set host-name R3
```

2. disable spanning tree

```
config
no spanning-tree
exit
```

3. remove network ports from default vlan 1

```
config
vlan 1
no ports fa 0/4,0/3 untagged fa 0/3-4
exit
```

4. assign vlans and corresponding IP interfaces

```
vlan 103
ports fastethernet 0/3
exit
vlan 104
ports fastethernet 0/4
exit
interface vlan 103
shutdown
ip address 172.18.103.203 255.255.255.0
no shutdown
exit
interface vlan 104
shutdown
ip address 172.18.104.203 255.255.255.0
no shutdown
exit
```

5. configure OSPF

```
router ospf
router-id 10.10.10.103
network 172.18.104.203 255.255.255.0 area 0.0.0.0
network 172.18.103.203 255.255.255.0 area 0.0.0.0
end
write startup-cfg
```

R4 configuration

1. Set host name (optional)

```
set host-name R4
```

2. disable spanning tree

```
config
no spanning-tree
exit
```

3. remove network ports from default vlan 1

```
config
vlan 1
no ports fa 0/4,0/1 untagged fa 0/1,0/4
exit
```

4. assign vlans and corresponding IP interfaces

```
vlan 101
ports fastethernet 0/1
exit
vlan 104
ports fastethernet 0/4
exit
interface vlan 101
shutdown
ip address 172.18.101.204 255.255.255.0
no shutdown
exit
interface vlan 104
shutdown
ip address 172.18.104.204 255.255.255.0
no shutdown
exit
```

5. configure OSPF

```
router ospf
router-id 10.10.10.104
network 172.18.104.204 255.255.255.0 area 0.0.0.0
network 172.18.101.204 255.255.255.0 area 0.0.0.0
end
write startup-cfg
```

VRRP

Virtual Router Redundancy Protocol (VRRP)is supported at the unit providing a virtual gateway to IP hosts connected and thus achieving higher reliability and availability.

VRRP (Virtual Router Redundancy Protocol) is an election protocol that dynamically assigns responsibility for one or more virtual router(s) to the VRRP routers(s) on a LAN, allowing several routers on a multi-access link to utilize the same virtual IP address. A VRRP router is configured to run the VRRP protocol in conjunction with one or more other routers attached to a LAN. In a VRRP setup, one router is elected as the local router with the other routers acting as backups in case of the failure of the local router.

VRRP is designed to eliminate the single point of failure inherent in the static default routed environment

VRRP Commands Hierarchy

+root

+ router vrrp

- auth-deprecate {enable | disable}

+ [no] interface vlan <vlan-id>

- vrrp <vrid(1-255)> ipv4 <ip_addr> [secondary]

- vrrp <vrid(1-255)> preempt [delay minimum <value(0-30)>]

- vrrp <vrid(1-255)> priority <priority(1-254)>

- vrrp <vrid(1-255)> text-authentication <password>

- vrrp <vrid(1-255)> timer [msec] <interval(1-255)secs>

- vrrp <vrid(1-255)> timers advertise [msec] <interval(1-255)secs>

- vrrp <vrid(1-255)> authentication {text <password> | none}

- vrrp group shutdown

- show vrrp [interface vlan <vlan-id>] [{brief|detail |statistics}]

- show running-config vrrp

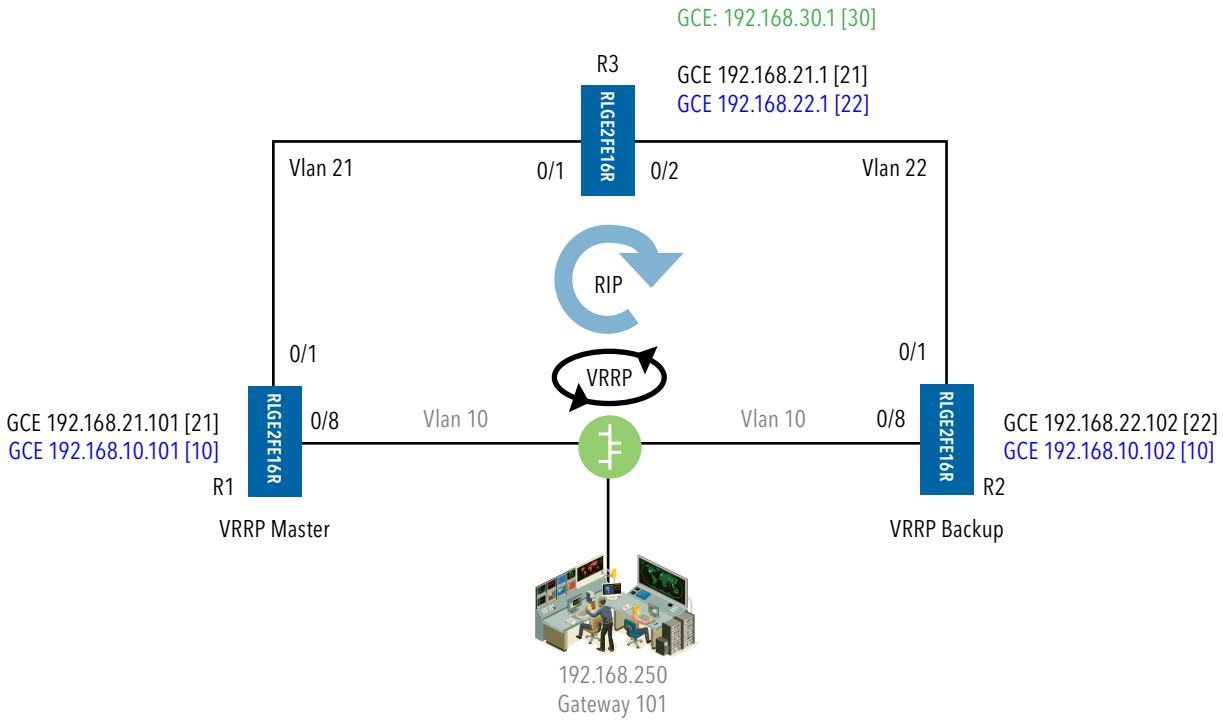
VRRP Commands Descriptions

Command	Description
Config	Enters the Global Configuration mode
[no] router vrrp	Enables/ disables VRRP in the router. Enabling the VRRP router will transition the state of the virtual router from 'initialize' to 'backup' or 'local' (Initialize indicates that the virtual router is waiting for a startup event. Backup indicates that the virtual router is monitoring the availability of the local router Master indicates that the virtual router is forwarding the packets for IP addresses that are associated with this router.). Disabling the VRRP router will transition the state from 'backup' or 'local' to 'initialize'. State transitions may not be immediate but may depend on other factors such as the interface state.
auth-deprecate	VRRP auth deprecation flag. enable |disable
Interface {vlan <id> }	Enter a specific IP vlan interface level. The interface must be preconfigured
Vrrp (1-255)	Virtual router ID
authentication	None : No authentication Text : Clear text authentication
ipv4 <> [secondary]	Sets the associated IP addresses for the virtual router. The no form of the command deletes the associated IP addresses for the virtual router. Once this command is executed, the VRRP Module starts the transition from "Initial" state to either "Backup" state or "Master" state as per the election process on the specific interface. This command should precede any other interface command for this vrid. If the 'secondary' attribute is added and the IP interface is the router own vlan interface, the router will be set as the vrrp local at the given ID.
Preempt	Preempt mode related configuration. delay minimum (0-30). Number of seconds that the router will delay before issuing an advertisement claiming local ownership.
Priority (1-254)	Priority used for the virtual router local election process. Higher values imply higher priority A priority of 255 is used for the router that owns the associated IP address (es) The command vrrp <vrid(1-255)> ipv4 <ip address> must be entered for the current interface (with the proper vrid) before the execution of this command
text-authentication	
<random_str>	Simple password authentication related configuration. <random_str> . Authentication password used to validate the incoming VRRP packets
Timer	Time interval, in seconds/milliseconds, between successive advertisement messages. permissible values :(1-255secs)/(100-255000msecs). msec : Unit is changed to milliseconds
Timers advertise	Time interval, in seconds/milliseconds, between successive advertisement messages. permissible values :(1-255secs)/(100-255000msecs). msec : Unit is changed to milliseconds

Example 1

Following is a configuration example of a VRRP together with RIP.

Setup drawing



Configuration

Router R1 configuration (Master router)

1. Set vlans and assign ports

```
set host-name R1
config t
no spanning-tree
vlan 1
no ports
exit
interface vlan 1
shutdown
no ip address
exit
vlan 10
 ports fastethernet 0/7-8  gigabitethernet 0/3 untagged fastethernet 0/7-8 name LAN
 exit
vlan 21
 ports fastethernet 0/1 name RIP
```

```
 exit
interface fastethernet 0/1
 alias NNI
 switchport pvid 21
 exit
interface fastethernet 0/7
 alias VRRP
 switchport pvid 10
 exit
interface fastethernet 0/8
 alias UNI
 switchport pvid 10
exit
```

2. Set ip interfaces AND rip

```
interface vlan 11
interface vlan 10
 ip address 192.168.10.101 255.255.255.0
 no shut
 exit
interface vlan 21
 ip address 192.168.21.101 255.255.255.0
 no shut
 exit
router rip
 network 192.168.21.101
 network 192.168.10.101
 passive-interface vlan 10
exit
```

3. set vrrp instance (local router)

```
router vrrp
interface vlan 10
  vrrp 1 ipv4 192.168.10.101
  vrrp 1 ipv4 192.168.10.101 secondary
exit
write startup-cfg
Router R2 configuration
```

```
1.    Set vlans and assign ports
set host-name R2
config t
no spanning-tree
vlan 1
no ports
exit
interface vlan 1
shutdown
no ip address
exit
vlan 10
 ports fastethernet 0/7-8  gigabitethernet 0/3 untagged fastethernet 0/7-8 name LAN
 exit
vlan 22
 ports fastethernet 0/1 name RIP
 exit
interface fastethernet 0/1
 alias NNI
 switchport pvid 22
 exit
interface fastethernet 0/7
 alias VRRP
 switchport pvid 10
 exit
interface fastethernet 0/8
 alias UNI
 switchport pvid 10
exit
```

2. Set ip interfaces

```
interface vlan 11
interface vlan 10
 ip address 192.168.10.102 255.255.255.0
 no shut
 exit
interface vlan 22
 ip address 192.168.22.102 255.255.255.0
 no shut
 exit
```

```
router rip
 network 192.168.22.102
 network 192.168.10.102
 passive-interface vlan 10
exit
```

3. set vrrp instance

```
router vrrp
interface vlan 10
  vrrp 1 ipv4 192.168.10.102
  vrrp 1 ipv4 192.168.10.101 secondary
exit
write startup-cfg
```

Router R3 configuration

```
set host-name R3
config t
no spanning-tree
vlan 1
no ports
exit
interface vlan 1
shutdown
no ip address
exit
vlan 21
 ports fastethernet 0/1
 exit
vlan 22
 ports fastethernet 0/2
 exit
vlan 30
 ports fastethernet 0/8 gigabit 0/3 untagged  fastethernet 0/8
 exit
interface fastethernet 0/1
 alias NNI
 switchport pvid 21
 exit
interface fastethernet 0/2
 alias NNI
 switchport pvid 22
```

```
 exit
interface vlan 21
 ip address 192.168.21.1 255.255.255.0
 no shut
 exit
interface vlan 22
 ip address 192.168.22.1 255.255.255.0
 no shut
 exit
interface vlan 30
 ip address 192.168.30.1 255.255.255.0
 no shut
 exit
router rip
 network 192.168.22.1
 network 192.168.21.1
 network 192.168.30.1
 passive-interface vlan 30
 exit
exit
write startup-cfg
```

Show at R1

```
R1# show vrrp

P indicates configured to preempt

Interface    vrID Priority   P   State     Master Addr      VRouter Addr
---------    ---- --------   -   -----     -----------      ------------
vlan10       1     255         P   Master    192.168.10.101   192.168.10.101

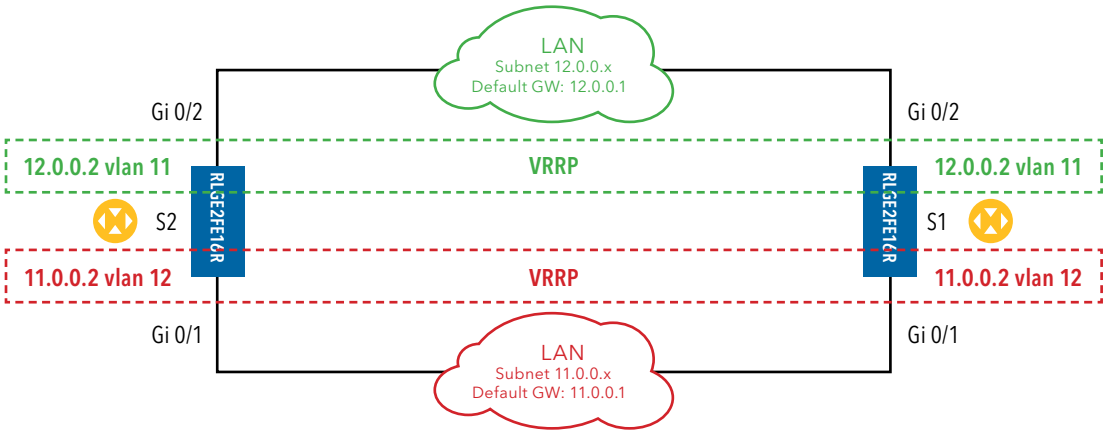
R1# show ip rip database

Vrf default
192.0.0.0/8   [1]          auto-summary
192.168.10.0/24  [1]          directly connected, vlan10
192.168.21.0/24  [1]          directly connected, vlan21
192.168.22.0/24  [2]          via 192.168.21.1, vlan21
192.168.30.0/24  [2]          via 192.168.21.1, vlan21
```

Example 2

Following is a configuration example of a VRRP multiple instance setup.

Setup drawing



Configuration

Switch S2 configuration (Master router)

1. Set VLANs and assign ports

```
config t
no spanning-tree
vlan 11
ports add gigabitethernet 0/1 untagged gigabitethernet 0/1
exit
interface gigabitethernet 0/1
switchport pvid 11
exit
vlan 12
ports add gigabitethernet 0/2 untagged gigabitethernet 0/2
exit
interface gigabitethernet 0/2
switchport pvid 12
exit
```

2. Set IP interfaces

```
interface vlan 11
ip address 11.0.0.1 255.0.0.0
no shutdown
exit
interface vlan 12
```

```
ip address 12.0.0.1 255.0.0.0
no shutdown
exit
```

3. set VRRP instance (local router)

```
router vrrp
interface vlan 11
vrrp 1 ipv4 11.0.0.1
vrrp 1 ipv4 11.0.0.1 secondary
exit
interface vlan 12
vrrp 1 ipv4 12.0.0.1
vrrp 1 ipv4 12.0.0.1 secondary
end
write startup-cfg
```

Switch S1 configuration

1. Set VLANs and assign ports

```
config t
no spanning-tree
vlan 11
ports add gigabitethernet 0/1 untagged gigabitethernet 0/1
exit
interface gigabitethernet 0/1
switchport pvid 11
exit
vlan 12
ports add gigabitethernet 0/2 untagged gigabitethernet 0/2
exit
interface gigabitethernet 0/2
switchport pvid 12
exit
```

2. Set IP interfaces

```
interface vlan 11
ip address 11.0.0.2 255.0.0.0
no shutdown
```

```
exit
interface vlan 12
ip address 12.0.0.2 255.0.0.0
no shutdown
exit
```

3. set VRRP instance

```
router vrrp
interface vlan 11
vrrp 1 ipv4 11.0.0.2
vrrp 1 ipv4 11.0.0.1 secondary
exit
interface vlan 12
vrrp 1 ipv4 12.0.0.2
vrrp 1 ipv4 12.0.0.1 secondary
end
write startup-cfg
```

RIPv2

RIP (Routing Information Protocol), is a distance-vector routing protocol, which employs the hop count as a routing metric.

RIPv2 protocol is supported in the application layer of the ComNet switch and as such the configuration is available in the ACE mode and related to IP interfaces configured in the application.

RIP routing and configuration is available at both GCE mode and ACE modes.

GCE RIP Commands Hierarchy

+root

+ config

+ [no] router rip

- [no] network { A.B.C.D}

- [no] passive-interface {vlan <vlan-id> | <interface-type> <interface-id>}

- [no] redistribute {connected | static |all}

- [no] neighbor A.B.C.D

- [no] default-metric (1-16)

- ip rip retransmission { interval <timeout-value (5-10)> | retries <value (10-40)> }

- version {1 |2 |1 2}

- clear

+ interface vlan <vlan id >

- [no] ip rip

- ip rip authentication mode { text | md5 } key-chain <key-chain-name (16)>

- send version {1 |2}

- receive version {1 |2}

- show ip rip database

- show ip rip statistics

- show running-config rip

GCE RIP Commands Descriptions

Command	Description
config	Enters the GCE mode
router rip	enter rip level network – Enable routing on an IP network. Network is be given as A.B.C.D. passive-interface – Suppress routing updates on an interface. given using the interface vlan id or the physical port. redistribute – Redistribute information from another routing protocol. neighbor – Specify a neighbor router. given as A.B.C.D . version – 1 |2. The default is to send RIPv2 while accepting both RIPv1 and RIPv2 (and replying with packets of the appropriate version for REQUESTS / triggered updates). The version to receive and send can be specified globally, and further overridden on a per-interface basis if needs be for send and receive separately (see below). It is important to note that RIPv1 cannot be authenticated. Further, if RIPv1 is enabled then RIP will reply to REQUEST packets, sending the state of its RIP routing table to any remote routers that ask on demand.
Interface vlan <vlan id>	Enter the VLAN IP interface level.
ip rip authentication	Key-chain : Specify Keyed MD5 chain. Mode : Set the interface with authentication method. **md5**- Set the interface with RIPv2 MD5 authentication. **text** - Set the interface with RIPv2 simple password authentication. String - sets authentication string. The string must be shorter than 16 characters.
ip rip send |receive	This interface command overrides the global rip version setting, and selects which version of RIP to send /receive packets with, for this interface specifically. Choice of RIP Version 1, RIP Version 2, or both versions. In the latter case, where '1 2' is specified, packets will be both broadcast and multicast. Default: Send packets according to the global version (version 2)

ACE RIP Commands Hierarchy

+root

+ application connect

- router interface {create | remove} <IP address> [netmask] [vlan id]

+ router rip

- enable

- exit

- show ip rip

+ configure terminal

+ [no] router rip

- [no] network { A.B.C.D/M | <interface name ,eth1.(id)> }

- [no] passive-interface <interface name,eth1.(id)>

- [no] redistribute {connected | static}

- [no] neighbor A.B.C.D

- version {1 |2}

- write

- exit

- show running-config

+ [no] interface < IFNAME>

- [no] ip rip

- authentication {key-chain <key>| mode {md5 |text}|string <string>}

- send version {1 |2| 1 2}

- receive version {1 |2| 1 2}

- split-horizon

- show running-config

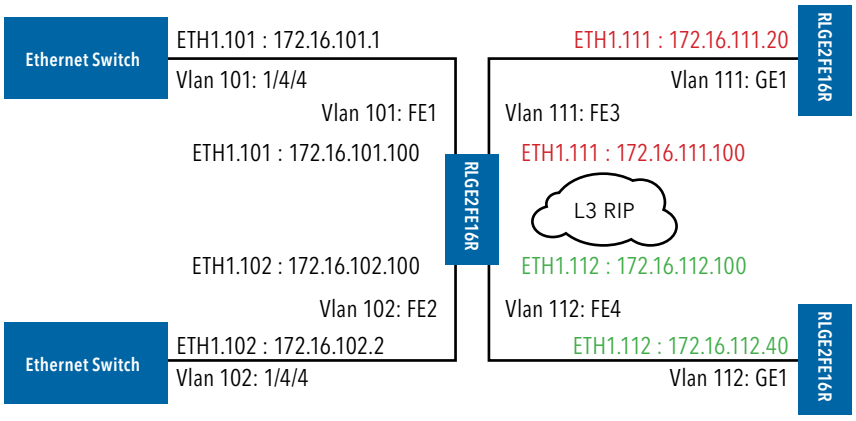
- exit

ACE RIP Commands Descriptions

Command	Description
Application connect	Enters the Configuration mode
router interface create | remove	Add or Remove an IP interface for the application engine. The configuration should include: Address-prefix : IP address in the format aa.bb.cc.dd/xx VLAN : vlan ID that the application engine will use for this IP interface The interface will be name eth1.<vlan id>
Router rip	enable
Configure terminal	Enter configuration mode
Router rip	network – Enable routing on an IP network. Network can be given as A.B.C.D/M or as a name of a preconfigured interface eth1.<vlan id>. passive-interface – Suppress routing updates on an interface. given as a name of a preconfigured interface eth1.<vlan id>. redistribute – Redistribute information from another routing protocol. neighbor – Specify a neighbor router. given as A.B.C.D/M . version – 1 |2. The default is to send RIPv2 while accepting both RIPv1 and RIPv2 (and replying with packets of the appropriate version for REQUESTS / triggered updates). The version to receive and send can be specified globally, and further overridden on a per-interface basis if needs be for send and receive separately (see below). It is important to note that RIPv1 cannot be authenticated. Further, if RIPv1 is enabled then RIP will reply to REQUEST packets, sending the state of its RIP routing table to any remote routers that ask on demand. write – commit and preserve configuration
Interface < IFNAME>	Enter the interface level. IFNAME can be for example eth1.x whereas x is the vlan identifier. Set a RIP enabled interface by ifname. Both the sending and receiving of RIP packets will be enabled on the port specified in the network ifname command. The no network ifname command will disable RIP on the specified interface
ip rip authentication	Key-chain : Specify Keyed MD5 chain. Mode : Set the interface with authentication method. **md5**- Set the interface with RIPv2 MD5 authentication. **text** - Set the interface with RIPv2 simple password authentication. String - sets authentication string. The string must be shorter than 16 characters.
ip rip send |receive	This interface command overrides the global rip version setting, and selects which version of RIP to send /receive packets with, for this interface specifically. Choice of RIP Version 1, RIP Version 2, or both versions. In the latter case, where '1 2' is specified, packets will be both broadcast and multicast. Default: Send packets according to the global version (version 2)
ip rip split-horizon	Control split-horizon on the interface. Default is ip split-horizon. If you don't perform split-horizon on the interface, please specify no ip split-horizon.

Example

Following example will detail how to configure the RLGE2FE16R as a router using the RIP protocol at the GCE.



Router configuration

1. Set host name (optional)

```
set host-name ROUTER
```

2. Create the subnet vlans

```
config
vlan 101
ports    gigabitethernet 0/3 fastethernet 0/1 untagged fastethernet 0/1
exit
vlan 102
ports    gigabitethernet 0/3 fastethernet 0/2 untagged fastethernet 0/2
exit
vlan 111
ports    gigabitethernet 0/3 fastethernet 0/3 untagged fastethernet 0/3
exit
vlan 112
ports    gigabitethernet 0/3 fastethernet 0/4 untagged fastethernet 0/4
exit
```

3. Assign PVID to the untagged ports

```
interface fastethernet 0/1
alias Net _ 101
      switchport pvid 101
```

```
exit
interface fastethernet 0/2
alias Net _ 102
switchport pvid 102
exit
interface fastethernet 0/3
alias Net _ 103
switchport pvid 103
exit
interface fastethernet 0/4
alias Net _ 104
switchport pvid 104
exit
end
```

4. Assign the Application IP interfaces

```
application connect
router interface create address-prefix 172.16.101.100/24 vlan 101 purpose application-host
router interface create address-prefix 172.16.102.100/24 vlan 102 purpose general
router interface create address-prefix 172.16.111.100/24 vlan 111 purpose general
router interface create address-prefix 172.16.112.100/24 vlan 112 purpose general
```

5. Configure the RIP

```
router rip
enable
configure terminal
router rip
network eth1.101
network eth1.102
network eth1.111
network eth1.112
write
end
exit
exit
show configuration and state
 [/] router interface show
+------+----------+------------------+-----------------+-------------+
```

```
| VLAN |    Name    |      IP/Subnet   |      Purpose     | Description |
+======+============+==================+==================+=============+
| 101  | eth1.101 | 172.16.101.100/24 | application host |             |
+------+----------+-------------------+------------------+-------------+
| 102  | eth1.102 | 172.16.102.100/24 |      general     |             |
+------+----------+-------------------+------------------+-------------+
| 111  | eth1.111 | 172.16.111.100/24 |      general     |             |
+------+----------+-------------------+------------------+-------------+
| 112  | eth1.112 | 172.16.112.100/24 |      general     |             |
+------+----------+-------------------+------------------+-------------+
[/] router route show
Kernel IP routing table
Destination      Gateway          Genmask          Flags Metric Ref    Use Iface
172.16.101.0     0.0.0.0          255.255.255.0    U     0      0        0 eth1.101
172.16.102.0     0.0.0.0          255.255.255.0    U     0      0        0 eth1.102
127.128.127.0    0.0.0.0          255.255.255.0    U     0      0        0 eth1
172.16.112.0     0.0.0.0          255.255.255.0    U     0      0        0 eth1.112
172.16.111.0     0.0.0.0          255.255.255.0    U     0      0        0 eth1.111
Completed OK
 [/] router rip
router/rip> show ip rip
Codes: R - RIP, C - connected, S - Static, O - OSPF, B - BGP
Sub-codes:
       (n) - normal, (s) - static, (d) - default, (r) - redistribute,
       (i) - interface
Network             Next Hop          Metric From             Tag Time
C(i) 172.16.101.0/24     0.0.0.0                1 self               0
C(i) 172.16.102.0/24     0.0.0.0                1 self               0
C(i) 172.16.111.0/24     0.0.0.0                1 self               0
C(i) 172.16.112.0/24     0.0.0.0                1 self               0
router/rip> show ip rip status
Routing Protocol is "rip"
  Sending updates every 30 seconds with +/-50%, next due in 12 seconds
  Timeout after 180 seconds, garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set
  Default redistribution metric is 1
  Redistributing:
  Default version control: send version 2, receive any version
    Interface         Send  Recv   Key-chain
```

```
    eth1.101           2      1 2
    eth1.102           2      1 2
    eth1.111           2      1 2
    eth1.112           2      1 2
  Routing for Networks:
    eth1.101
    eth1.102
    eth1.111
    eth1.112
  Routing Information Sources:
    Gateway           BadPackets BadRoutes   Distance Last Update
  Distance: (default is 120)
router/rip> exit
Connection closed by foreign host
[/]
```

Serial Ports and Services

The serial RS-232 connects legacy serial-based industrial devices to an Ethernet network. Each of the serial ports can be configured to work in one of these modes of operation:

1. Transparent tunneling
2. Terminal Server
3. Protocol Gateway.

The transparent tunneling has three types of implementations:

1. Transparent tunneling.
2. Transparent 9bit.
3. Bitstream.

NOTE: Configuration and management of the serial interfaces and services are done at the ACE

Serial interfaces

Depending on hardware variant available, up to 4 RS-232 ports may be available.

Services configuration structure

Below table group the relevant configuration areas which should be included per application type

Hierachy Level	Transparent Tunneling	Transparent 9Bit	BitStream	Terminal Server	101/104 Gateway
Router IP Interface	X	X	X	X	X
Serial Port	X	X	X	X	X
Serial Local end point	X	X	X	X	X
Serial Remote end point	Required if service is remote				
iec101-gw					X
termserver				X	

Below table details the state required for main configuration parameters depending on the used application.

Hierarchy Level	Configurable Parameter	Transparent Tunneling	Transparent 9bit	BitStream	Terminal Server	101/104 Gateway
Serial Port	mode-of-operation	transparent	transparent9bit	bitstream	transparent	transparent
Serial Local end point	application	Serial-tunnel	Serial-tunnel	Serial-tunnel	Terminal-server	iec101-gw

Below table group relevant configuration options to the different application modes.

Parameter	Transparent Tunneling	Transparent 9bit	BitStream	Terminal Server	101/104 Gateway
baudrate	X	X	X	X	X
databits	X	X		X	X
stopbits	X	X		X	X
allowed-latency	X	X	X	X	X
bus-idle-time	X	X		X	X
parity	X			X	X
dtr-dsr	X	X			
rts-cts	X	X			
local-dsr-delay	X	X			
local-cts-delay	X	X			
tx-delay			X		
bits-for-sync1			X		
bits-for-sync2			X		

Serial Commands Hierarchy

+ application connect

+ serial

-Service show

-serial local-end-point filter show

+ card

-auto-recover {enable |disable |show}

-show

+ port

- clear counters

- create {slot <1>} {port <1-4>}
  [baudrate <9600,(50-368400)>] databits {8,<5-8>}
  [parity {no,no| odd| even}] [stopbits <1,1|2>]
  [bus-idle-time <bits (30-1000>] [bus RS232]
  [mode-of-operation { transparent ,transparent| transparent9bit| bitstream}]
  [admin-status {up,up| down}][allowed-latency <20msec,(2-255)>]
  [rts-cts <disable,(enable |disable)>][dtr-dsr <disable,(enable |disable)>]
  [local-cts-delay <msec,(0 |5-255)>

[tx-delay <msec,(0-255)>][local-dsr-delay <msec,(0|(5-255)>
[bits-for-sync1 <0-255>] [bits-for-sync2 <0-255>]

- remove {slot <1>} {port <1-4>}

- update {slot <1>} {port <1-4>}
[baudrate <9600,(50-368400)>] [parity {no| odd| even}]
[stopbits <1|2>][bus-idle-time <bits (30-1000>] [bus RS232]
[mode-of-operation {transparent| transparent9bit| bitstream}]
[admin-status {up| down}][allowed-latency <20msec,(2-255)>]
[rts-cts <disable,(enable |disable)>][dtr-dsr <disable,(enable |disable)>]
[local-cts-delay <msec,(0 |5-255)>
[tx-delay <msec,(0-255)>][local-dsr-delay <msec,(0|(5-255)>
[bits-for-sync1 <0-255>] [bits-for-sync2 <0-255>]]

- show [slot <1> port <1-4>]

+ local-end-point

- create {slot <1>} {port <1-4>} {service-id <1-100>} {position <local| remote>} [protocol <any>]
[application {serial-tunnel |terminal-server |iec101-gw |modbus-gw}] [buffer-mode {byte| frame}]
[iec101-link-address <0-65535>] [iec101-link-address-len (2,<1|2>]
[iec101-originator-address {none| present}] [unit-id-len (2,<1|2>]
[unit-id <0-65535>]

- remove {slot <1>} {port <1-4>} {service-id <1-100>}

- show

+ tunnel settings

- update low-border-ip-port (9849, <1025- 65434>)

- show

+ remote-end-point

- create {remote-address <A.B.C.D>} {service-id <1-100>} {position <local| remote>} [buffer-mode
{byte| frame}] [connection-mode [<udp| tcp>]

- remove {remote-address < A.B.C.D>} {service-id <1-100>}

- show

Serial Commands Description

Command	Description
Application connect	Enter the industrial application menu
serial	Access serial configuration hierarchy. Configuration for ports, local-end-point, and remote-end-point are available here.
Service show	Provides configuration state of a serial service
local-end-point filter show	Provides detailed configuration state of an iec101 serial tunneling service
card	**Auto-recover**: allows automatic recovery when identifying continuous loss of serial infrastructure keep alive (between the serial processor and the Ethernet processor). Enable: auto recovery will reboot the process. Disable: no action taken. Show : show state **Show** : display the version and the provision state of the serial processor
port slot 1 port <1-4>	Create/update the serial port
Clear counters	Clear counters
Create | update	Slot : 1 (constant) Port : port number .1-4 Baud rate : 50,75,100,110,134,150,200,300, 600,1200,2400,4800,9600,19200, 38400,57600,115200,230400, 460800,921600 Parity: no, odd, even. Default: no. Stopbits: 1, 2. Default: 1. **admin-status**: up| done. Default= up. **Mode of operation:** transparent , transparent9bit ,bitstream. default= transparent. **bus-idle-time** : number of total serial bits received over the local serial link to be considered as a single message **allowed-latency**: given in milliseconds this value describe the network allowed latency. This value affects the time to be allowed to delay before transmitting UDP packets. The higher the value is the more serial frames can accumulate into a single UDP packets. Default value is 10msec which corresponds to max 3 bytes of serial data to be packed at a single UDP packet (with 9.6kbps rate) **rts-cts**: enabling /disabling the RTS CTS control lines. Relevant in transparent tunneling only. default = disable **dtr-dsr** : enabling /disabling the DTR /DSR control lines. Relevant in transparent tunneling only. default = disable

Command	Description
Create | update	**local-cts-delay** : delay for sending the serial connected device a CTS status following the device RTS request. Setting the value 0 will result in not sending a CTS back. Permissible values are 0,5-255 msec. Relevant in transparent tunneling only. default=0. **local-dsr-delay** : delay for sending the serial connected device a DSR status following the device DTR request. Setting the value 0 will result in not sending a DSR back. permissible values are 0,5-255 msec. Relevant in transparent tunneling only. default=0. **tx-delay** : 0-255 msec. The IP packet will be delayed from egress to the network with this time. **bits-for-sync1** : relevant for bitstream mode only. number of consecutive '1' bits to represent end of serial frame before encapsulating it to IP packet. <0-255> **bits-for-sync2** : relevant for bitstream mode only. Number of consecutive '1' bits to wait before sending the serial data to the local connected serial end device. <0-255>
Remove	Slot : 1 (constant) Port : port number .1-4
Show	
Local-end-point	
Create	Slot : 1 (constant) Port: port number .1-4 Service id: numeric value of serial service. Position: N/A - point to point Master – point to multipoint Slave – point to multipoint Application : Serial-tunnel (default) Terminal-server iec101-gw modbus-gw buffer mode: byte (default) frame protocol : any (default) modbus_rtu iec101 iec101-link-address: set the IEC 101 link address. Applicable when 'application'=' iec101-gw' and 'protocol'=' iec101'. <0-65535> iec101-link-address-len: set the IEC 101 link address length. Applicable when 'application'=' iec101-gw' and 'protocol'=' iec101'. <1|2> bytes. Default is 2. iec101-originator-address: set if the 'originator' i=field is included in the IEC 101 message. This will reflect on the Cause Of Transmission being 1 byte or 2 byte size. If 'present', COT=2. If 'none', COT=1. unit-id: set the IEC 101 unit ASDU address. Applicable when 'application'=' iec101-gw' and 'protocol'=' iec101'. <0-65535> unit-id-len: set the IEC 101 ASDU length. Applicable when 'application'=' iec101-gw' and 'protocol'=' iec101'. <1|2> bytes. Default is 2.

Command	Description
Remove	Slot : 1 (constant) Port : port number .1-4 Service id: numeric value of serial service. Position: Master – point to multipoint Slave – point to multipoint Application : Serial-tunnel (default) Terminal-server iec101-gw modbus-gw
show	
tunnel settings	**update low-border-ip-port**: define here the range of port number used for tcp/udp connection. The set number will define the low border range value 'x' and result in a permissible range of x to x+100. The actual port number which will be used is dependent on the 'service-id' value as such: ['service-id'+ 'low-border-ip-port']. Default value is 9849 which results in port number 9850 for service-id=1. Changing the default 9849 is permitted to a value higher than 1024.
Remote-end-point	Defines the remote end points in a transparent serial tunneling service.
Create	remote-address : IPv4 address A.B.C.D Service id: numeric value of serial service. <1-100. Position: Master Slave connection mode: udp – default tcp Buffer mode: byte – default frame
Remove	address : IPv4 address A.B.C.D Service id: numeric value of serial service.
show	

Declaration of ports

Example of serial port declaration:

```
+ root
      Application connect
            serial
                  Port create slot 1 port 1
                  Port create slot 1 port 2
                  Port create slot 1 port 3
                  Port create slot 1 port 4
```

Default State

The default state of the serial ports is non-configured.

```
[/] serial port show
+-----+------+------+-----+------+------+------+--------+------+---------+-------+-------+-------+-------+-----+
| idx | slot | port | bus | mode | baud | data | parity | stop | latency |  tx   | start | stop  | admin | svc |
|     |      |      |     |      | rate | bits |        | bits |         | delay | delim | delim |       | id  |
+=====+======+======+=====+======+======+======+========+======+=========+=======+=======+=======+=======+=====+
+-----+------+------+-----+------+------+------+--------+------+---------+-------+-------+-------+-------+-----+

[/] serial local-end-point show
+-------+---------+------+------+-------------+----------+----------+----------+
| index | service | slot | port | application | position | firewall | firewall |
|       |   id    |      |      |             |          |   mode   | protocol |
+=======+=========+======+======+=============+==========+==========+==========+
+-------+---------+------+------+-------------+----------+----------+----------+
```

System default VLAN 4093

The system VLAN 4093 is used for internal purposes. The user should not make any changes to this VLAN.

Serial default VLAN 4092

The system VLAN 4092 is used by the application for serial services. This VLAN is configured by default and remains after “delete startup-cfg”. The following VLAN assignment must take place as is, and should not be tampered by the user.

```
interface gigabitethernet 0/3
no shut
exit
vlan 4092
ports add gigabitethernet 0/3
ports add fastethernet 0/10 untagged all
exit
interface fastethernet 0/10
switchport pvid 4092
no shut
exit
write startup-cfg
```

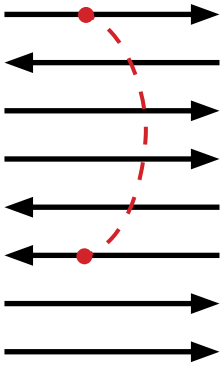
RS-232 Port Pin Assignment

Below is the pin assignment of the serial ports.

ComNet RJ-45 Female DTE		
line	**pin**	**direction**
DCD	2	in
TX	6	out
RX	5	in
DSR	1	in
GND	4	
DTR	3	out
CTS	7	in
RTS	8	in

When using the DTR/DST control lines the following cable assembly is required to ensure DCD and DSR are connected together.

Customer Port (DTE)		
line	**pin**	**direction**
DCD	1	in
RX	2	in
TX	3	out
DTR	4	out
GND	5	
DRS	6	in
RTS	7	out
CTS	8	in
R	9	in



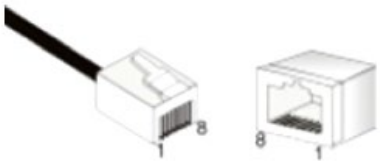
ComNet RJ-45 Female DTE		
line	**pin**	**direction**
DCD	2	in
TX	6	out
RX	5	in
DSR	1	in
GND	4	
DTR	3	out
CTS	7	in
RTS	8	in

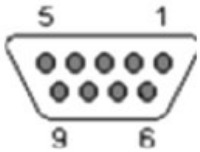
RS-232 Serial cable

The RS-232 ports are of RJ-45 type, a cable is available as ordering option having one end of male RJ-45 and second end of female DB-9.

The cable should be used when no control lines are needed.

Serial port at the switch *DB-9 female connector for end device*





Pin out for crossed cable:

Customer Port (DTE)				Cable, DB-9 Female (DCE)				ComNet RJ-45 Female DTE		
line	**pin**	**direction**		**line**	**pin**	**direction**		**line**	**pin**	**direction**
								DCD	2	in
RX	2	in	←	RX	2	out	←	TX	6	out
TX	3	out	→	TX	3	in	→	RX	5	in
								DSR	1	in
GND	5		—	GND	5		—	GND	4	
								DTR	3	out
								CTS	7	in
								RTS	8	in

CAUTION: Take notice not to use the console cable for the user serial ports.

The console cable is uniquely colored white.

LED Indicators

Each serial port has a led to indicate its state.

Port created	Port admin state	Traffic passing	LED
No (default)	N/A	N/A	OFF
yes	down	N/A	OFF
yes	Up (default)	No	Green
yes	Up (default)	yes	Green blinking

ACE QOS

SCADA services are still commonly using serial legacy hardware. For such applications, the RLGE2FE16R supports services as protocol gateway, serial tunneling and terminal server. These low bandwidth application may be of high importance to the utility process and require high network availability.

The QOS allows setting priority for serial services.

ACE QOS Commands Hierarchy

+ application connect

+ qos

- mark-rule create {[src-ip <A.B.C.D/E>]| [dest-ip <A.B.C.D/E>]}
  [protocol {tcp| udp}] [src-port <1-65535>] [dest-port <1-65535>]]
  {dscp <dec,(0-63)>}

- mark-rule remove {src-ip <A.B.C.D/E>} [dest-ip <A.B.C.D/E>}

- mark-rule show

- show

ACE QOS Commands Descriptions

Command	Description
application connect	
qos	This command enters the quality of service configuration mode.
mark-rule	Create| update| show src-ip: IPv4 source IP of the packet. Should be one of the 1031 IP interfaces. **A.B.C.D/E** dest-ip: IPv4 destination IP of the packet. Protocol: tcp|udp protocol used at the packet. src-port: protocol source port used at the packet. dest-port: protocol source port used at the packet.

Example QOS for Serial Tunneling

Below network demonstrates a P2P topology of transparent serial tunneling. QOS will be set for the service to preserve dscp value of 10 over the network.

Configuration both switches

1. Create a vlan for the service and tag the network port. port gigabitethernet 0/3 must as well be a member.

```
Config
vlan 2
ports gigabitethernet 0/2
ports add gigabitethernet 0/3
end
write startup-cfg
```

Configuration switch A (local)

1. Configure ACE IP interface

```
application connect
router interface create address-prefix 192.168.2.201/24 vlan 2 purpose application-host
```

2. configure the QOS to assign dscp 10 for traffic between the ACE interfaces used for the serial tunneling

```
qos mark-rule create src-ip 192.168.1.201/24 dest-ip 192.168.1.202/24 dscp 10
```

3. configure the serial port and service (values are example only)

```
serial port create slot 1 port 1 baudrate 9600 parity even mode-of-operation transparent
serial local-end-point create slot 1 port 1 service-id 1 application serial-tunnel
position local
serial remote-end-point create remote-address 192.168.2.202 service-id 1 position remote
exit
write startup-cfg
[/] qos mark-rule show
+------------------+------------------+-------+------+------+------+
|        dest      |        src       | proto | dest | src  | dscp |
|         ip       |         ip       |       | port | port |      |
+==================+==================+=======+======+======+======+
| 192.168.1.201/24  | 192.168.1.202/24  |  any  | any  | any  |  10  |
+------------------+------------------+-------+------+------+------+
```

Configuration Switch B (Slave)

1. Configure ACE IP interface

```
application connect
router interface create address-prefix 192.168.2.202/24 vlan 2 purpose application-host
```

2. configure the QOS to assign dscp 10 for traffic between the ACE interfaces used for the serial tunneling

```
qos mark-rule create src-ip 192.168.1.202/24 dest-ip 192.168.1.201/24 dscp 10
```

3. configure the serial port and service (values are example only)

```
serial port create slot 1 port 1 baudrate 9600 parity even mode-of-operation transparent
serial local-end-point create slot 1 port 1 service-id 1 application serial-tunnel
position remote

serial remote-end-point create remote-address 192.168.2.201 service-id 1 position local
exit
write startup-cfg

[/] qos mark-rule show
+------------------+------------------+-------+------+------+------+
|        dest      |        src       | proto | dest | src  | dscp |
|         ip       |         ip       |       | port | port |      |
+==================+==================+=======+======+======+======+
| 192.168.1.202/24  | 192.168.1.201/24  |  any  | any  | any  |  11  |
+------------------+------------------+-------+------+------+------+
```

Transparent Serial Tunneling

In transparent tunneling mode the switch encapsulates the serial frames into UDP packets. The UDP packet is sourced with a local IP interface configured in the application layer of the RLGE2FE16R switch. Topologies supported are P2P, P2MP and MP2MP over a single switches or IP network.

Control line signals are as well supported in this mode.

The condition for transparent serial tunneling is having a ComNet switch at both ends of the network, connecting the devices.

The transparent tunneling has three types of implementations:

1. Transparent tunneling: encapsulation of standard serial frames is supported. The serial frames are structured with start, stop, data, and parity bits.
2. Transparent 9bit: in this special mode the parity bit is regarded as an additional data bit.
3. Bitstream: this is an oversampling mode in which no start, stop bits are available for the frames. The number of data bits is usually higher the “standard” 5-8 data bits.

Following chapter will explain key serial properties and modes of operation.

Concept of Operation

The benefit of transparent serial tunneling is its simplicity.

Serial traffic received from the customer serial device at the switch serial port, is encapsulated as UDP or TCP Ethernet packets by the switch.

An ACE IP interface is configured to route the packets over the Ethernet network. The Ethernet cloud may be layer 2 based, or layer 3 routing based and may involve any type of networking including cellular connectivity and VPN between the switches.

The serial devices must all be connected to ComNet switches.

The switch serial port is configurable with a full set of serial properties.

Each serial port is assigned to a service-id. The service-id groups serial devices in the network to a logic communication segment at which members can communicate with each other.

At each service-id group there must be at least one device which is set a local and at least one device set as a remote.

The communication rules, which are maintained between service-id group members, are as follows:

1. Traffic sent from a local will be received at all remotes.
2. Traffic sent from a remote will be received at all locals.
3. Traffic between locals is blocked
4. Traffic between remotes is blocked.

Supported Network topologies

Transparent serial tunneling supports following topologies:

» Point-to-point
» Point to multipoint point
» Multi Point to multipoint point

Point to Point

Below picture illustrates Point-to-point service at which the local and remote are connected locally at the same switch.

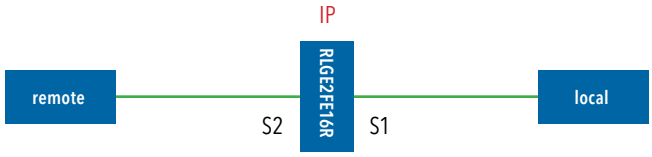


Figure 2: P2P, local service

Below picture illustrates Point-to-point service at which the local and remote are behind different switches.

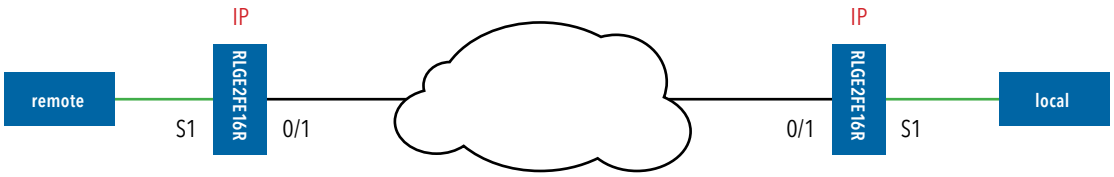


Figure 3: P2P, remote service

Point to multipoint point

Below picture illustrates Point-to-multipoint service at which the local and remotes are connected locally at the same switch.

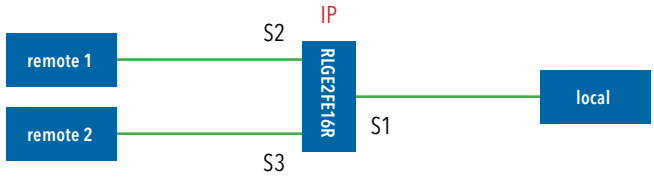


Figure 4: P2MP, local service

Below picture illustrates Point-to-multipoint service at which the service members are spread.

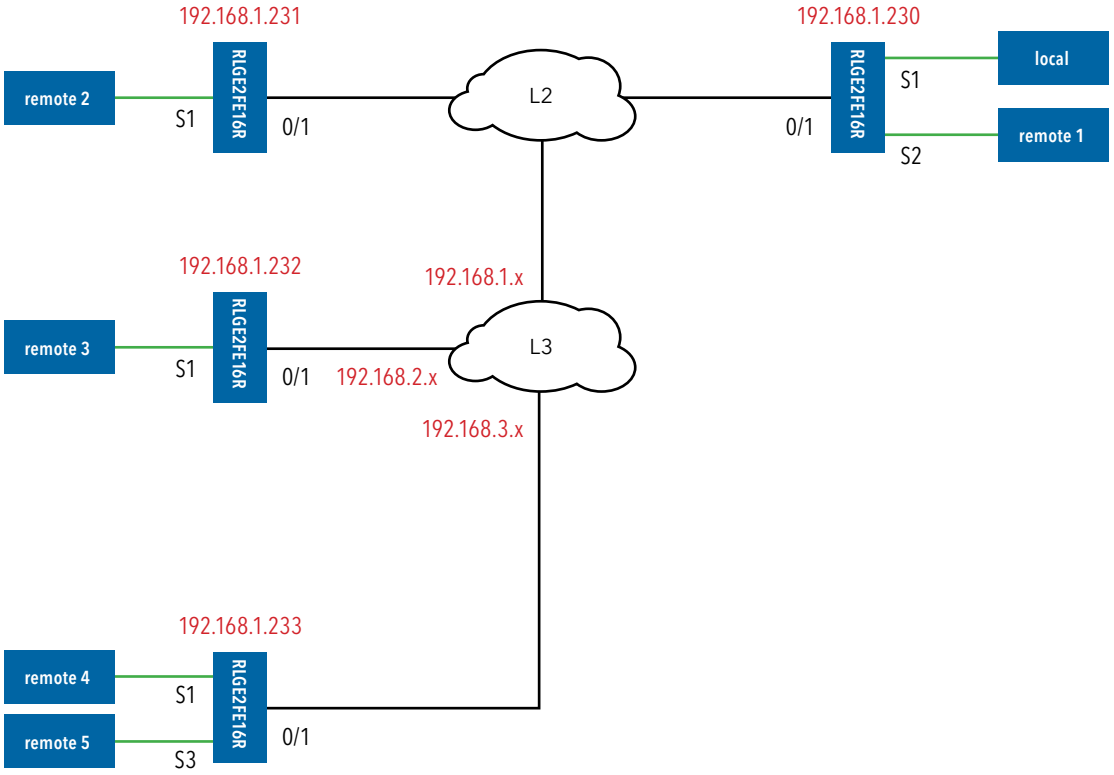


Figure 5: P2MP, remote service

Multi Point to multipoint point

Below picture illustrates a typical multipoint-to-multipoint service.

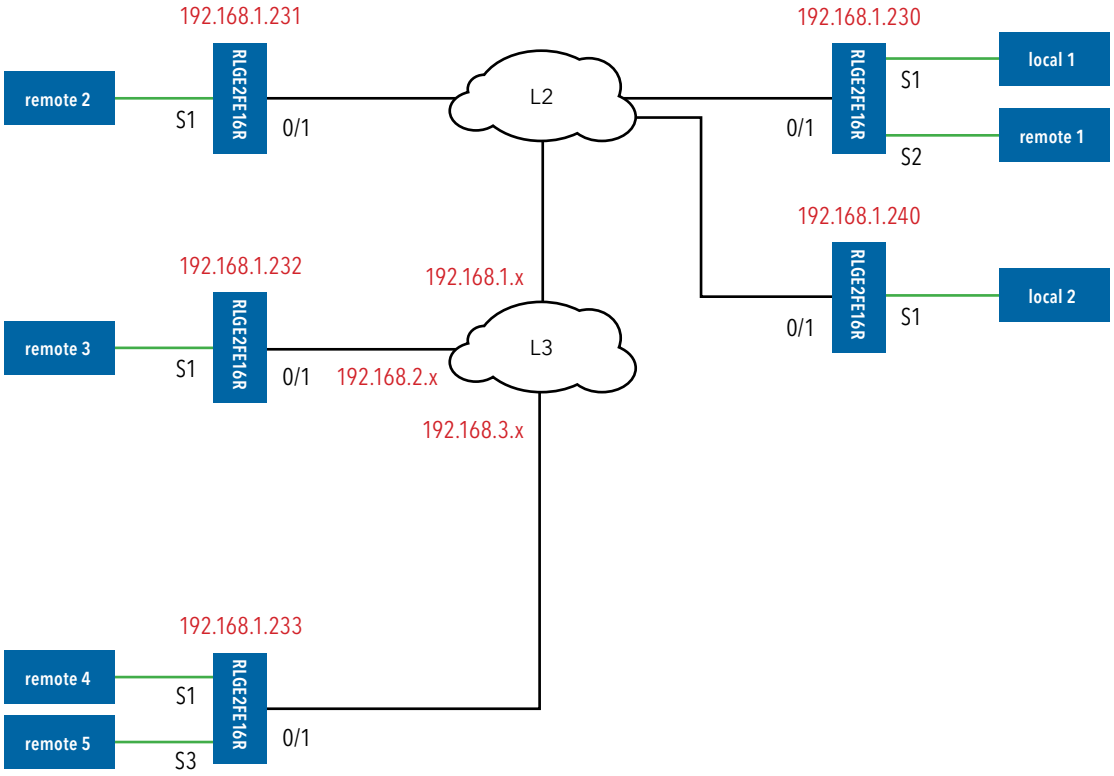


Figure 6: MP2MP, mixed service

Modes of Operation

Port Mode Of Operation

The port mode-of-operation is set at the serial port configuration level and defines how serial data is collected.

Transparent Tunneling

Transparent-tunneling is a mode at which serial data is sent with a distinct start bit, stop bit and a known length of data bits.

At this mode, the serial processor will collect data received until one of the following conditions is met:

» Bus idle time has expired.

» Allowed latency has expired.

At such time, the serial data collected will be encapsulated to a UDP packet and transmitted.

Bitstream

Bitstream is a mode at which serial data is sent without a distinct start bit, stop bit or a known length of data bits.

At this mode, the serial processor will collect data received until one of the following conditions is met:

» A silence on the line has been detected. Number of consecutive '1' bits received exceeds the 'bits-for-sync2' configured value.

» Allowed latency has expired.

At such time, the serial data collected will be encapsulated to a UDP|TCP packet and transmitted.

Service Buffer Mode

The service buffer-mode is set at local-end-point configuration level and defines the buffer operational mode for the service-id.

The default state is 'byte' mode. If the user keeps this field with its default state but configures the service 'connection-mode' to 'tcp', the buffer mode will be changed to 'frame' automatically. If the user explicitly set the buffer mode to either 'byte' or 'frame', the configuration will take effect for any connection-mode setting (tcp|udp).

Byte mode

A byte is structured as [start-bit, data-bits, parity-bit, stop-bits] whereas the number of data-bits may be 5 to 8.

At this mode, the serial-processor collects bytes and encapsulates the data at a UDP/TCP Ethernet frame.

The number of bytes collected to a single Ethernet packet is determined by the following factors:

» Allowed latency.

» Bus idle time.

Frame mode

A frame is a group of bytes sent by the customer equipment (CE) as complete message.

When using frame mode, the serial-processor will use the bus-idle-time to distinguish between frames. Each frame will be encapsulated as an individual UDP packet.

Service Connection Mode

The service connection-mode is set at remote-end-point configuration level and defines the protocol option to be used for the service-id.

UDP

1. Serial data will be encapsulated as UDP/IP frames. This is the default option for a serial service.
2. UDP connection mode will use by default, byte mode for the service 'buffer-mode'. That is unless 'buffer-mode' was explicitly set to 'frame' by the user.

TCP

1. Serial data will be encapsulated as TCP/IP frames.
2. This mode allows higher availability for the end to end connection and traffic validation.
3. TCP connection mode will use by default, frame mode for the service 'buffer-mode'. That is unless 'buffer-mode' was explicitly set to 'byte' by the user.
4. At TCP mode, the RLGE2FE16R router at which the serial configuration determines the serial port to be the 'local' at the service, will act as the tcp client and will initiate the tcp session towards the remote RLGE2FE16R routers holding the serial 'remotes' at the serial tunneling service.

Service Port number

The TCP/UDP port number used at a serial tunneling connection is defined by the values of 'service-id' and the 'low-border-ip-port' set at the 'serial' 'settings'.

Addressing Aware Modes

The service of 'transparent serial tunneling' aims to keep the end to end serial service simple and with no tempering of higher layer protocols.

Non aware mode

Serial data will be set to be received in either byte or frame mode with no awareness of the data content or protocol addressing. At this mode the following behavior is achieved within a service group:

» Traffic sent from a local device will received by all remotes.

» Traffic sent from a remote, will be received by all locals.

Aware mode

Serial data will be set to be received in frame mode. Each serial device connected to the switch is identified with its protocol unit-id. For IEC 101 as an example, the serial device Common Address of ASDU will be configured at the switch serial port. At this mode the following behavior is achieved within a service group:

» Broadcast traffic sent from a local device will received by all remotes.

» Traffic sent from a local and addressed to a specific unit-id, will be received by the target device only.

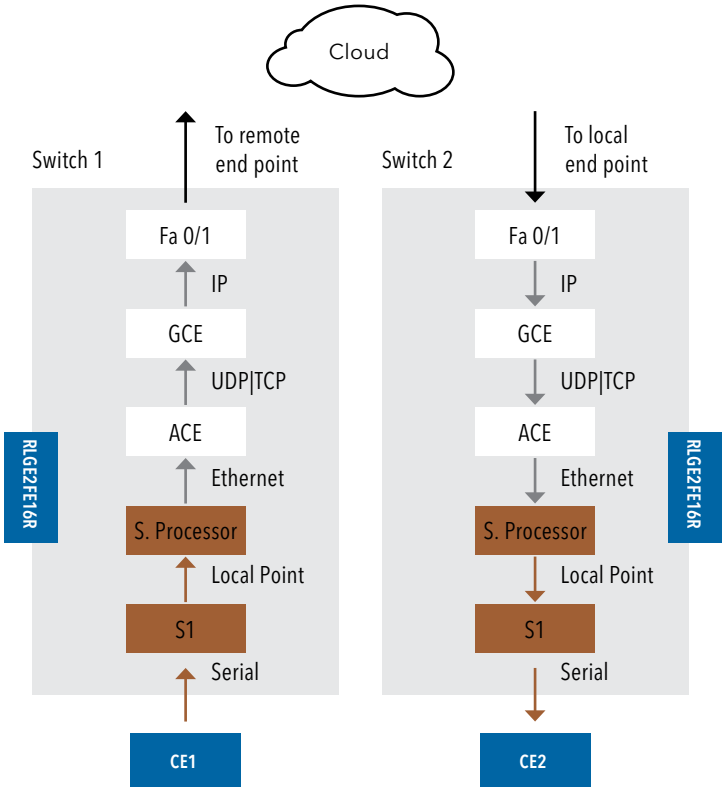
» Traffic sent from a remote, will be received by all locals.

NOTE: The aware mode supports IEC 101 addressing only.
The service 'local-end-point' must be set with ['application'= 'iec101-gw'] and ['protocol'=' iec101']

Reference drawing

For ease of explanation of following terms and serial properties at this chapter, below diagram will be used as a reference to follow on the serial traffic flow.

The diagram demonstrates two RLGE2FE16R switches, connected over an Ethernet network and sharing a transparent serial tunneling service.



The customer equipment #1 (CE1) is a serial local sending data to a serial remote CE2. For simplicity purposes, the diagram and explanations refer to unidirectional traffic from CE1 to CE2.

Serial Traffic Direction

Transmit direction represents the serial-processor traffic towards the CE, over the serial port.

Receive direction represents the traffic received at the serial-processor from the CE, over the serial port.

Serial ports counters

The Tx and Rx counters of the serial ports are controlled by the serial-processor.

Rx counters

» Switch1 – counters will increase when CE1 transmits. Data is received at the serial-processor via S1 and updates the counters.

» Switch2 – counters are not updated.

Tx counters

» Switch1 – counters are not updated.

» Switch2 –CE1 Data is received over the Ethernet network to switch 2 and to the serial-processor. The serial processor transmits the data to CE2 over S1 and increases the Tx counters.

Allowed latency

Allowed latency is the maximum time allowed for the serial-processor to collect serial data from CE1 transmission, before closing an Ethernet packet and sending it over the cloud.

This parameter refers to round-trip in milliseconds units. It reflects only the time for the serial processor to collect data, it does not consider the network self-latency.

Allowed latency is applicable in byte mode only.

» Switch1 – as CE1 transmits data to serial processor over S1, the allowed-latency properties are applicable. For a configured value x at allowed-latency, the serial processor will collect serial data for up to x/2 milliseconds time and then close the collected data as an Ethernet packet.

» Switch2- as CE2 is only receiving, the allowed-latency is not of influence.

Tx Delay

Tx-delay is set in bits. It determines a delay to take place by the serial processor before transmitting serial data to the port. Depending on the baudrate chosen, and the number of bits, a time is calculated for Tx-delay.

» Switch1 – as the serial processor only receives serial data, the tx-delay is of no affect.

» Switch2- the Ethernet encapsulated data is received at switch 2 and to its serial-processor. It is then transmitted to CE2 via S1 following a time elapse of the tx-delay. The serial-processor will delay transmitting the first serial byte to CE2. Following data bytes are sent without delay.

Bus Idle Time

This parameter determines a silence on the serial line to identify frame end. The configurable value for it is given in number of bits. Depending on the baud rate chosen, and the number of bits, a time is calculated for bus-idle-time.

Byte mode

When using byte mode, end of byte is determined by stop bits. Bus-idle-time is not applicable at this mode.

Frame mode

- Switch1- the serial-processor will collect serial data transmitted from CE1 until a silence is identified on the line for a time period equal or above the bus-idle-time.
- Switch2- the serial-processor transmits the serial frames to CE2 while maintaining a gap between frames. The gap is the bus-idle-time.

Bits for Sync

The parameters 'bits-for-sync1' and 'bits-for-sync2' are applicable for bitsream mode only.

bits-for-sync1

Similar in purpose to Tx-delay. When transmitting, the serial processor will add number of consecutive '1' bits before the data. The number of consecutive '1' bits is determined by 'bits-for-sync1'.

bits-for-sync2

Similar in purpose to 'bus-idle-time'. When receiving, the serial-processor looks for a silence on the line in order to identify end of message and encapsulate to a UDP packet. The silence on the line is identified as a number of consecutive '1' bits received. The number of consecutive '1' bits is determined by 'bits-for-sync2'.

RS-232 Control lines

The RLGE2FE16R support the use of the RS-232 control lines for the transparent serial tunneling service.

By default, the control lines are disabled, making the active lines at the ports Tx and Rx only.

The control lines are applicable for point-to-point serial services only.

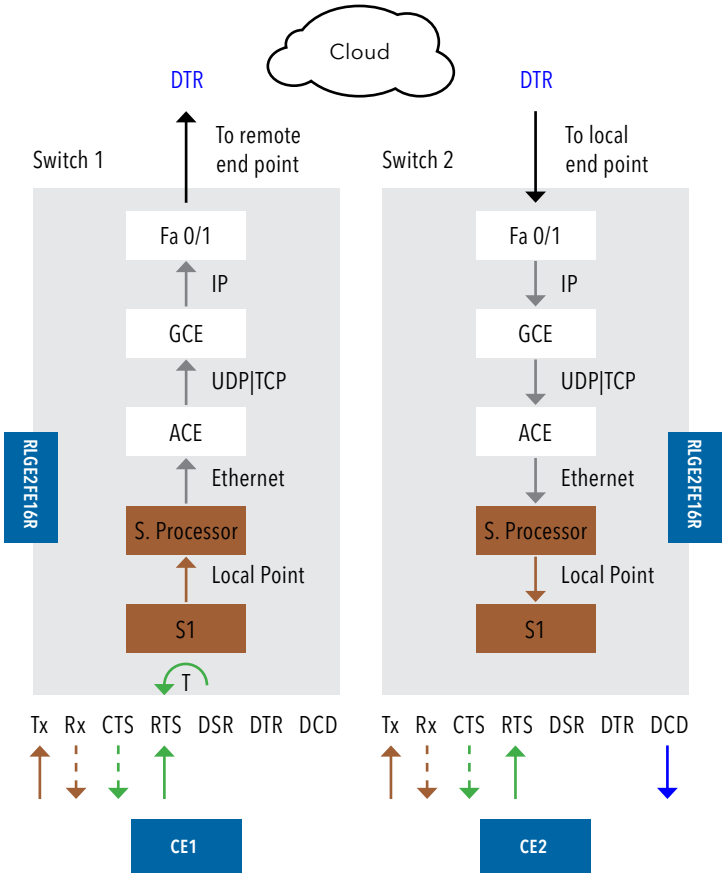
The control lines are:

» RTS (Request To Send)
» CTS (Clear to Send)
» DCD (Data Carrier Detect). Applicable only when DTR/DSR lines are disabled.
» DTR (Data Terminal Ready). Applicable only when RTS/CTS lines are disabled.
» DSR (Data Set Ready). Applicable only when RTS/CTS lines are disabled.

Modes of operation

Point-to-point, remote service, CTS/RTS

The below diagram illustrates a Point-to-point, remote service. RTS/CTS lines are enabled.

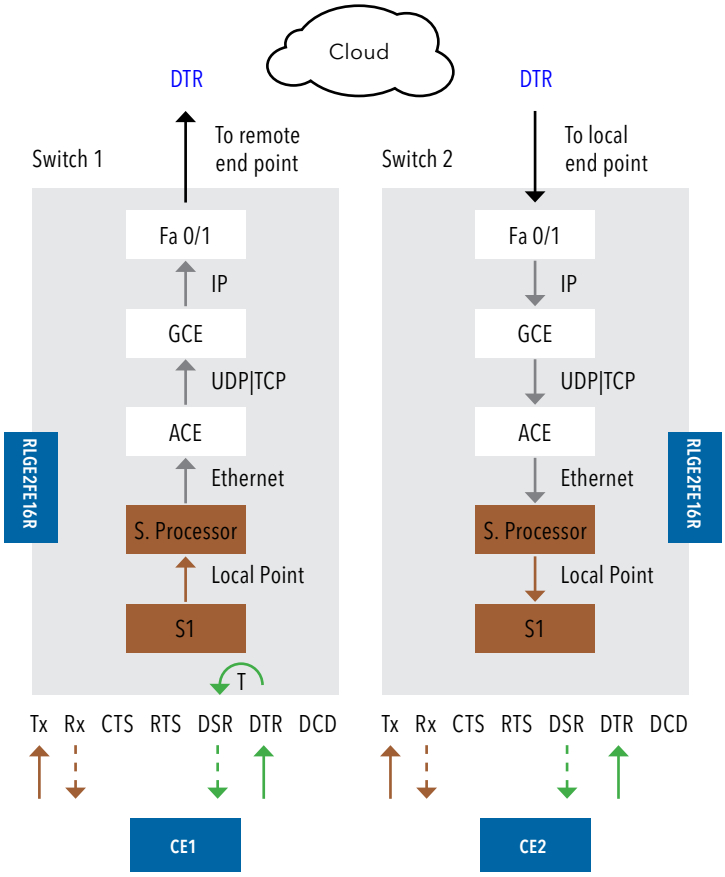


When CE1 sends RTS, following flow will take place:

1. The switch#1 serial-processor will reply with CTS back to CE1. The reply may be with or without a configurable time delay.
2. Simultaneously, the serial-processor of switch#1 will send DTR=1 to switch#2.
3. At switch#2, CE2 will receive the DCD.
4. CE1 data will be sent and received at CE2.

Point-to-point, remote service, DTR/DSR

The below diagram illustrates a Point-to-point, remote service. DTR/DSR lines are enabled.

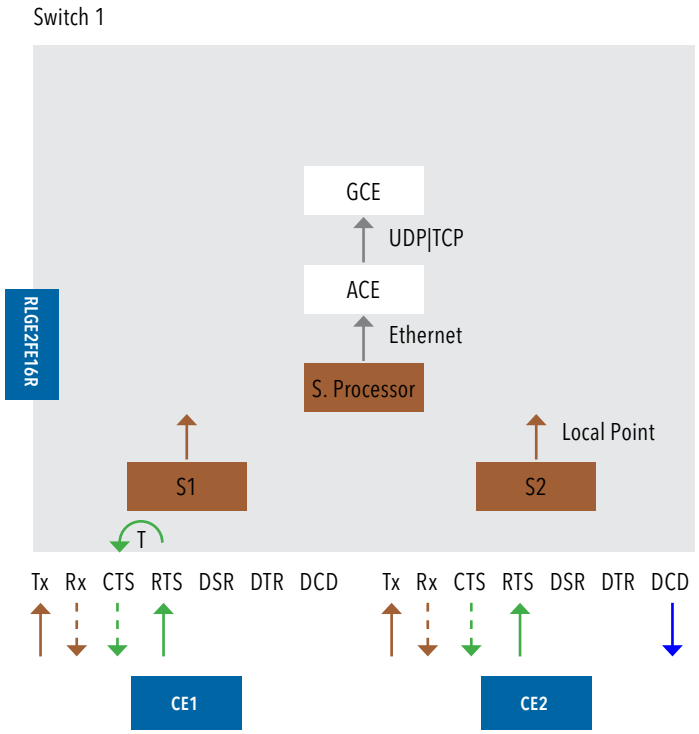


When CE1 sends DTR, following flow will take place:

1. The switch#1 serial-processor will reply with DSR back to CE1. The reply may be with or without a configurable time delay.
2. CE1 data will be sent and received at CE2.

Point-to-point, local service, CTS/RTS

The below diagram illustrates a Point-to-point, local service. RTS/CTS lines are enabled.



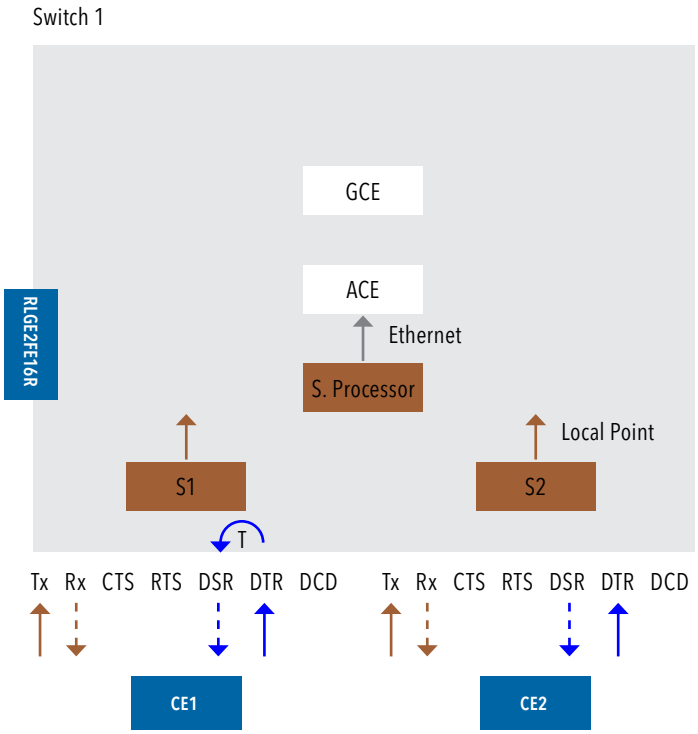
When CE1 sends RTS, the serial-processor will reply with CTS back to CE1. The reply may be with or without a configurable time delay.

Simultaneously, DCD will be received at CE2.

CE1 data will be sent and received at CE2.

Point-to-point, local service, DTR/DSR

The below diagram illustrates a Point-to-point, local service. DTR/DSR lines are enabled.

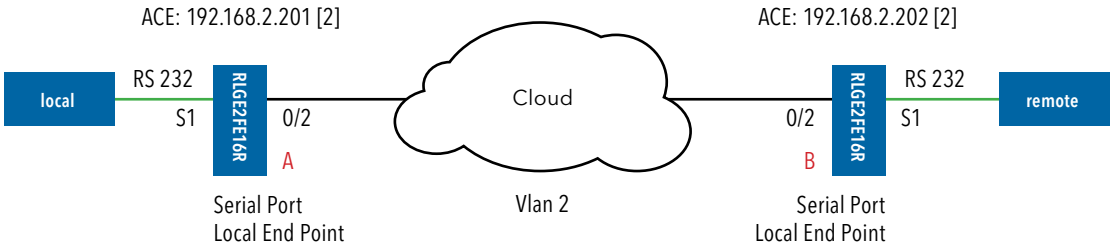


When CE1 sends DTR, the serial-processor will reply with DSR back to CE1. The reply may be with or without a configurable time delay.

CE1 data will be sent and received at CE2.

Example: Serial Tunneling

Below network demonstrates a P2P topology of transparent serial tunneling.



Configuration both switches

Create a vlan for the service and tag the network port

port gigabitethernet 0/3 must as well be a member.

```
Config
vlan 2
ports gigabitethernet 0/2
ports add gigabitethernet 0/3
end
write startup-cfg
```

Configuration switch A (local)

Configure the serial port and service (values are example only)

```
application connect
router interface create address-prefix 192.168.2.201/24 vlan 2
serial port create slot 1 port 1 baudrate 9600 parity even mode-of-operation transparent
serial local-end-point create slot 1 port 1 service-id 1 application serial-tunnel
position local
serial remote-end-point create remote-address 192.168.2.202 service-id 1 position remote
exit
write startup-cfg
```

Configuration switch B (Slave)

1. configure the serial port and service (values are example only)

```
application connect
router interface create address-prefix 192.168.2.202/24 vlan 2
serial port create slot 1 port 1 baudrate 9600 parity even mode-of-operation transparent
serial local-end-point create slot 1 port 1 service-id 1 application serial-tunnel
position remote
serial remote-end-point create remote-address 192.168.2.201 service-id 1 position local
exit
write startup-cfg
```

Terminal Server

Terminal Server service

ComNet routers allow a special service for transposing of a TCP session to serial session.

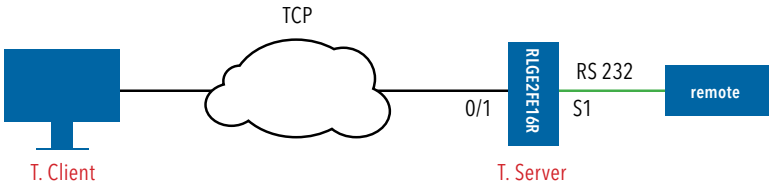
Networking:

A router acting as the terminal server can be connected to the Ethernet telnet client via:

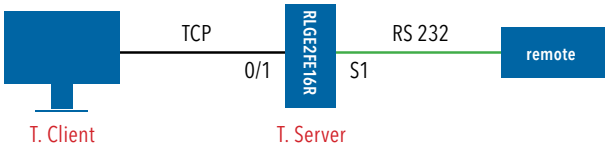
» local connection at its ports or

» Via IP network.

» In both cases the connection is TCP based.



Telnet Client connected over network.
Serial Remote connected locally.



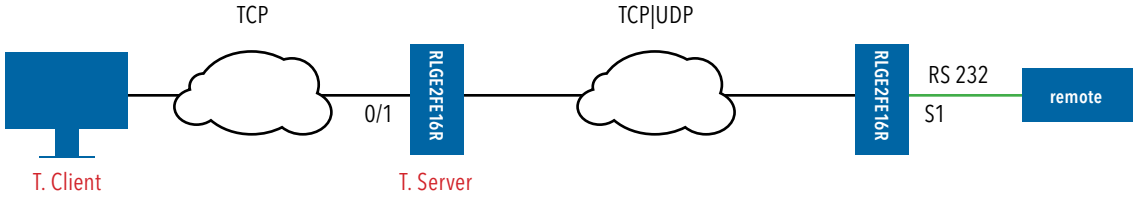
Telnet Client connected locally.
Serial Remote connected locally.

A router acting as the terminal server can be connected to the serial end device via:

» local connection at its RS-232 ports. This scenario is referred to 'local service' of the terminal server.

» Or Over UDP or TCP connection to a remote ComNet router at which the serial device is connected directly to. This scenario is referred to 'remote service' of the terminal server.

› At this case there will be a "transparent serial tunneling service" between the two routers over the IP network (encapsulation of serial data in UDP packets)



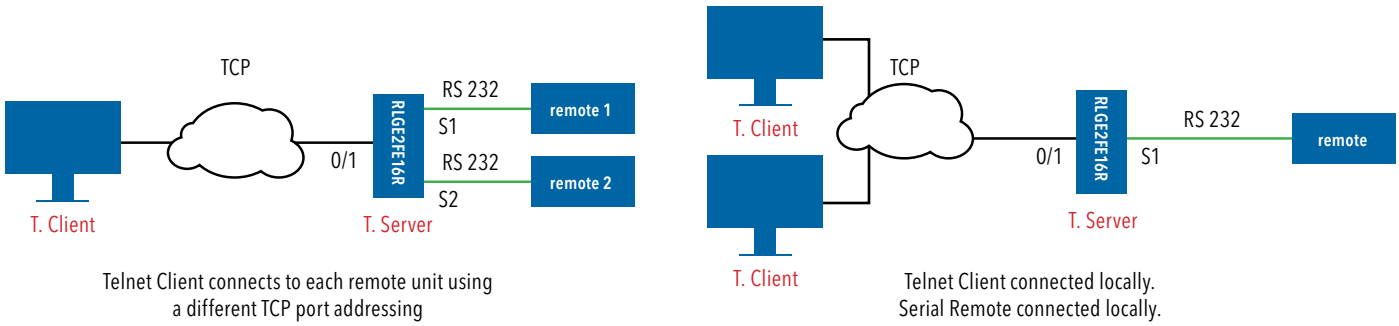
Telnet Client connected over network.
Serial Remote connected at remote server.

A usage example, console ports of remote devices to be reached via terminal server service using telnet from any PC with Ethernet link.

Topologies of MP2MP are supported.

» Over the same service using the same TCP port number.

» Over different services using multiple TCP sessions each with a different TCP port.



NOTE: The terminal server service requires the use of an ACE IP interface type 'application-host'

Service Buffer Mode

The service buffer-mode is set at the terminal server settings and defines the buffer operational mode for all the services.

Byte mode

A byte is structured as [start-bit, data-bits, parity-bit, stop-bits] whereas the number of data-bits may be 5 to 8.

At this mode, the serial-processor collects bytes and encapsulates the data at a UDP/TCP Ethernet frame.

The number of bytes collected to a single Ethernet packet is determined by the following factors:

» Allowed latency.

» Bus idle time.

Frame mode

A frame is a group of bytes sent by the customer equipment (CE) as complete message.

When using frame mode, the serial-processor will use the bus-idle-time to distinguish between frames. Each frame will be encapsulated as an individual UDP/TCP packet.

Service Operation Mode

The terminal server may act in one of two roles,

1. telnet server- expecting incoming TCP/UDP connections initiated from a customer telnet client. This is considered the more common operation mode.

2. telnet client- the router itself is a client and will initiate a telnet TCP session to a customer listening server.

Service Connection Mode

The service connection-mode is set at the terminal server settings and defines the protocol option to be used for all services.

UDP

Serial data will be encapsulated as UDP/IP frames. Since UDP is connectionless it is required by the user to configure the IP address of the UDP client as the destination. This is done at the 'terminal-serer' 'udp-service' cli hierarchy.

TCP

Serial data will be encapsulated as TCP/IP frames. This mode allows higher availability for the end to end connection and traffic validation.

TCP connection will be established between the RLGE2FE16R router acting as a terminal server and the tcp client. The tcp client must initiate the connection so at this case there is no need to configure in advance the ip address of the client (unlike at UDP).

Service Port number

The TCP/UDP port number used at a terminal server service is defined explicitly at the user configuration per 'service-id'. The port selected must be a member of the port range defined at the 'terminal-server' 'settings'.

Terminal Server Commands Hierarchy

+ application connect

  + router

    - interface create address-prefix <IP address>/[netmask] vlan <vlan id> purpose application-host [description <>]

    + serial

    + port

    - clear counters

    - create {slot <1>} {port <1-4>}
      [baudrate <9600,(50-368400)>] databits {8,<5-8>}
      [parity {no,no| odd| even}] [stopbits <1,1|2>]
      [bus-idle-time <bits (30-1000>]
      [mode-of-operation <transparent>]

    - remove slot <1> port <1-4>

    - show [slot <1> port <1-4>]

    + local-end-point

    - create slot <1> port <1-4> service-id <1-100> position <remote> application <terminal-server>

    - remove slot <1> port <1-4> service-id <id>

    - show

    + terminal-server

    - admin-status [enable | disable | show]

    - services show [service-id <>]

    + connections

    - dissconnect service-id <>

    - show service-id <>

    + counters [clear | show]

    + settings

    - restore

- update [low-border-telnet-tcp-port (2001,<2001-65434>]
  [low-border-telnet-udp-port (2001,<2001-65434>]
  [low-border-serial-tunnel-port (9850,<1025- 65434>]
  [dead-peer-timeout <min,10 (0-1440)>]
  [buffer-mode (frame,<frame |byte>)]

- show

+ tcp-service

- create {remote-address <A.B.C.D>} {service-id <1-100>} {telnet-port <port num>} [null-cr-mode (off,<off|on>)]
  [max-tcp-clients (1,<1-8>)]

- remove service-id <1-100>

- show

+ udp-service

- create {remote-address <A.B.C.D>} {service-id <1-100>}
  {udp-server-port <port number>}
  {udp-client-address <A.B.C.D>} [null-cr-mode (off,<off|on>)]

- remove service-id <1-100>

- show

+ client-service

- create {service-id <1-100>}
  {server-ip <A.B.C.D>} {server-port <port number>}
  {keepalive-period (30,<10-86400>)}
  [remote-address <A.B.C.D>]
  [null-cr-mode (off,<off|on>)]
  [bind-ip <A.B.C.D>]

- remove service-id <1-100>

- show

+ serial-tunnel

- create remote-address <A.B.C.D> service-id <1-100>

- remove service-id <1-100>

- show

Terminal Server Commands

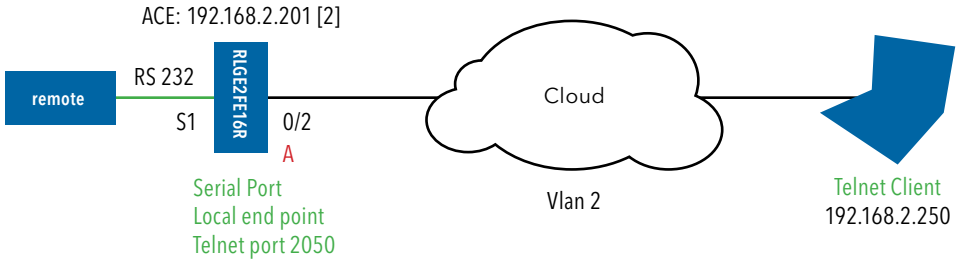
Command	Description
Application connect	Enter the industrial application menu
Serial port	Create/update the serial port
Clear counters	Clear counters
Create	Slot : 1 (constant) Port : port number .1-4 Baud rate : 50,75,100,110,134,150,200,300,600,1200,2400,4800,9600,19200,38400,57600,115200,230400,460800,921600. Parity : no, odd, even Stopbits : 1,2 Mode of operation : transparent
Remove	Slot : 1 (constant) Port : port number .1-4
Show	
Local-end-point	
Create	Slot : 1 (constant) Port : port number .1-4 Service id: numeric value of serial service. Application : Terminal-server
Remove	Slot : 1 (constant) Port : port number .1-4 Service id: numeric value of serial service.
show	
terminal-server	Enter terminal server configuration
Admin-status	Enable / disable terminal server
Connections [disconnect | show]	Manage the TCP connections to the terminal server **service-id** : serial service-id number assigned to the terminal server
counters	Display counters

Command	Description
settings	Manage the range of TCP ports used for the terminal server to respond to. By default the allowed range is 2001-2100. **Restore**: restore to the default range. **Update low-border-telnet-tcp-port <>**: a numeric value for the tcp port range low border. The value must be >=2001. The allowed range will be the entered value (x) to x+100. The serial encapsulation will be in TCP packets. **Update low-border-telnet-udp-port <>**: a numeric value for the udp port range low border. The value must be >=2001. The allowed range will be the entered value (x) to x+100. The serial encapsulation will be in UDP packets. **low-border-serial-tunnel-port <>**: this option is used when the serial device is not connected locally to serial ports of the terminal server router, but rather to a remote router via serial tunneling. A numeric value for the udp/tcp port range low border. The allowed range will be the entered value (x) to x+100. default is 9849. changing the default can be to a range starting from 1025. The serial encapsulation will be in UDP or TCP packets depending on the serial-tunneling 'remote-end-point' configuration. **Update dead-peer-timeout <0-1440>**: this parameter will release the open TCP socket after the configurable time so a new connection could be established. Set in units of minutes, default value is 10. Setting the value 0 will disable the timeout and keep the session open until administratively release or ended by the client. Updating the counter requires removing the services configured in advance. **Update buffer-mode**: default –frame. frame – the terminal server will hold from egress the TCP packet until receiving validation from the serial local end that a message is completed. This mode avoids fragmentation of serial messages to different TCP packets. byte – serial originated packets will be egressed without additional buffering at the terminal server. **Show** : display the current TCP port range
Serial-tunnel	Configuration options to be used at the switch where the serial port is connected at. These fields will determine the remote side to where to draw the serial service to (the remote side is the switch at which the terminal server is established). If the terminal server is configured on a local switch which as well accommodates the serial port then this configuration of "serial-tunnel" should not be used!. **Remote-address**: the IP address of the terminal server .this would be the address of the application interface at the remote switch acting as the terminal server. **Service-id**: the local serial service-id to be mapped to the terminal server. show: display the configuration.
tcp-service	Configuration options to be used at the router where the terminal server is set. This option relates to a TCP service settings. **Remote-address**: the router own ACE 'application-host' interface IP address. **Service-id**: the serial service-id to which the terminal server service relates to. the 'service-id' is created at the 'serial' 'local-end-point' and must be set to 'application'= 'terminal-server'. **telnet-port**: the TCP port to be used for the connection. Incoming TCP traffic with this port will be directed to the terminal server. Serial traffic will encapsulated to UDP and send to the UDP client with this port. **mmax-tcp-clients**: define how many TCP clients can open a connection at the specified service. **null-cr-mode**: this field settings (on|off) allows flexibility in working with different types of terminals (as PuTTY, hyper terminal, CRT..)as each handles the CR bit differently. When set to On the switch will drop <NULL> character only if it arrives immediately after the <CR> (^M, 0x0d). For all other modes of operation, NULL_CR is ignored. default - off **show** : display the configuration.

Command	Description
udp-service	Configuration options to be used at the router where the terminal server is set. This option relates to a UDP service settings. **Remote-address**: the router own ACE 'application-host' interface IP address. **Service-id**: the serial service-id to which the terminal server service relates to. the 'service-id' is created at the 'serial' 'local-end-point' and must be set to 'application'= 'terminal-server'. **Udp-server-port**: the UDP port to be used for the connection. Incoming UDP traffic with this port will be directed to the terminal server. Serial traffic will encapsulated to UDP and send to the UDP client with this port. **Udp-client-address**: an IPv4 address of the target UDP client to which the terminal server will reply to. **null-cr-mode**: this field settings (on|off) allows flexibility in working with different types of terminals (as PuTTY, hyper terminal, CRT..)as each handles the CR bit differently. When set to On the switch will drop <NULL> character only if it arrives immediately after the <CR> (^M, 0x0d). For all other modes of operation, NULL_CR is ignored. default - off **show** : display the configuration.
remove	**Address**: IP address in the form of aa.bb.cc.dd. The IP is of the Application interface at the switch at which the serial port is connected at. **Telnet-port**: TCP port number used for the service. **Service-id**: serial service id number which the designated serial port is configured as a member in ("local end point). **Slot** : 1 (constant) **Port** : port number .1-4
show	Show port mapping
Client-service	Set a client service at which the router initiates a telnet TCP connection towards the customer telnet server.
create	**Service-id**: serial service id number which the designated serial port is configured as a member in ("local end point). **server-ip**: The customer telnet server ipv4 address. **server-port**: the TCP port number in the range configured at the terminal server settings. The customer telnet server is expected to listen to incoming connections from the router with this port. **Remote-address**: optional field. The router own ACE 'application-host' interface IP address. keepalive-period: the time in seconds to keep the TCP session towards the customer telnet server when no traffic is sent. **null-cr-mode**: this field settings (on|off) allows flexibility in working with different types of terminals (as PuTTY, hyper terminal, CRT..)as each handles the CR bit differently. When set to On the switch will drop <NULL> character only if it arrives immediately after the <CR> (^M, 0x0d). For all other modes of operation, NULL_CR is ignored. default – off **bind-ip:** an optional field. Mostly intended to be used when needed with IPSec VPN at policy mode. Bind-ip expects entry of the a local ACE interface of the router. The telnet service will be initiated with this ACE interface as its source IP. This configuration basically forces the ACE to use a specific local interface for the telnet session.
remove	**Service-id**: serial service id number which the designated serial port is configured as a member in ("local end point).
Show	Show output of the configuration and state

Example local Service

Below example demonstrates a setup of a single switch to which the serial device is connected to directly and as well the user PC (telnet client).



1. Create vlan for the service. port ge 0/3 must as well be a member.

```
Configure terminal
vlan 2
ports fastethernet 0/2 gigabitethernet 0/3 untagged fastethernet 0/2
exit
interface fastethernet 0/2
no shut
switchport pvid 2
exit
end
write startup-cfg
```

2. Assign an IP to application interface and configure the serial port.

The application IP Interface acting as the terminal server must be created with the service vlan ,in this case vlan 2. The mode od f operation of the serial port must be “transparent”. The local end point applicatin type must be “terminal server”.

```
RLGE2FE16R# application-connect
[/] router interface create address-prefix 192.168.2.201/24 vlan 2 purpose application-host
[/] serial port create slot 1 port 1 mode-of-operation transparent
[/] serial local-end-point create service-id 1 slot 1 port 1 application terminal-server
```

3. Configure the terminal server to listen on port 2050

```
[/] terminal-server admin-status enable
[/] terminal-server settings update low-border-telnet-tcp-port 2001 buffer-mode frame
[/]terminal-server tcp-service create service-id 1 remote-address 192.168.2.201
   telnet-port 2050
```

NOTE: Configuration for terminal-server serial-tunneling is not required nor allowed as the terminal server is local

Testing the setup

Ping between the PC (192.168.2.250) to the application (192.168.2.201).

Open a telnet session from the PC to the switch “telnet 192.168.2.201 2050”.

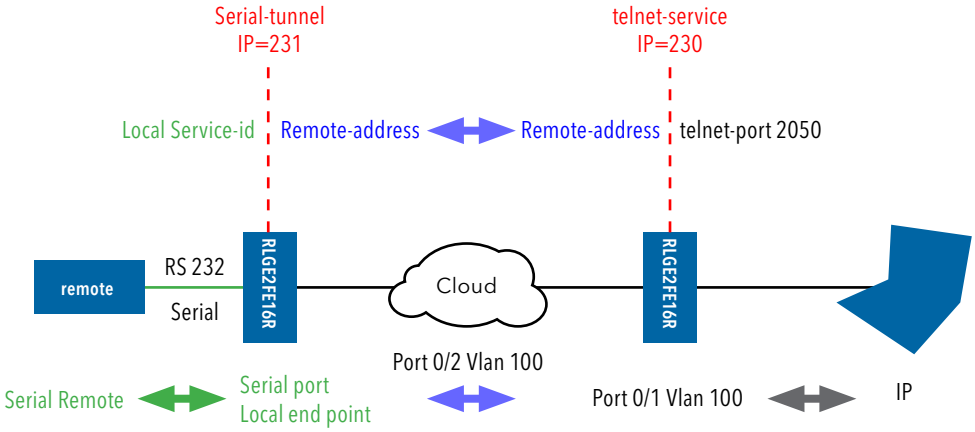
Your serial device shell will be available.

Show commands

```
[/] router interface show
+------+----------+------------------+-----------------+-------------+
| VLAN |   Name   |     IP/Subnet    |     Purpose     | Description |
+======+==========+==================+=================+=============+
| 2    | eth1.2   | 192.168.2.201/24 | application host |             |
+------+----------+------------------+-----------------+-------------+
[/] serial port show
+-----+------+------+-------+-------------+------+------+--------++
| idx | slot | port |  bus  |    mode     | baud | data | parity |
|     |      |      |       |             | rate | bits |        |
+=====+======+======+=======+=============+======+======+========+
|  1  |  1   |  1   | RS232 | Transparent | 9600 |  8   |  None  |
+-----+------+------+-------+-------------+------+------+--------+
[/] serial local-end-point show
+-------+---------+------+------+----------------+----------+----------+----------+
| index | service | slot | port |   application  | position | firewall | firewall |
|       |   id    |      |      |                |          |   mode   | protocol |
+=======+=========+======+======+================+==========+==========+==========+
|   1   |    1    |  1   |  1   | terminal-server |   N/A    | disable  |   any    |
+-------+---------+------+------+----------------+----------+----------+----------

[/] terminal-server telnet-service show
+-------+------------+------------+----------------+
| index | service id | telnet port |    dest ip     |
+=======+============+=============+================+
|   1   |     1      |    2050     | 192.168.2.201  |
+-------+------------+-------------+----------------+
[/] terminal-server connections show
+-------+---------+--------+---------------+---------------+---------+-----------
| index | service | telnet |  client   |  client   | service |  client   |  client  |
|       |   id    |  port  |  source IP  |  dest IP |  id   | dest slot | dest port |
+=======+=========+========+===============+===============+=========+===========
|   1   |    1    |  2050  | 192.168.2.250 | 192.168.2.201 |  1  |     1     |    1     |
+-------+---------+--------+---------------+---------------+---------+-----------
```

Example: Networking



Left Switch

1. Create vlan for the service. port ge 0/3 must as well be a member.

```
vlan 100
ports fastethernet 0/2 gigabitethernet 0/3
exit
interface fastethernet 0/2
no shut
exit
end
write startup-cfg
```

2. Assign an IP to application interface and configure the serial port. The application IP Interface acting as the local L3 interface for the serial servicing must be created with the service vlan, in this case vlan 100. The mode of operation of the serial port must be “transparent”. The local end point application type must be “terminal server”.

```
RLGE2FE16R# application-connect
[/] router interface create address-prefix 172.18.212.231/24 vlan 100 purpose application-host
[/] serial port create slot 1 port 1 mode-of-operation transparent
[/] serial local-end-point create service-id 1 slot 1 port 1 application terminal-server
```

3. Configure the terminal server

```
[/] terminal-server admin-status enable
[/]terminal-server serial-tunnel create service-id 1 remote-address 172.18.212.230
```

Right Switch

1. Create vlan for the service. port ge 0/3 must as well be a member.

```
vlan 100
ports fastethernet 0/1-2 gigabitethernet 0/3 untagged fastethernet 0/2
exit
interface fastethernet 0/1
switchport pvid 100
exit
interface fastethernet 0/2
switchport pvid 100
exit
end
write startup-cfg
```

2. Assign an IP to application interface The application IP Interface acting as the termnal server must be created with the service vlan ,in this case vlan 100.

```
RLGE2FE16R# application-connect
[/] router interface create address-prefix 172.18.212.230/24 vlan 100 purpose application-
host
```

3. Configure the terminal server

```
[/] terminal-server admin-status enable
[/]terminal-server tcp-service create service-id 1 remote-address 172.18.212.231
   telnet-port 2050
```

Setup is ready. you can now :

» Ping between the PC (172.18.212.240) to the application IP interfaces (172.18.212.230 and 231).

» Open a telnet session from the PC to the switch “telnet 172.18.212.230 2050”.

Your serial device shell will be available.

Modbus Gateway

The ComNet capability of gateway Modbus RTU to Modbus TCP is of yet another benefit to industrial area applications.

The switch allows connecting an RS232 Modbus RTU and gateway it to a remote Modbus TCP client (SCADA) over the Ethernet.

The Modbus RTU remote is connected at the switch local serial port, over an RS232 link. The Modbus TCP Client (SCADA) may be connected directly to the switch Ethernet port or via an IP cloud. The switch gateway will encapsulate the Modbus RTU to a TCP packet with port 502.

The switch Modbus gateway is assigned with the stations ID of the Modbus RTU devices connected to it.

The gateway is set to use a ACE IP interface as its TCP traffic source.

Packet sent from Modbus TCP Client will carry the gateway IP interface and the Modbus RTU station ID as its target. The gateway will listen to incoming packets and forward the message in a serial uniform to relevant Modbus RTU using the station id as identifier.

Up to 5 instances of a gateway can co-exist. Each must use a different ACE IP interface and have a unique gateway-id.

A serial port, connecting a Modbus RTU device, can be associated with a single gateway instance.

A Modbus RTU device must have at least one Modbus ID. Each Modbus ID must be unique behind the gateway.

Implementation

The Modbus gateway is supported between a Modbus TCP and a Modbus RTU.

Modbus TCP gateway to Modbus ASCII is not implemented.

The gateway translates Modbus frames of same structure, meaning is it a prerequisite to have the Modbus TCP device use the same frame structure as the Modbus RTU device.

NOTE: The terminal server service requires the use of an ACE IP interface type 'application-host'

Modbus Gateway Commands Hierarchy

+ root

+ application connect

  + router

    - interface create address-prefix <IP address>/[netmask] vlan <vlan id> purpose application-host [description <>]

    + serial

    + port

    - create {slot <1>} {port <1-4>} {mode-of-operation <transparent>} [baudrate <>][parity <>] [stopbits <>]

    - show

    + local-end-point

    - create create {slot <1>} {port <1-4>} {application <modbus-gw>}{service-id<>} [position <>] [protocol <>]

    - show

    + modbus-gw

    - show-gw-list

    - connection [clear | show]

    - counters

    - clear-id {gw-id <1-5>} {unit-id <1-255>}

    - clear-port {slot 1 port <1-4>}

    - show-by-id gw-id <1-5>} {unit-id <1-255>}

    - show-by-port {slot 1 port <1-4>}

    + debug

    - map-units-on-bus-show slot 1 port <1-4>

    - map-units-on-bus-start slot 1 port <1-4>

    - show-serial-points slot 1 port <1-4>

    - show-server-points slot 1 port <1-4>

    - show-tcp-points

+ history

- clear {gw-id <1-5>}

- show {gw-id <1-5>}

+ mapping

- add-gw {address-prefix <a.b.c.d/e>} {admin-status (enable| diable} {gw-id <1-5>} [timeout-period <500-100,000>]

- add-id {slot 1 port <1-4>} {gw-id <1-5>} {unit-id <1-255>}

- remove-gw {gw-id <1-5>}

- show-ids [gw-id <1-5>]

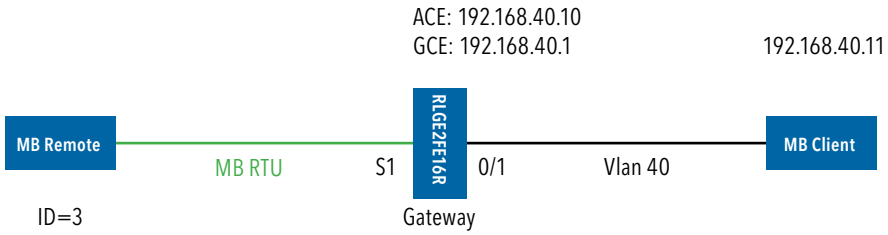
+ update [admin-status (enable| diable} | timeout {gw-id <1-5> timeout-period <500-100,000>}]

Modbus Gateway Commands Description

Command	Description
Application connect	Enter the industrial application menu
modbus-gw	
show-gw-list	Display the list of available gateway
Connection	Clear| show live and history TCP connections
counters	Clear| show counters per gateway id and unit id
debug	**map-units-on-bus-start** : initiate mapping of connected station ids behind a serial port. **map-units-on-bus-show** : show to station ids identified behind the serial port.
History	Show: Show latest reply from each unit and the time in seconds from that connection. Per gateway instance. Clear: Clear history table. Per gateway instance.
Mapping	Map a new gateway instance **address-prefix**: an IP address of an available ACE interface. A.b.c.d/e **admin-status**: (enable| disable) **gw-id**: unique gateway instance identifier. <1-5> **timeout-period**: set the maximum time allowed between incoming packets over the TCP session before dropping it <500-100,000> msec.
add-gw	add a gateway instance.
add-id	add a Modbus RTU station id to a serial port and a gateway instance.
Remove-gw	remove a gateway instance.
show-ids	show Modbus RTU station ids behind a gateway instance.
update	Update a gateway instance properties. **admin-status** (enable| disable. **timeout-period** <500-100,000>

Example

Following setup demonstrates Modbus gateway configuration.



1. set switch host name (optional)

```
set host-name Gateway
```

2. set service VLAN. Gigabitethernet 0/3 must be a tagged member.

```
config
vlan 40
ports fastethernet 0/1  gigabitethernet 0/3 untagged fastethernet 0/1
exit
interface fastethernet 0/1
alias MB_CLIENT
switchport pvid 40
exit
```

3. assign management IP (optional)

```
interface vlan 40
shutdown
ip address 192.168.40.1 255.255.255.0
no shut
end
```

4. access the ACE mode

```
application connect
```

5. assign IP interface for the gateway

```
router interface create address-prefix 192.168.40.10/24 vlan 40 purpose application-host
```

6. assign a serial port to be used for connecting the Modbus rtu remote

```
serial port create slot 1 port 1
serial local-end-point create slot 1 port 1 service-id 1 protocol modbus _ rtu application modbus-gw
```

7. Assign the gateway settings

```
modbus-gw mapping add-gw address-prefix 192.168.40.10/24 gw-id 4 admin-status enable
modbus-gw mapping add-id slot 1 port 1 gw-id 4 unit-id 3
```

output example

```
[/] modbus-gw connection show
+-------+-------+------------------+---------------+----------+
| Index | GW id |    GW IP/Subnet     |     ip addr      | src port |
+=======+=======+==================+===============+==========+
|   1   |   4   | 192.168.40.11/24  | 192.168.40.11 |  55132   |
+-------+-------+------------------+---------------+----------+
Completed OK
[modbus-gw/] debug map-units-on-bus-start port 1 slot 1
Port mapping started
Operation in process
[modbus-gw/] counters show-by-port
+------+------+----------+----------+----------+----------+
| Slot | Port | Rx valid | Rx error | Tx valid | Tx error |
+======+======+==========+==========+==========+==========+
|  1   |  1   |   477    |    0     |   582    |    0     |
+------+------+----------+----------+----------+----------+
[modbus-gw/] counters show-by-id gw-id 4
 gwid:4 unit id:65535
+----+---------+----------+----------+----------+----------+
| Gw | Unit Id | Rx valid | Rx error | Tx valid | Tx error |
+====+=========+==========+==========+==========+==========+
| 4  |    3    |   477    |    0     |   599    |    0     |
+----+---------+----------+----------+----------+----------+
+------+------+----------+----------+----------+----------+
| Slot | Port | Rx valid | Rx error | Tx valid | Tx error |
+======+======+==========+==========+==========+==========+
|  1   |  1   |   477    |    0     |   616    |    0     |
+------+------+----------+----------+----------+----------+
```

```
[modbus-gw/] debug map-units-on-bus-show
Operation in process
[modbus-gw/] history show gw-id 4
Units connected to Gw 4:
+----+-----------------+
| id | seconds elapsed |
+====+=================+
| 3  |       153       |
[modbus-gw/] mapping show-ids
+----------+-----------------+---------+------+------+-------+
| GW index |   GW IP/Subnet   | Unit Id | slot | port |  bus  |
+==========+=================+=========+======+======+=======+
|     4     | 192.168.40.10/24 |    3    |  1   |  1   | RS232 |
+----------+-----------------+---------+------+------+-------+

[modbus-gw/] debug show-serial-points
Serial points:
slot:1, port:1, pointer:0x1007c408
[modbus-gw/] debug show-server-points
Server points:
IP addr:192.168.40.10, GwId:4, Subnet mask:255.255.255.0, pointer:0x10081580,
[modbus-gw/] debug map-units-on-bus-show
List of units for slot[1] port[1]:
Port mapping ended
```

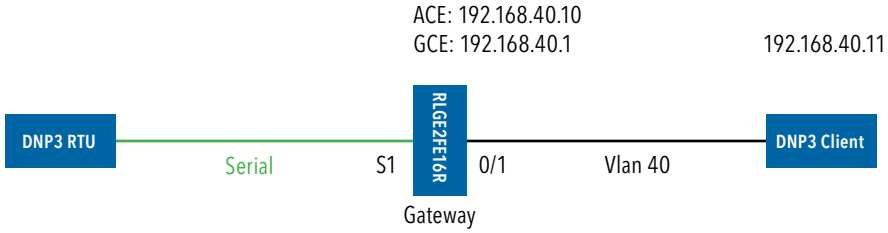
DNP3 Gateway

DNP3 (Distributed Network Protocol) is an important protocol set used at SCADA applications.

The ComNet switch supports gateway functionality between a DNP3 TCP client (local) and a DNP3 Serial RTU. Configuration of a DNP3 gateway is made using the terminal server feature with the protocol well known TCP port 20000. Please refer to the terminal server chapter for configuration structure.

Example

Following setup demonstrates DNP3 gateway configuration.



1. set switch host name (optional)

```
set host-name Gateway
```

2. Set service vlan. Gigabitethernet 0/3 must be a tagged member.

```
config
vlan 40
ports fastethernet 0/1  gigabitethernet 0/3 untagged fastethernet 0/1
exit
interface fastethernet 0/1
alias CLIENT
switchport pvid 40
exit
```

3. assign management IP (optional)

```
interface vlan 40
shutdown
ip address 192.168.40.1 255.255.255.0
no shut
end
```

4. access the ACE mode

```
application connect
```

5. assign IP interface for the gateway

```
router interface create address-prefix 192.168.40.10/24 vlan 40 purpose application-host
```

6. assign a serial port to be used for connecting the DNP3 RTU remote

```
serial port create slot 1 port 1 mode-of-operation transparent
serial local-end-point create slot 1 port 1 service-id 1 protocol application terminal-server
```

7. assign the gateway using terminal server settings

```
terminal-server admin-status enable
terminal-server settings update low-border-telnet-tcp-port 19999 buffer-mode frame
terminal-server tcp-service create service-id 1 remote-address 192.168.40.10 telnet-port 20000
exit
write startup-cfg
```

Protocol Gateway IEC 101 to IEC 104

The ComNet switch, using its application module implements the gateway for IEC101 serial devices to the IEC104 IP protocol. The IEC101 and IEC104 protocols are fully integrated in the application module thus allowing the IEC101 remote devices to be represented as a IEC104 server in the IP network and to be addressed as such by IEC104 clients located anywhere in the network.

The gateway implementation consists of 3 functions:

- IEC104 Server – The application module will act as a IEC104 server to any IEC104 clients that connect to it over the Ethernet network. This function includes the full implementation of the state-machine of the IEC104 server, response to keep-alive test frames and listening of TCP port 2404 for any client requests.
- IEC60870 message router – The application module will act as a application router translating the requests received by the IEC104 server to commands issued by the IEC101 local with the proper IEC101 address and sending the responses vice versa.
- IEC101 Master – The application module will act as a IEC101 local to the IEC101 server devices connected to the assigned serial interfaces in the switch. This function includes the full implementation of the state-machine of the IEC101 local, initialization and arbitration of the IEC101 bus and issuing commands to the appropriate IEC101 remote to provide the response to the requests which arrive from the message router.

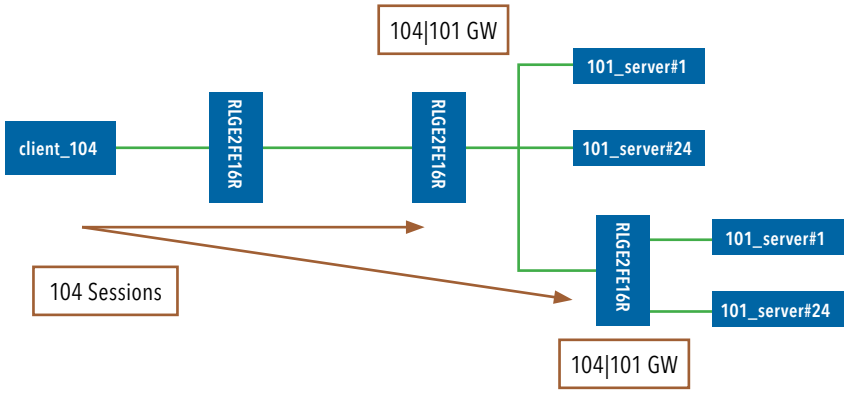
The IEC101 devices will be configured with their serial link properties, device address and ASDU address to be uniquely identified behind the gateway.

Overall the IEC101 devices will be addressed from the IEC104 remote client using the following hierarchical addressing scheme: IP address of the ACE module in which the IEC101/104 gateway is implemented, IEC101 device address, ASDU address and IOA (Information Object Address - for example ,the actual address of the discrete inputs mapped at the IEC101 RTU).

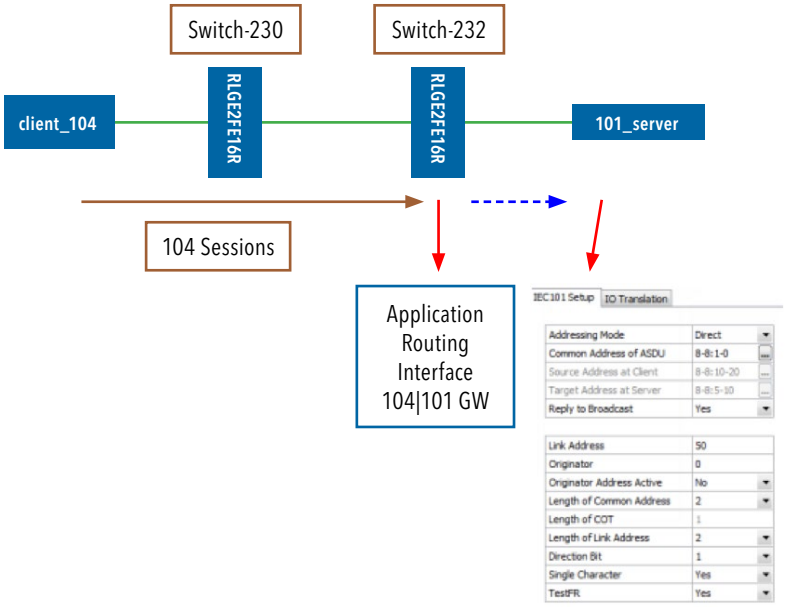
Modes of Operation

The gateway supports 2 topologies for the IEC101 devices as defined by the standard:

» Balanced Mode – Up to 24 unique IEC-101 servers behind each single gateway



- Unbalanced Mode – Up to 32 ASDU addresses behind each IEC101 server device



IEC101/104 Gateway properties IEC 101

- » System role : Controlling station definition (Master)
- » Network configuration :
  - › Point-to-point
  - › Multiple point-to-point
  - › Multipoint-party line (planned)
- » Physical layer
  - › Transmission speed in monitor & control direction: 300 – 38400bps
- » Link layer
  - › Link transmission procedure
    - ·Balanced transmission
    - ·Unbalanced transmission
  - › Address field of the link
    - ·Not present (balanced transmission only)
    - ·One octet
    - ·Two octets
    - ·Structured values translation
    - ·Unstructured
- » Application layer
  - › Common address of ASDU
    - ·One octet
    - ·Two octets
  - › Information object address
    - ·Two octets
    - ·Three octets
    - ·Structured
    - ·Unstructured
  - › Cause of transmission
    - ·One octet
    - ·Two octets (with originator address)

IEC101/104 Gateway Configuration

A gateway setup configuration should include the following parameters:

» ACE IP address – ACE IP interface is mandatory to be set and should be associated with a VLAN for the uplink traffic. This application IP interface acts as the IEC104 server in the Ethernet network and represents all the IEC101 devices connected locally to the switch towards the IEC104 clients.

» Optional remote IP addresses - When configuring the IEC104 service-group you should also provide the IP addresses of the IEC104 clients so the proper service-aware firewall rules can be defined.

» IEC101 device parameters - For the serial interfaces the physical link properties should be configured (baud-rate, parity, stop bits). Furthermore the IEC101 addressing information should be provided and the devices should be assigned to the IEC104/101 gateway.

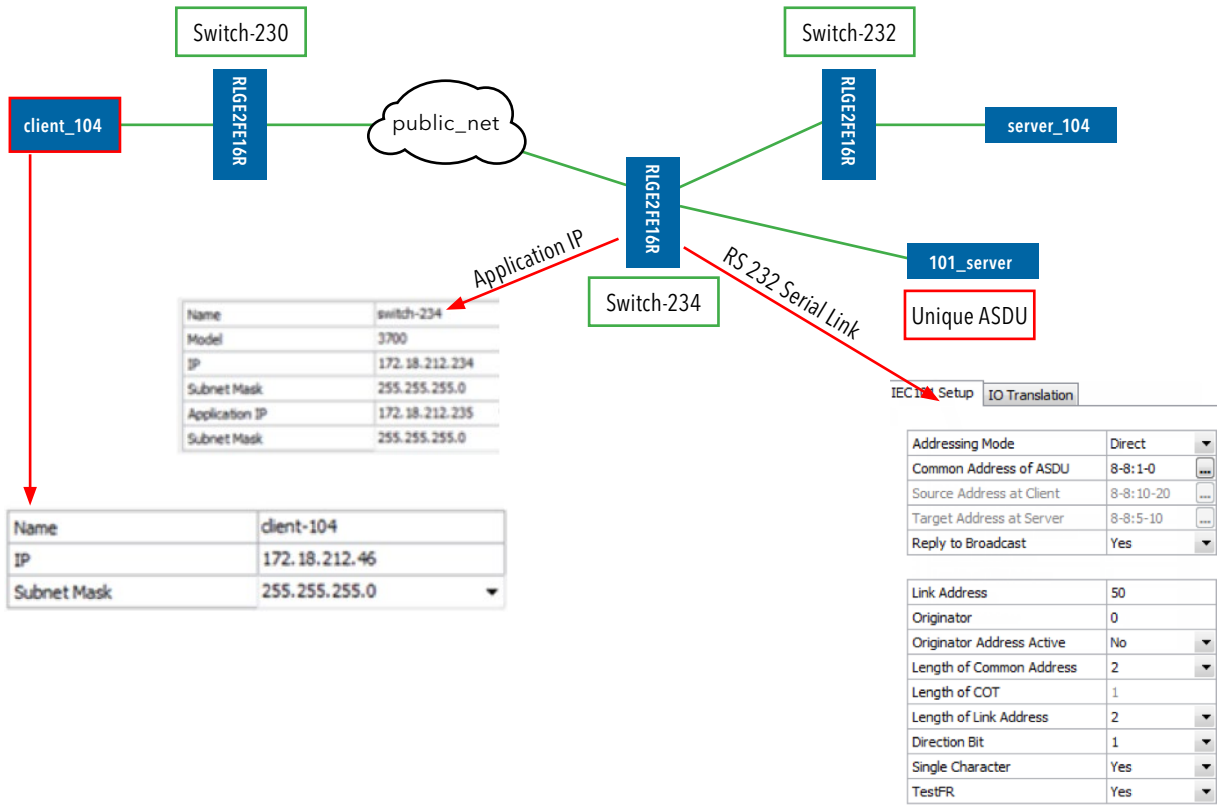


Figure 7 : Gateway service configuration in iSIM

Gateway 101/104 Configuration Flow

When attending a setup configuration, follow these below steps.

1. Ethernet connectivity towards the IEC 104 Client (SCADA)
    a. Set service vlan and assign relevant ports.
    b. Set ACE IP interface with the service vlan
    c. Set static or dynamic routing if needed to reach the IEC 104 Client.
    d. Verify by following methods
        i. Successful ping between the IEC 104 Client (SCADA) and the RLGE2FE16R ACE interface.
        ii. IEC 104 connection established. Use the command “iec101-gw show all” to verify connection at the switch.
2. Serial connection towards the locally connected IEC101 server (RTU)
    a. Configure a serial port
        i. Serial properties as baudrate, parity and such, must be consistent with those of the RTU.
        ii. The serial port must be configured with ‘mode-of-operation set to ‘transparent’.
    b. Configure a local service (serial local-end-point)
        i. Create a local-end-point and assign the serial port.
        ii. The local-end-point field ‘application’ must be set to ‘iec101-gw’
    c. Enable the gateway
        i. Assign the gateway to use the predefined ACE interface.
        ii. Set the desired mode ‘balanced’ or ‘unbalanced’.
    d. Configure the gateway with the RTU IEC101 properties. Key values are advised here
        i. Common Address of ASDU value (CLI field ‘asdu_addr’). As set at the RTU.
        ii. Common Address of ASDU length in bytes (CLI field ‘common_address_field_length’). As set at the RTU.
        iii. Link Address (CLI field ‘link_addr’). As set at the RTU.
        iv. Link Address length in bytes (CLI field ‘link_address_field_length’). As set at the RTU.
        v. Cause of Transmission length in bytes, determined by the usage of the originator address field in the protocol. (CLI field ‘orig_addr_participate’)
        vi. Connect the IEC101 server (RTU) to the serial port with a proper serial cable. Pin-out of the RS232 RJ45 port of the switch is given in this manual. Control lines are not supported for the gateway application. Usage of Tx,Rx and GND lines are allowed.

e. Verify by following methods

i. Use the command “iec101-gw show all” to verify the operational status (‘OP ST’) is UP.

ii. Follow serial port and gateway counters to check if serial traffic is received and transmitted at the serial port. Show commands “serial port show slot 1 port <x>” and “iec101-gw cnt show” are available.

3. Trouble shooting

a. Most trouble shooting is usually at the IEC101 connection to the locally connected RTU. The IEC 104 connection between the gateway and the client (SCADA) is based on straightforward Ethernet connectivity which is easy to establish and diagnose.

b. If the IEC101 (‘OP ST’) is in any other state other then ‘UP’, try the following

i. Verify your serial physical connection.

ii. Verify the RTU is on and properly configured.

iii. Follow the serial port counters to verify traffic is received and transmitted at the serial port. If only Rx counters are progressing, check again the serial properties of both the gateway and the RTU (baudrate, parity and such).

iv. Verify the IEC properties are consistent between the gateway and the RTU (CA, LA, CA length, LA length, COT)

NOTE: The terminal server service requires the use of an ACE IP interface type ‘application-host’

Gateway 101/104 Commands Hierarchy

+ application connect

    + router

        - interface create address-prefix <IP address>/[netmask] vlan <vlan id> purpose application-host [description <>]

        + serial

        + port

        - clear counters

        - create {slot <1>} {port <1-4>} {mode-of-operation < transparent >} [baudrate <9600,(50-368400)>] [parity {no,no| odd| even}]
          [stopbits <1|2>] databits {8,<5-8>}
          admin-status [up| down]

        - update {slot <1>} {port <1-4>} {mode-of-operation < transparent >} [baudrate <9600,(50-368400)>] [parity {no,no| odd| even}]
          [stopbits <1|2>] databits {8,<5-8>}
          admin-status [up| down]

        - show

        + local-end-point

        - create {slot <1>} {port <1-4>} {application <iec101-gw>}
          {service-id <1-100>} [position <remote>]

        - remove {slot <1>} {port <1-4>} {service-id <1-100>}

        - show

        + iec101-gw

        - operation {start | stop}

        - cnt show

        - show {all| iec101 {log| state} {slot <1>} {port <1-4>} }

        + config

        - gw update mode {balanced,(balanced| unbalanced)} ip_addr <A.B.C.D>

        - iec101 {create | update}
          {slot <1>} {port <1-4>} {asdu_addr {(1-255)| (1-65534)}}
          {link_addr {(1-255)| (1-65534)}}
          [common_address_field_length <2,(1|2)>]

[translated_cmn_addr {(1-255)| (1-65534)}]
[link_address_field_length <2,(1|2)>]
[ioa_length <3,(1|2|3)>] [orig_address <1-255>]
[orig_addr_participate <y,(y|n)>]
[dir_bit<AUTO,(AUTO|0|1)>] [single_char <y,(n|y)>]
[test_proc <y,(n|y)>] [gen_inter <n,(n|y)>] [time_tag <n,(n|y)>]

- iec101 remove {slot <1>} {port <1-4>}

- iec101 [add_asdu | remove_asdu] slot <1> port <1-4>
  {asdu_addr {(1-255)| (1-65534)}} {link address {(1-255)| (1-65534)}}

- iec101 [add_ioa_trans>| remove_ioa_trans] slot <1> port <1-4>
  src_ioa {a1-a2-a3| a1-a2| a} trans_ioa {a1-a2-a3| a1-a2| a}

- iec104 {update | remove} {ip_addr <>} [clock_sync <n|y>] [orig_addr <>] [t0 <30sec,[1-255]>] [t1 <15sec,[1-255]>] [t2 <10sec,[1-255]>] [t3 <20sec,[1-255]>]

Gateway 101/104 Commands

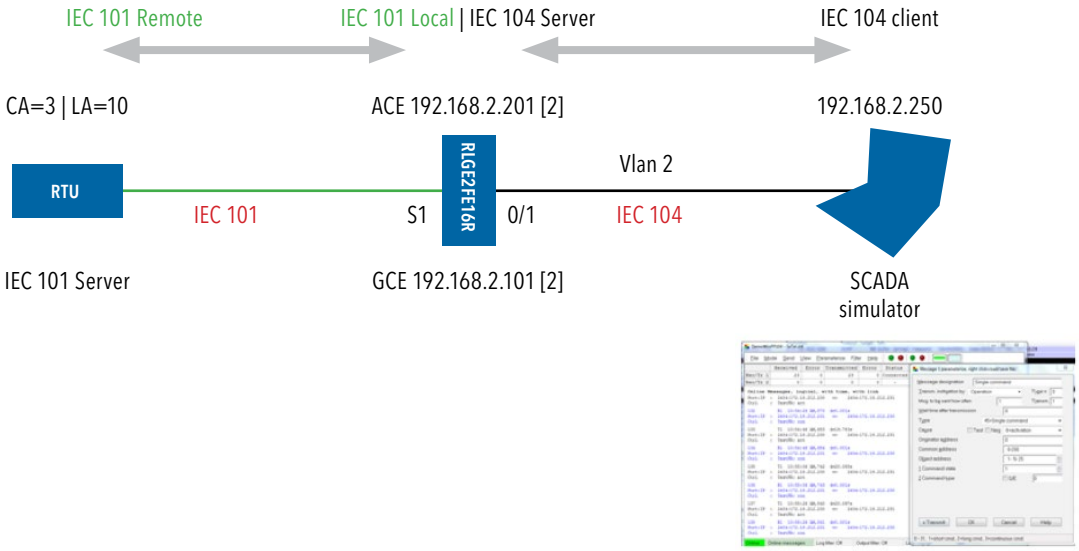
Command	Description
iec101-gw	Configuration mode of 101/104 gateway
Operation	Start : activate the gateway Stop : stop the gateway *takes effect on all IEC 101 nodes connected to the switch
Config	
gw update mode	**Unbalanced** – for 101 servers unbalanced topology. **Balanced** (default)– for 101 servers balanced topology. **ip_addr**– IP address of a chosen application IP interface. The IP interface must be configured prior to it be used by the gateway **!changing this field requires reloading the switch**
iec101 create | update | remove	**Slot ,Port:** physical interface where the 101 remote is connected at. **asdu_addr** : Common Address of ASDU. Usually Should be configured as the ASDU address of the IEC101 Server unless a translation service is required. In the latter case, should be configured as the address which is set at the 104 Client for the server. A decimal value of 1-255 or 1-65534 is allowed depending if 'common_address_field_length' is set to one byte or two. **common_address_field_length**: length in bytes of the Common Address of ASDU. Permissible values are one or two bytes. Should be identical to the configuration at the IEC 101 server. **translated_cmn_addr** – used when a translation service required for the common address of asdu. The value should be identical to the actual common address of the IEC101 Server. A decimal value of 1-255 or 1-65534 is allowed depending if 'common_address_field_length' is set to one byte or two. **link_addr**: Should be configured as the Link address of the 101 remote. A decimal value of 1-255 or 1-65534 is allowed depending if 'link_address_field_length' I set to one byte or two. **link_address_field_length**: length in bytes of the Link Address. Permissible values are one or two bytes. Should be identical to the configuration at the 101 remote. **orig_addr**: Should be configured as the Originator address set at the 101 remote. **orig_addr_participate**: y|n to indicate if the 101 remote uses the originator address field. Should be identical to the configuration at the 101 remote. the Cause Of Transmission (COT) will be influenced by this configuration. 'y' – COT will be 2 byte in size. 'n' - COT will be 1 byte in size. **dir_bit**: y|n are permissible values. Should be opposite to the configuration at the 101 remote. relevant in Balanced mode only. **single_char**: y|n are permissible values. Should be configured identical to the 101 remote configuration. relevant in Balanced mode only. **ioa_len** – IO object length. Permissible values are 1|2|3 bytes. Should be identical to the configuration at the 101 remote.
[add_ioa_trans>| remove_ioa_trans]	**Slot, Port**: physical interface where the 101 remote is connected at. **src_ioa**: value of the 101 server Object address as set at the 104 client. May be 1/2/3 bytes long depending on the settings of 'ioa_length'. A value is expected as 'byte1'-'byte2'-'byte3' or 'byte1'-'byte2' or 'byte-1'. Permissible value for each byte is 1-255. example for 3 bytes size IOA: 5-212-151. **trans_ioa**: value of the 101 server Object address. May be 1/2/3 bytes long depending on the settings of 'ioa_length'. A value is expected as 'byte1'-'byte2'-'byte3' or 'byte1'-'byte2' or 'byte-1'. Permissible value for each byte is 1-255. example for 3 bytes size IOA: 5-212-151.
iec104 {update | remove}	**ip_addr**: IP address of the SCADA **orig_addr**: originator address of the SCADA. **to**: Time-out of connection establishment **t1**: Time-out of send or test APDUs **t2** : Time-out for acknowledges in case of no data messages t2 < t1 **t3**: Time-out for sending test frames in case of a long idle state

Example Gateway 101/104

Below example demonstrates an IEC 101 Server (remote) – IEC104 Client (SCADA) service using the RLGE2FE16R as the gateway.

The settings for IEC101 include the serial link properties and the RTU 101 parameters for Common Address, Link address and such.

Following the below configuration the 104 Client is able to send the various Type-IDs (commands) via its TCP connection to the serial RTU.



Configuration

1. Create vlan for the service. Port gigabitethernet 0/3 must as well be a member.

```
Config
vlan 2
ports fastethernet 0/1 gigabitethernet 0/3 untagged fastethernet 0/1
exit

interface fastethernet 0/1
switchport pvid 2
exit
```

2. Assign L3 interface for management to vlan 2 (not mandatory)

```
interface vlan 2
shutdown
ip address 192.168.2.101 255.255.255.0
no shutdown
end

write startup-cfg
```

3. Create an ACE interface for the gateway

```
application connect
router interface create address-prefix 192.168.2.201/24 vlan 2 purpose application-host
```

4. Configure the serial port properties. Field 'mode-of-operation must be set to 'transparent'. The port properties must be in-line with the IEC 101 server device connected (same baud rate, parity, stop bits, data bits and such)

```
serial port create slot 1 port 1 mode-of-operation transparent baudrate 9600 parity even
```

5. Create the local serial service for the port. the field 'application' must be set to 'iec101-gw'

```
serial local-end-point create slot 1 port 1 service-id 1 application iec101-gw
```

6. Configure the gateway mode of operation and choose the ACE interface to be used. the ACE interface must be available in advance.

```
iec101-gw config gw update mode balanced ip _ addr 192.168.2.201
```

7. Configure the gateway properties to be in line with the IEC101 server settings.

```
iec101-gw config iec101 create slot 1 port 1 asdu _ addr 3 orig _ addr 0 link _ addr 10
link _ address _ field _ length 2 common _ address _ field _ length 2 orig _ addr _ participate y
```

8. Show commands to follow gateway configuration and state

```
[/] serial local-end-point show
+-------+---------+------+------+-------------+----------+----------+----------+
| index | service | slot | port | application | position | firewall | firewall |
|       |   id    |      |      |             |          |   mode   | protocol |
+=======+=========+======+======+=============+==========+==========+==========+
|   1   |    1    |  1   |  1   |   101-gw    |   N/A    | disable  |   any    |
+-------+---------+------+------+-------------+----------+----------+----------+
[/]
[/] iec101-gw show iec101 state slot 1 port 1
Connection state at slot 1 and port 1 is UP
[/] iec101-gw show all
101-104 ROUTER
BALANCED MODE
IEC 104:
+---------------+-----------+-----------+----------+----+----+----+----+
```

```
|        IP        | ORIG. ADDR | CLOCK SYNC | TIME TAG | T0 | T1 | T2 | T3 |
+==================+============+============+==========+====+====+====+====+
| 192.168.2.201    |      0     |      n     |     n    | 30 | 15 | 10 | 20 |
| 192.168.2.250    |      0     |      n     |     n    | 30 | 15 | 10 | 20 |
+------------------+------------+------------+----------+----+----+----+----+

IEC 101:
+------+------+-------+----------+---------+--------------+----------+---------+---------+----
-----+---------+--------
|SLOT|PORT|OP ST|LINK ADR|CMN ADR|CONV CMN ADR|LINK LEN|CMN LEN|COT LEN|IOA LEN|SRC IOA|CONV
+======+======+=======+==========+=========+==============+==========+=========+========
| 1  | 1  |  UP   |  10   |   3    |      0      |  2    |   2   |   2    |   3    |     |      |
+----+---+-------+------+--------+-------------+------+-------+---------+-------+-----+------
+----+---+-------+------+--------+---------+---------+--------+---------+-------+-----+------+
|SLOT|PORT|ORIG. ADR|S CH|DIR BIT|TEST FR|GEN INT|TIME TAG|COT LEN|IOA LEN|CMN (UB)|LINK (UB)|
+======+======+===========+======+=========+=========+=========+==========+=========+========+===
| 1  | 1  |     0     |  y | AUTO |  y    |  n    |    n    |  2    |  3    |   3    |  10     |
+------+------+-----------+------+---------+---------+---------+----------+---------+---------
[/]

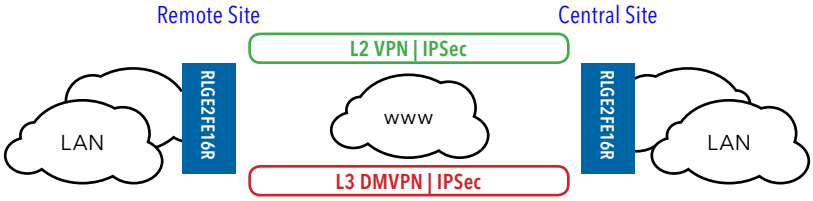

[/] iec101-gw cnt show
#Msgs error for 101       : 0
#Msgs error for 104       : 0
#Msgs(RF) IEC101 RECV     : 332
#Msgs(RF) IEC101 SEND     : 354
#Msgs(RF) IEC104 RECV     : 64
#Msgs(RF) IEC104 SEND     : 63
# IEC104 CONNECTED          : 1
[/]
```

VPN

Background

When a distributed operational network uses public transport links for the inter-site connectivity, the traffic must be encrypted to ensure its confidentiality and its integrity. The ComNet switches support such a VPN (Virtual Private Network) connection using GRE tunnels (RFC2 2784) over an IPSec encrypted link. The IPSec tunnel can be set to use 3DES or AES encryption per the user configuration.

IPSec policy determines the 'interesting traffic', meaning the type or subset of the customer traffic to be encrypted.



Modes supported

With the ComNet routers both L2 and L3 VPNs are supported. Both modes are based on GRE tunnelling.

Operational Modes:

1. L2 GRE VPN.

2. DM-VPN .GRE, Route based.

3. IPSec VPN. Route based

4. IPSec VPN. Policy based

NOTE: Multiple VPN types cannot co-exist simultaneously

Layer 2 VPN

The mode of layer 2 GRE VPN provides a GRE encapsulation of the traffic over the network. Used together with IPSec will result in encrypted tunnel as a main measure against min in the middle attack. This mode maintains layer 2 connectivity between the customer equipment thus minimizing the effort for the customer in configuration and network routing planning.

At below drawing, a GRE tunnel is established between the routers interfaces 'eth1.20' and 'eth1.30'.

The customer equipment (PC, RTU) reside at the same subnet. The PC and RTU will not have a connection between them (due to the layer 3 network in between) until the L2-VPN has established.

At the HUB,

» The interesting traffic is VLAN 10 at which the PC is connected. The ACE gigabit 0/4 port will be assigned as a tagged member at this VLAN to mark this VLAN for IPSec encryption.

» The IPSec policy must define the encryption of GRE traffic.

» The IPSec policy should define protocol 'any' and source/ destination subnets 'any' as its rules. This is because the interesting traffic to encrypt was already determined by tagging gigabit 0/4 at relevant customer VLANs.

Topologies supported and guidelines:

1. Single Hub vs Multiple Spokes

2. Multiple tunnels allowed at the hub.

3. Single tunnel allowed at each spoke towards the Hub.

4. The hub must be connected to the network using one of its Ethernet ports. A cellular unit may not act as hub.

5. A Spoke may have L2 VPN set over its cellular interface (at supported hardware) or Ethernet ports.

If using an Ethernet port (not a cellular link) for the wan connections. the spoke must be set to use an ACE interface of 'application-host' type as the tunnel source.

6. The hub listens for incoming NHRP requests from the spokes to initiate VPN. As such it must hold a static IP address which is routable over the network. The hub must be set to use an ACE interface of 'application-host' type as the tunnel source.

7. The L2 VPN is MAC aware.

8. Layer 2 protection protocols as RSTP are supported to allow protection between a VPN uplink and a physical uplink.

9. IPSec policy should be defined to encrypt GRE protocol.

10. The interesting traffic is determined by tagging the ACE port gigabitethernet 0/4 at the relevant user vlans.

Main advantages

1. Easy to configure and maintain

2. Users connected at remote ends of the tunnel maintain layer 2 connectivity sharing the same VLAN and subnet.

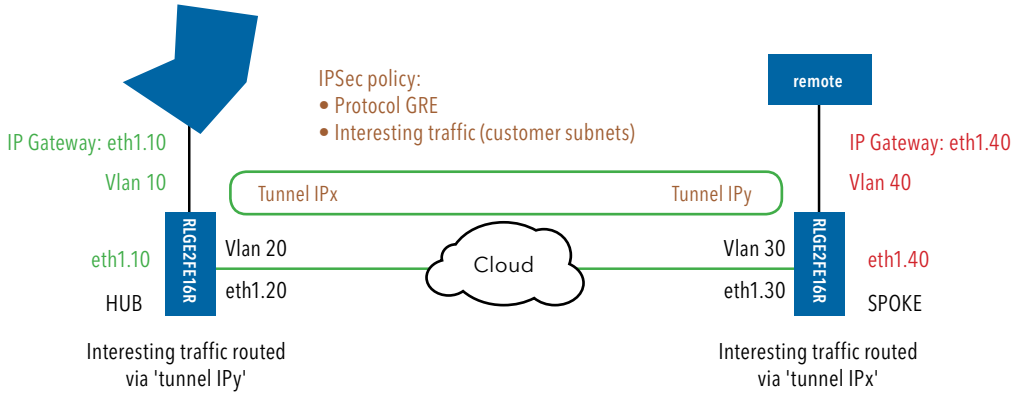
DM-VPN

The DM-VPN mGRE mode is routing based and supports more complex networking and protection over the L2-VPN, providing higher scalability.

At below drawing, a GRE tunnel is established between the routers interfaces 'tunnel IPx' and 'tunnel IPx'.

At the HUB:

- A designated interface is created as the local tunnel source ('tunnel IPx').
- The local tunnel interface 'tunnel IPx' is using the local vlan interface et1.20 as a 'lower layer' for the wan networking.
- Traffic designated towards the subnet of the RTU is routed via the tunnel remote interface 'tunnel IPx' using static route entry or dynamic protocols.
- The IPSec policy must define the encryption of GRE traffic, which means traffic routed via the VPN interfaces.
- The IPSec policy may define the subnets of the PC and of the RTU as the interesting traffic to encrypt. It may as well use 'any' as the protocol rule to encrypt since the traffic routed via the GRE tunnel interfaces should be only the interesting traffic. In other words, if the traffic is not to be encrypted, it should not be routed via the tunnel to begin with.



Topologies supported and guidelines

1. Multiple Hubs vs Multiple Spokes
2. Multiple Clouds
3. Multiple tunnels allowed at the hub.
4. Multiple tunnels allowed at each spoke towards different Hubs or towards the same hub via different clouds.
5. Supports static routing and OSPF
6. Layer 3 protection
7. The hub is recommended to be connected to the network using one of its Ethernet ports. A cellular uplink at the hub is not recommended as an aggregation interface to multiple VPNs.
8. A Spoke may have DM-VPN set over its cellular interface (at supported hardware) or Ethernet ports.
9. The hub listens for incoming NHRP requests from the spokes to initiate VPN. As such, it must hold a static IP address which is routable over the network.
10. mGRE interface('s) is created as the local end point of the GRE tunnel. The mGRE is assigned to a 'lower layer' VLAN interface which is established for the wan connection.
11. IPSec policy should be defined to encrypt GRE protocol.
12. The interesting traffic is determined by routing it via the mGRE interface.

Main advantages

1. Robust and supports large scale networks
2. Encryption of traffic as a protective measure against man in the middle attacks.
3. Addition of Spokes may not require further configuration at the Hub.

IPSec-VPN

IPSec VPN is designated for simple P2P networking where encryption is required. Two modes are supported:

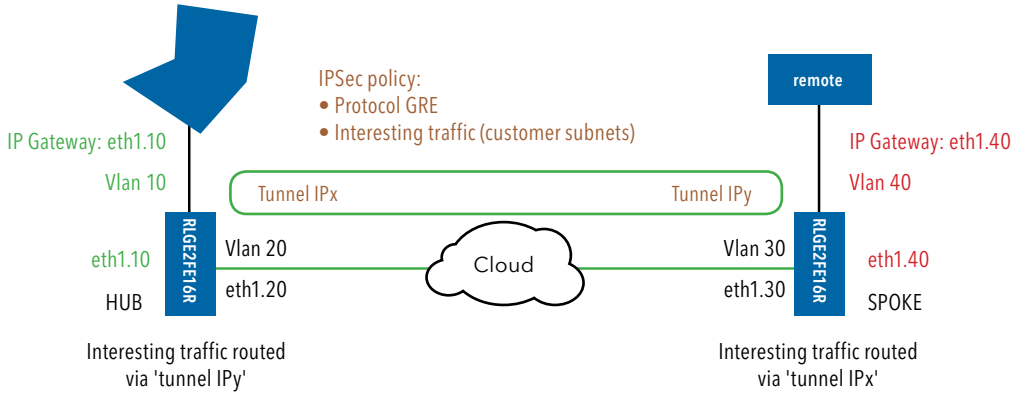
Transport Mode (Route based)

This mode is a route based, meaning the interesting traffic is routed via a specific path in order to be encrypted. A Tunnel interface is created at the routing table. The interesting traffic is routed over the tunnel interface. The IPSec policy must define 'ipencap' as the protocol to encrypt and the customer subnets.

At below drawing, a tunnel is established between the routers interfaces 'tunnel IPx' and 'tunnel IPx'.

At the HUB:

- A designated interface is created as the local tunnel source ('tunnel IPx').
- The local tunnel interface 'tunnel IPx' is using the local VLAN interface et1.20 as a 'lower layer' for the wan networking.
- Traffic designated towards the subnet of the RTU is routed via the tunnel remote interface 'tunnel IPx' using static route entry or dynamic protocols.
- The IPSec policy must define the encryption of ipencap traffic, which means traffic routed via the VPN interfaces.
- The IPSec policy may define the subnets of the PC and of the RTU as the interesting traffic to encrypt.



Tunnel Mode (Policy Based)

This mode is referred to as policy based. The interesting traffic is defined at the IPSec policy. Since there is no addition IP interface created specifically for the tunnel source, the IPSec policy must define both the interesting traffic source/ destination and the network interfaces source/ destination.

At below drawing, a tunnel is established between the routers wan interfaces 'eth1.20' and 'eth1.30'. No additional tunnel specific interfaces are required.

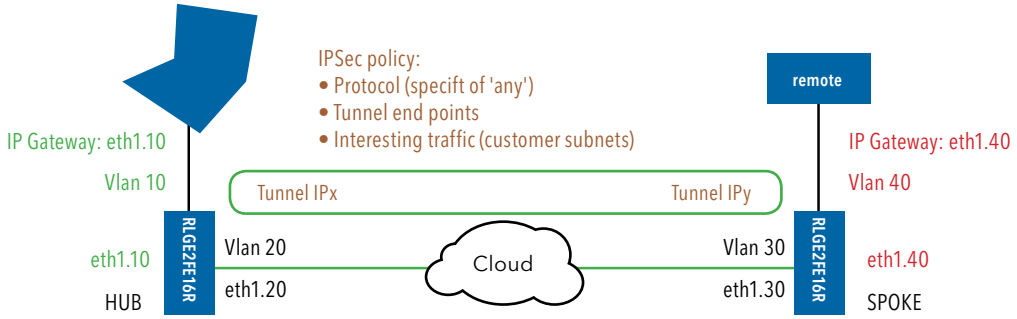
At the HUB:

» Routing is established to provide networking towards the RTU.

» The IPSec policy will define the subnets of the PC and of the RTU as the interesting traffic to encrypt.

» The IPSec policy must define the routers interfaces eth1.20 and eth1.30 as the source/ destination of the tunnel.

» The IPSec policy may define a specific type or protocol to be encrypted or 'any'.



Topologies supported and guidelines

1. Point to Point, Hub vs Spoke.
2. Single tunnel allowed at the hub.
3. Single tunnel is allowed at the spoke.
4. The hub must be connected to the network using one of its Ethernet ports.
5. The spoke is recommended to be connected to the network using one of its Ethernet ports. The spoke may use a cellular connection only if the SIM is allocated by the ISP with a public, static IP address, without NAT.
6. Layer 3 protection to a second uplink is supported.
7. The hub must hold a static IP address which is routable over the network.
8. The spoke must hold a static IP address which is routable over the network.

Main advantages

1. Easy to configure an maintain.

2. Encryption of traffic as a protective measure against man in the middle attacks.

3. Interoperability with other vendors.

L2-VPN Commands Hierarchy

+ root

+ application connect

+ vpn

+ l2

+ tunnel

- create {local-end-point <>} {remote-address <>} {name <>}

- remove {name <>}

- show

- parameters [icmp-send-fragmentation-needed <enabled| disabled>] [spanning-tree-mode [normal| transparent>]

+ nhrp

- hub show

- spoke {[update {private-ip <>} {remote-ip <>}] | [show]}

+ fdb

- show

- clear

NOTE: See IPSec chapter for IPSec configuration

L2-VPN Commands

Command	Description
Application connect	Enter the industrial application menu
L2-vpn	Enter the tunnel configuration
nhrp	For cellular application only
Hub show	For cellular application only show : show IP of currently connected cellular spokes
Spoke {update | show}	For cellular application only Update remote-ip: configure remote IP of Hub in format of A.B.C.D. Update private-ip: configure local identifier in the form IP A.B.C.D.
Tunnel	Clears tunnel counters
Create | remove	Name : name of the tunnel Local-end-point : local IP of the application interface Remote-end-pont : application interface IP at remote switch.
Fdb {clear | show}	Clear / Show FDB

DM-VPN Commands Hierarchy

+ application connect

+ vpn gre

+ tunnel

- create {name <>} {address-prefix <A.B.C.D/M>}
  {lower-layer-dev <ppp0| ETH1.(vlan-id)>} {key <0.0.0.0,<a.b.c.d>}
  [ttl <64,0-255>] [holding-time<7200,1-65535>]
  [mtu (1418,<128-9600>)] [tos (inherint,<hex(0-255)>)]
  [cisco-authentication <>]

- remove {name<>}

- show [name<>]

+ nhrp

+ map

- {craete | update} {multipoint-gre-name<>}
  {nbma-address<A.B.C.D>} {protocol-address-prefix< A.B.C.D/M>} [initial-register<no|yes>]
  [is-cisco<no|yes>]
  [protection-group<>] [position<local |remote>]

- remove {multipoint-gre-name<>}

- show

- show-status

- cache-flush

- cache-purge

- cache-show

- {enable | disable}

- log-show

- route-show

- show

+ protection-group

- {create |udate |remove} {name<>} [default-route<yes,no|yes> wait-to-restore<0-1440>]

- show

NOTE: See IPSec chapter for IPSec configuration

IPSec-VPN Transport mode Commands Hierarchy

+ application connect

+ vpn ipsec

+ tunnel

- create {name <>} {address-prefix <A.B.C.D/M>}
  {lower-layer-dev <ppp0| ETH1.(vlan-id) >} {remote-address< A.B.C.D >} [mtu<1400,128-1500>][ttl <64,0-255>]
  [tos (inherint,<hex(0-255)>)]

- remove {name <>}

- show [name <>]

NOTE: See IPSec chapter for IPSec configuration

IPSec-VPN Transport mode Commands

Command	Description
application connect	Access the ACE mode
vpn ipsec tunnel	Enter the tunnel configuration
Create	**Name**: tunnel name. mandatory field. String, 2-16 chars. Special characters allowed except !. **Address-prefix**: an IPv4 address for the tunnel local end point <A.B.C.D/M>. mandatory field. **lower-layer-dev**: a local ACE interface which is used as the network uplink. May be the cellular interface ppp0 or eth1.<vlan id>. Cellular may be used only at the spoke and only if a static, routable IP is provided by the ISP to the SIM. mandatory field. The interface must be pre-configured before creating the tunnel. **remote-address**: the network IP address of the remote side of the tunnel. mandatory field. **mtu**: set mtu for the tunnel 128-1500. Default 1418. **ttl**: set ttl for the tunnel 0-255. Default 64. **tos**: set type of service for the tunnel 0-255. Default is 'inherint' which sets the tunnel header to use the tos value of the encapsulated packet.
remove	Delete a tunnel. **Name**: tunnel name.
show	Show the tunnels configuration. **Name**: tunnel name. optional field IPSec-VPN Tunnel mode Commands Hierarchy

NOTE: See IPSec chapter for IPSec configuration

IPSec

Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and/or encrypting each IP packet of a communication session. The IPSec protocol suite includes the modules described in this chapter.

Applications

IPSec should be configured when a VPN is used :

1. DM-VPN: IPSec is mandatory.
2. IPSec-VPN: IPSec is mandatory.
3. L2-VPN: IPSec Mandatory when the VPN is established over the public network and /or when security is required.

Authentication Header (AH)

The IP Authentication Header (AH) is used to provide connectionless integrity and data origin authentication for IP datagrams.

» Supported mode per IKE phase 2. (transport ,tunnel)

» No specific configuration is available for AH. Authentication and encryption are implemented for ESP

Encapsulating Security Payload (ESP)

ESP provides origin authenticity, integrity and confidentiality protection of IP packets.

» Supported exchange mode per IKE phase 1. (main ,aggressive)
» Supported mode per IKE phase 2. (transport ,tunnel)
» Origin Authentication supported by IKE phase 1 and phase 2 HASH Cryptographic.
» Encryption supported by IKE phase 1 and phase 2 algorithms.

Security Associations

A Security Association (SA) is a relationship between two or more entities that describes how the entities will utilize security services to communicate securely. These entities are the VPN Hubs and Spokes.

This relationship is represented by a set of information that can be considered a contract between the entities. The information must be agreed upon and shared between all the entities.

ISAKMP provides the protocol exchanges to establish a security association between negotiating entities followed by the establishment of a security association by these negotiating entities in behalf of ESP/AH.

ISAKMP

ISAKMP provides a framework for a agreeing to the format of SA attributes, and for negotiating, modifying, and deleting SAs.

First, an initial protocol exchange allows a basic set of security attributes to be agreed upon. This basic set provides protection for subsequent ISAKMP exchanges. It also indicates the authentication method and key exchange that will be performed as part of the ISAKMP protocol. After the basic set of security attributes has been agreed upon, initial identity authenticated, and required keys generated, the established SA can be used for the protection of the VPN tunnels.

ISAKMP implementations guards against denial of service, replay / reflection and man-in-the-middle. This is important because these are the types of attacks that are targeted against protocols.

As mentioned, A security association (SA) is a set of policy and key(s) used to protect information. The ISAKMP SA is the shared policy and key used by the negotiating peers in this protocol to protect their communication.

ISAKMP uses the Internet Key Exchange (IKEv1)for the authentication and encryption establishment.

Sources: RFC 4109, 2408, 2631, 2412, racoon5.

IKE

Internet Key Exchange (IKE) negotiates the IPSec security associations (SAs). This process requires that the IPSec systems first authenticate themselves to each other and establish ISAKMP (IKE) shared keys.

Phase 2 is where Security Associations are negotiated on behalf of The VPN GRE services.

ISAKMP Phase 1

Phase 1 is where the two ISAKMP VPN peers establish a secure, authenticated channel with which to communicate. This is called the ISAKMP Security Association (SA) or IKE Security Association.

The authentication is supported with Pre-Shared Keys or Digital Signatures (X.509)

Diffie and Hellman

Diffie and Hellman describe a means for two parties to agree upon a shared secret. This secret may then be converted into cryptographic keying material for other (symmetric) algorithms.

Diffie-Hellman key agreement requires that both the sender and recipient of a message have key pairs.

The private key of each member is never sent over the insecure channel.

The public key is generated from the private key by each member and is the one sent over the insecure channel.

By combining one's private key and the other party's public key, both parties can compute the same shared secret number.

This number can then be converted into cryptographic keying material. That keying material is typically used as a key-encryption key (KEK) to encrypt the VPN GRE traffic. This key is kept secret and never exchanged over the insecure channel.

The D-H groups are identified by the length of the keys in bits. The larger the key (higher group id)the higher is the security but as well the resources required are higher and the user should consider performance degradation.

The D-H exchange can be authenticated with RSA signatures or pre-shared keys.

The exchange modes are "Main Mode" and "Aggressive Mode" and are accomplished at the phase 1.

Authentication

Pre-shared Key (PSK)

A PSK is an option for the IKE phase 1 authentication.

The encryption, hash, and authentication algorithm for use with a pre-shared key are a part of the state information distributed with the key itself.

Each VPN end point (Hubs, Spokes) must have a unique ID and a common shared key known to the remote VPN partner. Together these form the station PSK.

When a pre-shared key is used to generate an authentication payload, the certification authority is "None", the Authentication Type is "Preshared", and the payload contains the ID, encoded as two 64-bit quantities, and the result of applying the pseudorandom hash function to the message body with the KEY forming the key for the function

The PSK can be set as one of two forms:

1. IP address form A.B.C.D.
    a. Allowed in bot Main and Aggressive IKE modes
    b. The PSK of all members should be taken as their VPN network IP address.
2. Fully qualified domain name (FQDN).
    a. Allowed only when Aggressive IKE mode is used.

Below is an example of PSK configuration

1. Detail the preshared IDs of the VPN members and specify the id of local unit

```
RLGE2FE16R#application connect
ipsec isakmp update authentication-method pre _ shared _ key
ipsec preshared create id SA.ComNet.com key secretkey
ipsec preshared create id SB.ComNet.com key secretkey
ipsec isakmp update my-id SA.ComNet.com
ipsec policy create protocol gre
ipsec enable
```

```
[/] ipsec show global-defs
IPSec general defs
+-------------------------------+-----------------+
|           Parameter           |      Value      |
+===============================+=================+
| Admin Status                  |     enabled     |
+-------------------------------+-----------------+
| My ID                         |  SA.comnet.net  |
+-------------------------------+-----------------+
| Authentication method         |       PSK       |
+-------------------------------+-----------------+
| RSA Name                      |       N/A       |
+-------------------------------+-----------------+
| Log Level                     |      info       |
+-------------------------------+-----------------+
| DPD delay                     |        5        |
+-------------------------------+-----------------+
| DPD retry                     |        5        |
+-------------------------------+-----------------+
| DPD max fail                  |        5        |
+-------------------------------+-----------------+
| phase1 IKE mode               |   aggressive    |
+-------------------------------+-----------------+
| phase1 encryption algo        |     aes 128     |
+-------------------------------+-----------------+
| phase1 hash algo              |      sha1       |
+-------------------------------+-----------------+
| phase1 lifetime               |      86400      |
+-------------------------------+-----------------+
| Diffie Hellman group          |    modp1024     |
+-------------------------------+-----------------+
| phase2 encryption algo        |      3des       |
+-------------------------------+-----------------+
| phase2 auth algo              |       md5       |
+-------------------------------+-----------------+
| phase2 lifetime               |      86400      |
+-------------------------------+-----------------+
| PFS group                     |    modp1024     |
+-------------------------------+-----------------+

[ipsec/] show preshared
IPSec preshared keys
+-----------------+-----------------+
|   identifier    |       key       |
+=================+=================+
|   SA.comnet.net | ********** |
+-----------------+-----------------+
|   SA.comnet.net | ********** |
+-----------------+-----------------+
Total: 2

[ipsec/] policy show
IPSec policy database
+----------------+----------------+-------+-------+
|      from      |       to       | proto | notes |
+================+================+=======+=======+
| 0.0.0.0/0[any] | 0.0.0.0/0[any] |  gre  |       |
+----------------+----------------+-------+-------+
```

The above configuration example will result in following show output

RSA Signatures (X.509)

Uses a digital certificate authenticated by an RSA signature.

The user is required to generate certificates from a trusted source and to import these to the VPN parties (Hubs ,Spokes).

Two files are required, one is the certificate itself and the other is the key.

The files should have extensions of .crt and .key.

Below is a screenshot of such 2 files placed on a PC with tftp client and CLI example of importing them.

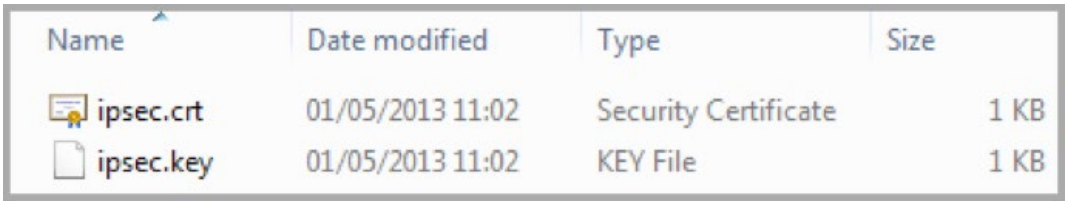


Figure 8 The certificate files

1. Import the key file

```
RLGE2FE16R# rsA-signature import tftp://172.17.203.31/ipsec.key
 RSA signature file (ipsec.key) imported successfully
```

2. Import the certificate file

```
RLGE2FE16R# rsA-signature import tftp://172.17.203.31/ipsec.crt
 RSA signature file (ipsec.crt) imported successfully
Validate successful import
```

```
RLGE2FE16R# show rsA-signature list
ipsec.crt
ipsec.key
```

3. Activate the certificate

```
application connect
ipsec rsa-signature activate crt-file ipsec.crt key-file ipsec.key rsa-sig-name test _ 1
```

4. Update the ipsec isakmp to use the certificate instead of the PSK

```
ipsec isakmp update authentication-method rsasig
```

NOTE: The ipsec isakmp property "my id" is not of importance when using certificates as the authentication method

The above configuration example will result in following show output

```
[/] ipsec show global-defs
IPSec general defs
+--------------------------------+------------+
|           Parameter            |   Value    |
+================================+============+
| Admin Status                   |  enabled   |
+--------------------------------+------------+
| My ID                          |    N/A     |
+--------------------------------+------------+
| Authentication method          |  RSA-SIG   |
+--------------------------------+------------+
| RSA Name                       |   test1    |
+--------------------------------+------------+
| Log Level                      |    info    |
+--------------------------------+------------+
| DPD delay                      |     5      |
+--------------------------------+------------+
| DPD retry                      |     5      |
+--------------------------------+------------+
| DPD max fail                   |     5      |
+--------------------------------+------------+
| phase1 IKE mode                | aggressive |
+--------------------------------+------------+
| phase1 encryption algo         |  aes 128   |
+--------------------------------+------------+
| phase1 hash algo               |    sha1    |
+--------------------------------+------------+
| phase1 lifetime                |   86400    |
+--------------------------------+------------+
| Diffie Hellman group           |  modp1024  |
+--------------------------------+------------+
| phase2 encryption algo         |    3des    |
+--------------------------------+------------+
| phase2 auth algo               |    md5     |
+--------------------------------+------------+
| phase2 lifetime                |   86400    |
+--------------------------------+------------+
| PFS group                      |  modp1024  |
+--------------------------------+------------+
```

Exchange Modes

Main

Main mode is the more secure option for phase1 as it involves the identity protection.

Session flow:

- Session begins with the initiator sending a proposal to the responder describing what encryption and authentication protocols are supported, the life time of the keys, and if phase 2 perfect forward secrecy should be implemented. The proposal may contain several offerings. The responder chooses from the offerings and replies to the initiator.
- The next exchange passes Diffie-Hellman public keys and other data. All further negotiation is encrypted within the IKE SA.
- The third exchange authenticates the ISAKMP session. Once the IKE SA is established, IPSec negotiation (Quick Mode) begins.

In applications at which the IP addresses used for the VPN network are not static (for example a cellular spoke retrieving dynamic IP from the ISP over its PPP interface) the Main mode of IKE is not applicable.

Pre-shared key: When used in main mode the PSK must be in the form of IP address and use the VPN network addresses of the parties.

NOTE: In Applications where the VPN is used over a cellular link, the IKE mode to be used is Aggressive. Main mode is not applicable.

Aggressive

In this mode the negotiation is quicker as the session is completed in only 3 messages. The disadvantage is in that the identity of the peers is not protected.

The first two messages negotiate policy, exchange Diffie-Hellman public values and ancillary data necessary for the exchange, and identities. In addition the second message authenticates the responder. The third message authenticates the initiator and provides a proof of participation in the exchange.

- The initiator send a request with all required SA information.
- The responder replies with authentication and its ID.
- The initiator authenticates the session in the follow-up message.

Pre-shared key : When used in Aggressive mode the PSK may be either in the form of IP address or fqdn. The PSK doesn't have to be the actual IP addresses of the VPN network interfaces as it considers the enter value as text (in the format of IP) and not as a valid IP address.

NOTE: In Applications where the VPN is used over a cellular link, the IKE mode to be used is Aggressive. The PSK may be of IP format or fqdn

Settings structure

- » Authentication method (PSK ,X.509)
- » Diffie–Hellman key exchange group (a.k.a OAKLY groups)
- » IKE exchange mode
  - › Main
  - › Aggressive
- » Encryption algorithm
  - › Advanced Encryption Standard (AES)
    - ·128 and 256 key size options
    - ·symmetric algorithm
  - › Triple Data Encryption Algorithm (3DES)
    - ·comprises of three DES keys, K1, K2 and K3, each of 56 bits
- » Authentication s HASH algorithms
    - ·Secure Hash Algorithm SHA-1 (160 bit)
    - ·Secure Hash Algorithm SHA-2 (256 |512 bit)
    - ·Message Digest (MD5) (128 bit)
- » Life time and Dead Peer Discovery settings

ISAKMP Phase 2

At this phase the negotiation of SA to secure the VPN GRE data using IPSec is made.

Modes

The common mode to use between end stations supporting IPSec (the VPN parties) is called Transport mode. This is the mode supported by ComNet.

Perfect forward secrecy (PFS)

The PFS is a part of the key agreement session and has a purpose to ensure that a session key derived from a set of long-term public and private keys will not be compromised if one of the (long-term) private keys is compromised in the future. The VPN (GRE, IPSEC) sessions can negotiate new keys for every communication and if a key is compromised only the specific session it protected will be revealed.

The PFS uses as well the D-H groups but independently from phase 1.

Settings structure

- » Supported mode
  - › Transport (yes)
  - › Tunnel (no)

- » Authentication s HASH algorithms
  - › Secure Hash Algorithm SHA-1 (160 bit)
  - › Secure Hash Algorithm SHA-2 (256 |512 bit)
  - › Message Digest (MD5) (128 bit)
- » Perfect Forward Secrecy type (PFS)
- » Encryption algorithm
  - › Advanced Encryption Standard (AES)
    - ·128 and 256 key size options
    - ·symmetric algorithm
  - › Triple Data Encryption Algorithm (3DES)
    - ·comprises of three DES keys, K1, K2 and K3, each of 56 bits
- » Life time
  - › Soft – hard coded. At this threshold value the IKE starts a new phase 2 exchange.
  - › Hard- SA which has exceeded this threshold value will be discarded.

IPSec Command Association

Below are detailed the configuration fields of the IPSec in their respective association to the ISAKMP structure.

Highlighted in blue are the CLI names of the configurable fields.

Enable IPSec

{enable |disable}

Settings

Log level (log-level)

Dead Peer Discovery

delay (dpd-delay)

max failure (dpd-maxfail)

max retires (dpd-retry)

flush Security Association (flush-sa proto)

id-type (id-type)

soft timer (soft-lifetime)

Phase 1

Authentication method {pre_shared_key | rsasig}

Diffie–Hellman key exchange Group (dh-group)

Internet Key Exchange mode (ike-phase1-mode)

Encryption Algorithm (phase1-encryption-algo)

Hash Algorithm (phase1-hash-algo)

Life Time (phase1-lifetime)

Phase 2

Perfect Forward Secrecy (pfs-group)

Encryption Algorithm (phase2-encryption-algo)

Authentication Algorithm (phase2-auth-algo)

Life Time (phase2-lifetime)

IPSec Policy

Name (notes)

Source address (src-address-prefix)

Destination address (dst-address-prefix)

Source protocol port (src-port)

Destination protocol port (src-port)

Protocol (protocol)

Preshared Keys

- Key : (key)
- Own PSK id : (id)
- Partner PSK id : (id)
- Partner PSK id : (id)

Certificates X.509

Import crt file (flush-sa proto)

Import key file (rsA-signature import)

Activate certificate file (rsa-signature activate)

Certificate name (rsa-sig-name)

IPSec Commands Hierarchy

+ root

+ application connect

+ ipsec {enable | disable}

- flush-sa proto {ah | esp | ipsec | isakmp}

- rsa-signature activate {crt-file <file name> | key-file <file name> |rsa-sig-name <name>}

+ isakmp update

- authentication-method {pre_shared_key | rsasig}

- dh-group <none | modp768 | modp1024 | modp1536 | modp2048 | modp3072 |modp4096 | modp6144>

- pfs-group < none | modp768 | modp1024 | modp1536 | modp2048 | modp3072 |modp4096 | modp6144 |modp8192>

- dpd-delay <5,0-120> dpd-maxfail <5,2-20> dpd-retry <5,1-20>

- log-level <error |warning |notify |info |debug |debug2>

- my-id <>

- soft-lifetime <1-99>

- id-type {none| fqdn| asn1dn}

- ike-phase1-mode <aggressive |main> phase1-encryption-algo <3des | aes-128 | aes-256> phase1-hash-algo <md5 |sha1 |sha256 |sha512>

- phase2-auth-algo < hmac_md5 | hmac_sha1 | hmac_sha256 | hmac_sha512> phase2-encryption-algo <3des |aes-128 |aes-256>

- phase1-lifetime <86400,(180-946080000)> phase2-lifetime <86400,(180-946080000)>

- rsa-sig-name <name> rsa-ca-cert <name.crt>

+ policy {create | remove | show} mode (transport,<transport| tunnel>

For both transort and tunnel modes
{src-address-prefix <A.B.C.D/E>} {dst-address-prefix < A.B.C.D/E >}

[src-port <>] [dst-port <> [notes <text>]
[protocol (any,<gre |tcp |udp| any| icmp| ipencap| modbus_tcp|
iec104| dnp3>)]

For tunnel mode
{endpoint-dst-address < A.B.C.D >} [endpoint-dst-port <0-999,999>]
[endpoint-src-address < A.B.C.D >] [endpoint-src-port <0-999,999>]

+ preshared {create | remove} key <> id <>

+ show

- log {grep| num-of-lines }

- global-defs

- policy

- preshared

- rsa-signature-file

- sa [proto {ah | esp | ipsec | isakmp}]

IPSec X.509 Commands Hierarchy

X.509 is only available in the Enhanced Security product configuration.

IPsec Commands

Command	Description
application connect	Enter the industrial application menu
certificates	Show the files available
local	
export	This option is not supported at current release
import	certificate-file-pem: the certificate name and extension at the server. name: name for the certificate with which it will be saved locally at the unit. Mandatory field. tftp-address: IPv4 address of the server holding the certificate. comment: optional descriptive test. private-key-pem: server key.

Command	Description
generate	**Name**: use a unique name to identify the certificate request. Alpha numeric, special characters supported except the sign !. mandatory field. **Comments**: optional descriptive test. No spaces allowed. **Common-name**: add a common name typically used to identify the host. **Country (region)**: the country where the unit is installed. **State(province)**: the state where the unit is installed. **Locality(city)**: the city where the unit is installed. **Organization**: formal name of the company you are working at. **Email**: your email address. **organization-unit**: name of the department you work at. **auto-regenerate-days:** 0-14. Applicable in 'enrollment-method' of 'online-scep' only. Send regenerate request x days prior to the certificate expiration date. default=0 (no automatic request). **auto-regenerate-days-warning**: 0-14. Applicable in 'enrollment-method' of 'online-scep' only. Send a warning x days prior to the certificate expiration date. default=0 (no automatic message). **scep-url:** url address of SCEP server. For example http://comnet.net **scep-password-string**: authentication password at server. key-size: 1024| 1536| 2048. Default 2048. Large key size enhances security but is slower to generate. enrollment-method: file-based| online-scep. Default online-scep. 'fiel based' is not supported at this version.
remove	name: the name of the certificate with which it was saved when generated/ imported.
show	name: the name of the certificate with which it was generated/ imported
update	**name**: the name of the certificate with which it was generated/ imported **comment**: ption descriptive test. **auto-regenerate-days**: 0-14. Applicable in 'enrollment-method' of 'online-scep' only. Send regenerate request x days prior to the certificate expiration date. default=0 (no automatic request). **auto-regenerate-days-warning**: 0-14. Applicable in 'enrollment-method' of 'online-scep' only. Send a warning x days prior to the certificate expiration date. default=0 (no automatic message).
ca	
export	certificate-file-pem: export the file to the server. Applicable when using 'file based' only. This option is not supported at current version. name: the name of the certificate with which it was saved when generated/ imported. tftp-address: IPv4 address of the target server.
import	certificate-file-pem: the certificate name and extension at the server. Applicable when using 'file based' only. name: name for the certificate with which it will be saved locally at the unit. Mandatory field. tftp-address: Pv4 address of the server holding the certificate. comment: **http-url**: url address of SCEP server. **import-method**: ad-hoc operation using 'file based' (tftp) or automatically with SCEP protocol using 'online-scep' option. **auto-update-days**: 0-14. Applicable in 'enrollment-method' of 'online-scep' only. Send update request x days prior to the certificate expiration date. default=0 (no automatic request). **auto-update-days-warning**: 0-14. Applicable in 'enrollment-method' of 'online-scep' only. Send a warning x days prior to the certificate expiration date. default=0 (no automatic message).
remove	name: the name of the certificate with which it was saved when generated/ imported.
show	name: the name of the certificate with which it was saved when generated/ imported.

Command	Description
update	name: the name of the certificate with which it was saved when generated/ imported comment: optional descriptive test. **auto-update-days**: 0-14. Applicable in 'enrollment-method' of 'online-scep' only. Send update request x days prior to the certificate expiration date. default=0 (no automatic request). **auto-update-days-warning**: 0-14. Applicable in 'enrollment-method' of 'online-scep' only. Send a warning x days prior to the certificate expiration date. default=0 (no automatic message).
crl	
export	This option is not supported at current release
import	certificate-file-pem: the certificate name and extension at the server. name: name for the certificate with which it will be saved locally at the unit. Mandatory field. tftp-address: IPv4 address of the server holding the certificate. **comment**: optional descriptive test. ca-name: **http-url**: url address of the server managing the automatic crl updates. **import-method**: ad-hoc operation using 'file based' (tftp) or automatically with SCEP protocol using 'online-scep' option. **update-interval-sec**: time interval for the unit to check for an updated crl.
remove	name: the name of the certificate with which it was saved when generated/ imported.
show	name: the name of the certificate with which it was saved when generated/ imported.
update	name: the name of the certificate with which it was saved when generated/ imported. comment: optional descriptive test. update-interval-sec: time interval for the unit to check for an updated crl.
rsA-signature import	Import the X.509 certificate file and key file to the application from a connected USB drive or tftp/ sftp servers. These files are mandatory for IPSec to encrypt using X.509 certificates. These files are not required if IPSec is used with preshared keys.
show rsA-signature list	Show the files available
Application connect	Enter the industrial application menu
IPsec	Enter the IPsec configuration mode
Enable | disable	Default is disable
rsa-signature activate	Activation of the available certificate and key files. Crt-file ; name of the certificate file. Key-file : name of the key file. rsa-sig-name : user configurable name for the signature.
isakmp update	
authentication-method	pre_shared_key : preshared keys will be used. (default) Rsasig : X.509 certificates will be used.
dh-group	Diffie–Hellman key exchange Group. Relates to phase 1. Determines the strength of the key used in the key exchange process. The higher the group number, the stronger the key and security increases. Options : none modp768 (DH group 1) modp1024 (default) (DH group 2) modp1536 (DH group 3 and 5) modp2048 (DH group 14) modp3072 (DH group 15) modp4096 (DH group 16) modp6144 (DH group 17) modp8192 (DH group 18)

Command	Description
pfs-group	Perfect Forward Secrecy type. Relates to phase 2. Determines the strength of the key used in the key exchange process. The higher the group number, the stronger the key and security increases. Options: none modp768 modp1024 (default) modp1536 modp2048 modp3072 modp4096 modp6144 modp8192
dpd-delay	Dead Peer Discovery delay .defines the interval between following keep alive messages. Permissible range : 0-120 (default is 5)
dpd-maxfail	Dead Peer Discovery max attempts to determine failure. Permissible range :2-20 (default is 5)
dpd-retry	Dead Peer Discovery max retry attempts. A retry is initiated after a failure at "dpd-maxfail". Permissible range : 1-20 (default is 5)
log-level	Syslog warnings levels to be logged. error warning notify info (default) debug debug2
my-id	Own pre-shared id. Dependent on "id-type" set ,my-id can be in either domain name format or ipv4 format. If "id-type" is set to "none": No need to set value in "my-id" as it will automatically use a valid IP address. If "id-type" is set to "fqdn": "my-id" should be set with a domain name format. for example: Spoke.ComNet.com
Id-type	Set the type of form used for the IPSec local id. None: the units own pre-shared id will be the default IP interface. Address : this option is not supported in current version. fqdn : the units own pre-shared id will be in a domain name format. For example spoke.ComNet.com default: none
ike-phase1-mode	Internet Key Exchange mode type use for Phase 1. Aggressive (default) main
phase1-encryption-algo	Encryption Algorithm used for phase 1. 3des aes-128 (default) aes-256
phase1-hash-algo	Hash Algorithm used for phase 1. md5 sha1 (default) sha256 sha512
phase1-lifetime	The lifetime of the key generated between the stations. 180-946080000 sec. Default is 86400

Command	Description
phase2-auth-algo	Authentication Algorithm for phase 2. hmac_md5 (default) hmac_sha1 hmac_sha256 hmac_sha512
phase2-encryption-algo	Encryption Algorithm for phase 2. 3des (default) aes-128 aes-256
Phase2-lifetime	The lifetime of the key generated between the stations. 180-946080000 sec. Default is 86400
soft-lifetime	When a dynamic IPSec SA is created, two types of lifetimes are used: hard and soft. The hard lifetime specifies the lifetime of the SA. The soft lifetime, which is derived from the hard lifetime, informs the IPSec key management system that the SA is about to expire. This allows the key management system to negotiate a new SA before the hard lifetime expires. Permissible values are 1-99 and represents percentage. soft lifetime = <1-99>*hard lifetime /100
rsa-sig-name	The name set by the user for the signature
Policy create	Configure the policy to determine the type of traffic to encrypt mode: choose mode of operation transport- this is the default mode. Supported for route based VPNs. tunnel- policy based vpn. Supported only for IPSec-VPN. src-ip : A.B.C.D/x format. The ACE IP interface which is the local end of the tunnel. dst-ip : A.B.C.D/x format. The IP interface which is the remote end of the tunnel. src-port : source port number at the packet originated from the 'src-ip'. dst-port : destination port number at the packet originated from the 'src-ip'. protocol : the type of protocol to encrypt. For example any, TCP ,UDP,GRE, icmp, ipencap. Default-'any'. When using IPSec-VPN, the use of 'ipencap' is mandatory at the policy. endpoint-dst-address: applicable in IPSEC-VPN at 'policy based' mode only. A.B.C.D IPv4 format. Encryption will be made for packets which are sent with this destination IP address. endpoint-src-address: applicable in IPSEC-VPN at 'policy based' mode only. A.B.C.D IPv4 format. Encryption will be made for packets which are sent with this source IP address. endpoint-dst-port: applicable in IPSEC-VPN at 'policy based' mode only. Numeriv value <0-999,999>. Encryption will be made for packets which are sent with this destination port number. endpoint-src-port: applicable in IPSEC-VPN at 'policy based' mode only. Numeric value <0-999,999>. Encryption will be made for packets which are sent with this source port number.
Preshared {create | remove}	Configuration of pre shared identifiers for local node and all remote IPsec nodes. ID: unique identifier for the IPSec participant node Can be in either domain name format or ipv4 format.) Key: pre-shared key which should be common for all nodes participating. text, numerical or combination string. notes : name of the policy
Show	Show IPsec

IPSec defaults

```
/] ipsec show global-defs
PSec general defs
---------------------------------+----------------
           Parameter             |      Value
=================================+================
 Admin Status                    |    disabled
---------------------------------+----------------
 ID Type                         |      none
---------------------------------+----------------
 My ID                           |      N/A
---------------------------------+----------------
 Authentication method           | pre_shared_key
---------------------------------+----------------
 RSA Name                        |      N/A
---------------------------------+----------------
 Log Level                       |      info
---------------------------------+----------------
 DPD delay                       |       5
---------------------------------+----------------
 DPD retry                       |       5
---------------------------------+----------------
 DPD max fail                    |       5
---------------------------------+----------------
 phase1 IKE mode                 |   aggressive
---------------------------------+----------------
 phase1 encryption algo          |     aes128
---------------------------------+----------------
 phase1 hash algo                |      sha1
---------------------------------+----------------
 phase1 lifetime                 |     86400
---------------------------------+----------------
 Diffie Hellman group            |    modp1024
---------------------------------+----------------
 phase2 encryption algo          |      3des
---------------------------------+----------------
 phase2 auth algo                |    hmac_md5
---------------------------------+----------------
 phase2 lifetime                 |     86400
---------------------------------+----------------
 PFS group                       |    modp1024
---------------------------------+----------------
```

Cellular Modem

Cellular coverage is ubiquitous and has become a proven and reliable medium. Hence an integrated cellular modem interface provides a measurable benefit, especially in applications where small sites require a backup traffic path on top of the physical line or at remote or temporary locations where a physical line is not available.

The RLGE2FE16R supports options for GPRS/UMTS or LTE modem.

The modem provides a key solution for connectivity to remote sites.

The modem supports dual SIM cards for redundancy and backup between two Internet Service Providers.

LTE Modem

Two ordering options are available for the LTE modem, for European type frequencies and bands and for the North American ones. In both cases the modem supports LTE (in corresponding bands) and GSM/GPRS/EDGE. The following table describes the frequencies and bands supported per ordering option.

Topic	Type	Frequency	Band	N.America	Europe
AIR INTERFACE	LTE			Y	Y
AIR INTERFACE	HSPA+			Y	Y
AIR INTERFACE	GSM			Y	Y
AIR INTERFACE	GPRS			Y	Y
AIR INTERFACE	EDGE			Y	N
LTE FREQUENCY BANDS	LTE	2100	1	N	Y
		1900	2	Y	N
		1800	3	N	Y
		AWS	4	Y	N
		850	5	Y	N
		2600	7	N	Y
		900	8	N	Y
		700	13	Y	N
		700	17	Y	N
		800	20	N	Y
		1900	25	Y	N
		2600	38	N	N
		2300	40	N	N
		700	-	N	N

GPRS/UMTS Modem

Following modes and spectrums are supported:

- » 3G UMTS– HSDPA. cat 5/6
  - › Triple band : 2100/1900/900 MHz
  - › Triple band : 2100/1900/850 MHz
- » 2G GSM- EDGE / GPRS. class 12
  - › Quad band :850/900/1800/1900 MHz

The maximum data throughput is determined according to the cellular service and might be different for down-stream and up-stream.

Topologies supported:

Point to Point – single Spoke to a single Hub.

Multi Point to Point – multiple spokes to a single Hub.

Extensive QOS capabilities (IEEE 802.1P VPT) are planned to be supported for prioritizing traffic to through cellular link.

NAT support using the IPsec encryption enables the spoke the important availability also when retrieving private IP from the ISP.

Hardware

Hub – a ComNet switch with application card installed and configured, or a RLGE2FE16R switch. The Hub requires a fixed connection to the internet with a static, public IP address assigned to its application interface.

CAUTION: Before taking a SIM card out of its port the cellular application must be switched off.

Spoke – a ComNet RLGE2FE16R product variant ordered with cellular interface.

Cellular modem as a USB device

All cellular modems in the ComNet RLGE2FE16R units are USB modems. Current version allows operation of a single USB device. By default in all RLGE2FE16RS models equipped with any cellular modem, the selected device is the cellular modem. In order to allow usage of the exernal USB device please refer to the commands below.

Cellular Commands Hierarchy

+ root

+ application connect

    + usb

        + select

            + device {storage|modem}

Cellular Commands Description

Command	Description
Application connect	Enter the industrial application menu
usb select device	Select the active USB device: **storage**: external USB **modem**: cellular modem

Interface Name

In applications the addressing of configuration to the cellular interface will be by its name.

A cellular interface established with a cellular modem is referenced as ppp0.

Examples of addressing the cellular modem via its name:

DM-VPN

```
vpn gre tunnel create address-prefix 10.10.10.20/24 lower-layer-dev ppp0 name mgre1 key
10.0.0.0 admin-status enable
```

NAT

```
router nat dynamic create interface-name ppp0 description natcellular
```

Method of operation

At the spoke side, a simple configuration of the cellular modem is enough to have the spoke approach the ISP to retrieve an IP address using known link protocol PPP. Authentication versus the ISP will be made using the SIM cards and PAP protocol. Dependent on the ISP service this IP might be private behind NAT or public.

The Cellular connection must be accompanied with a VPN setup to establish a service towards a supporting Hub. Modes of VPN supported:

1. L2 GRE VPN

2. L3 DM-VPN

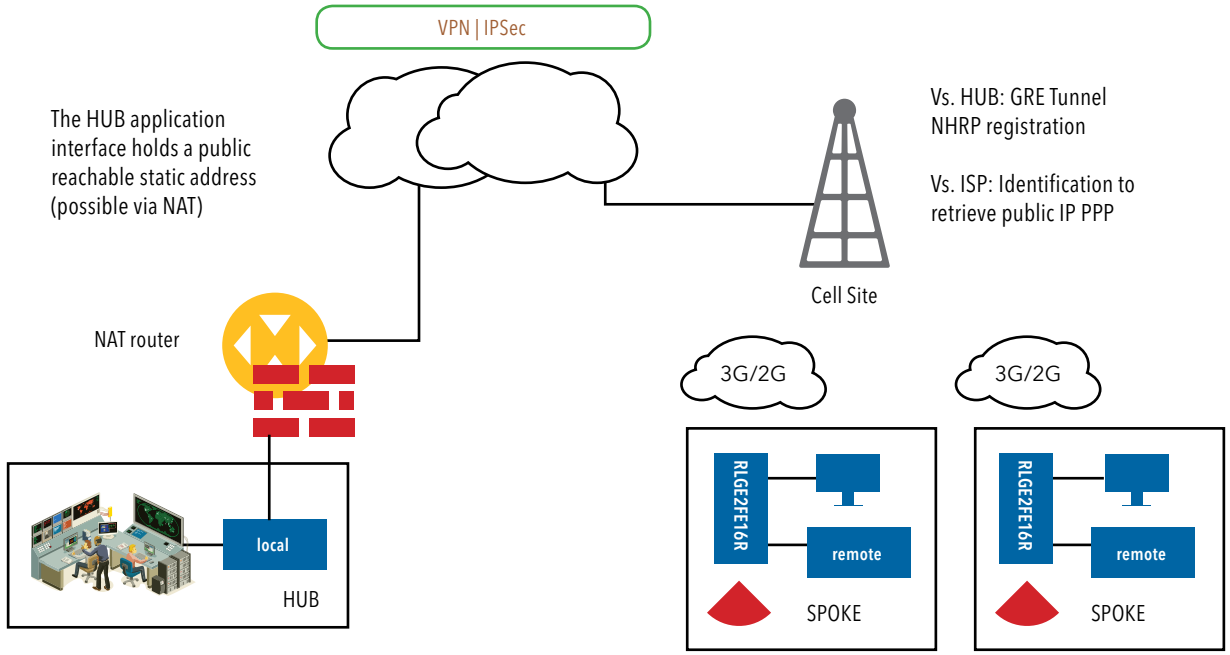
L3 IPSec VPN

Once holding an IP address retrieved from the ISP at its PPP interface, and with a VPN configured, the Spoke will initiate NHRP request for registration towards the Hub.

The Hub must be a well know participant in the network by holding a static address. The IP assigned to the hub must be routable with the IPs the cellular ISP will allocate to the cellular Spokes. If the network cloud is a public one (as www) then the Hub must have a PUBLIC, STATIC IP assigned to it.

The Hub will listen on its interface to NHRP requests from the spoke and will allow the VPN establishment dependent on the authentication.

A Hub must have a fixed connection to the network, it may not be connected with the cellular modem as a spoke.



SIM card state

The modem can host 2 different SIMs. The SIMs may be of the same vendor or not.

At a given moment a connection can be available via a single SIM.

Redundancy can be achieved using RSSI measurements and echo tests to determine which SIM is preferred to be used.

The user can decide whether to select a specific SIM as preferred for default connection.

Each SIM can be individually configured and enabled /disabled.

Dependent on configuration and availability, the status of a SIM may be one of the following at the modem:

- Unknown – SIM is either:
  - Not available at the slot
  - Cellular modem is not enabled
  - Cellular modem in under refresh state
  - Unavailable due to modem malfunction
- Disabled – The modem is enabled but the SIM was not configured.
- Ready – SIM is available and configured.
- Connecting – Modem is trying to retrieve IP from the ISP using the SIM
- Connected – the modem retrieved an IP address from the ISP with the selected SIM.
- Failed – failure to connect with the selected SIM.
- Connected as Secondary – Modem is connected with the alternative SIM, meaning not to the SIM originally chosen by the user as preferred.
- Connected as Alternative – modem is connected with the alternative SIM, due to a recognized failure in connecting to the preferred SIM.

SIM state example

Below is an example of SIMs admin state. SIM in slot 1 had been enabled while SIM in slot 2 is disabled.

The show command used is cellular wan show.

```
[/] cellular wan show
+----------+-----------+----------+-----------+-----------+----------------+-----+------------+---------+
| sim slot | sim admin | operator | apn name  | user name |    password    | pin |   radio    |  flow   |
|          |   status  |   name   |           |           |                |     |   access   | control |
|          |           |          |           |           |                |     | technology |         |
+==========+===========+==========+===========+===========+================+=====+============+=========+
|    1     |  enabled  | cellcom  | internetg |   guest   | ************** | N/A |    auto    |   YES   |
+----------+-----------+----------+-----------+-----------+----------------+-----+------------+---------+
|    2     | disabled  |   N/A    |    N/A    |    N/A    | ************** | N/A |    auto    |   YES   |
+----------+-----------+----------+-----------+-----------+----------------+-----+------------+---------+
```

SIM 1 is connected following the modem enable and the SIM properties configured.SIM 2 is configured an in READY state.

```
Application connect

cellular enable

cellular wan update admin-status enable apn-name internetg sim-slot 1 operator-name
cellcom user-name guest password guest


cellular wan update admin-status enable apn-name internet.pelephone.net.il sim-slot 2
operator-name pelephone user-name pcl@3g password pcl
```

```
[/] cellular show
cellular enabled
[/] cellular wan show
+----------+-----------+-----------+--------------------------+-----------+---------------+-----+------------+---------+
| sim slot | sim admin | operator  |         apn name         | user name |    password   | pin |   radio    |  flow   |
|          |   status  |    name   |                          |           |               |     |   access   | control |
|          |           |           |                          |           |               |     | technology |         |
+==========+===========+===========+==========================+===========+===============+=====+============+=========+
|    1     |  enabled  |  cellcom  |         internetg        |   guest   | ************* | N/A |    auto    |   YES   |
+----------+-----------+-----------+--------------------------+-----------+---------------+-----+------------+---------+
|    2     |  enabled  | pelephone | internet.pelephone.net.il |  pcl@3g   | ************* | N/A |    auto    |   YES   |
+----------+-----------+-----------+--------------------------+-----------+---------------+-----+------------+---------+
[/] cellular network show
+------+------------+-------------+---------+----------+---------+--------+-------+------------+
| slot |    oper    |    Last     | Changes | Failures |  Last   | Caveat | RSSI  | Last RSSI  |
|      |   status   | update(sec) |         |          | Failure |        | [dBm] | check(sec) |
+======+============+=============+=========+==========+=========+========+=======+============+
|  1   | CONNECTED! |     96      |   10    |    0     |   N/A   |   No   |  -67  |    132     |
+------+------------+-------------+---------+----------+---------+--------+-------+------------+
|  2   |   READY    |     117     |    5    |    0     |   N/A   |   No   |  -79  |    113     |
+------+------------+-------------+---------+----------+---------+--------+-------+------------+
```

The modem retrieved an IP from the ISP

```
[/] cellular connection show
+-----------+----------------+----------+----------+-----------+----------+
| interface |    local ip    |    tx    |    tx    |    rx     |    rx    |
|           |                |  packet  |  error   |  packets  |  error   |
+===========+================+==========+==========+===========+==========+
|   ppp0    | 46.210.197.173 |    6     |    0     |     5     |    0     |
+-----------+----------------+----------+----------+-----------+----------+
```

Backup and redundancy

Backup between ISP (SIM cards watchdog)

A properly configured SIM card along with a proper ISP service will be indicated by the modem as "ready" state.

If connected, the SIM card slot will be indicates as "connected".

A SIM card slot which is not occupied, not configured or set to "disable" will not be used as backup option.

A primary (preferred) SIM card can optionally be set manually by the user to connect to a preferred vendor as default. A default state is that both SIM cards are with equal privilege and so no preference is determined. If a preferred SIM is chosen:

- The system will use the preferred SIM for the GSM connection and will keep this link as long as the connection meets the conditions set at the watchdog.
- As long as the primary link hold a proper reliable connection, the secondary SIM remains in "ready" mode.
- Once the Primary does not meet the minimum watchdog tests criteria, the second SIM interface will be enabled as "ALTERNATIVE" and the system will establish a link with it.
- The modem will switch back form the "ALTERNATIVE" to the preferred SIM after time set at the configurable timers (assuming its in "ready state).

If no specific SIM is chosen as preferred:

- The modem will connect to the SIM with best RSSI.
- As long as the link hold a proper reliable connection, the second SIM remains in "ready" mode.
- Once the connection does not meet the minimum watchdog tests criteria, the second SIM interface will be enabled as "ALTERNATIVE" and the system will establish a link with it.
- The modem will not switch back form the "ALTERNATIVE" to the preferred SIM unless it will explicitly not meet the watchdog conditions.

The watchdog can be configured with several tests and criteria:

- Several remote destinations to send echo requests to.
- Average threshold for round trip echo replies towards a remote target.
- Percentage of lost echo requests towards a remote target.
- RSSI threshold.
- LCP echo test loss threshold towards the ISP
- Packet size of echo messages
- Timers and intervals

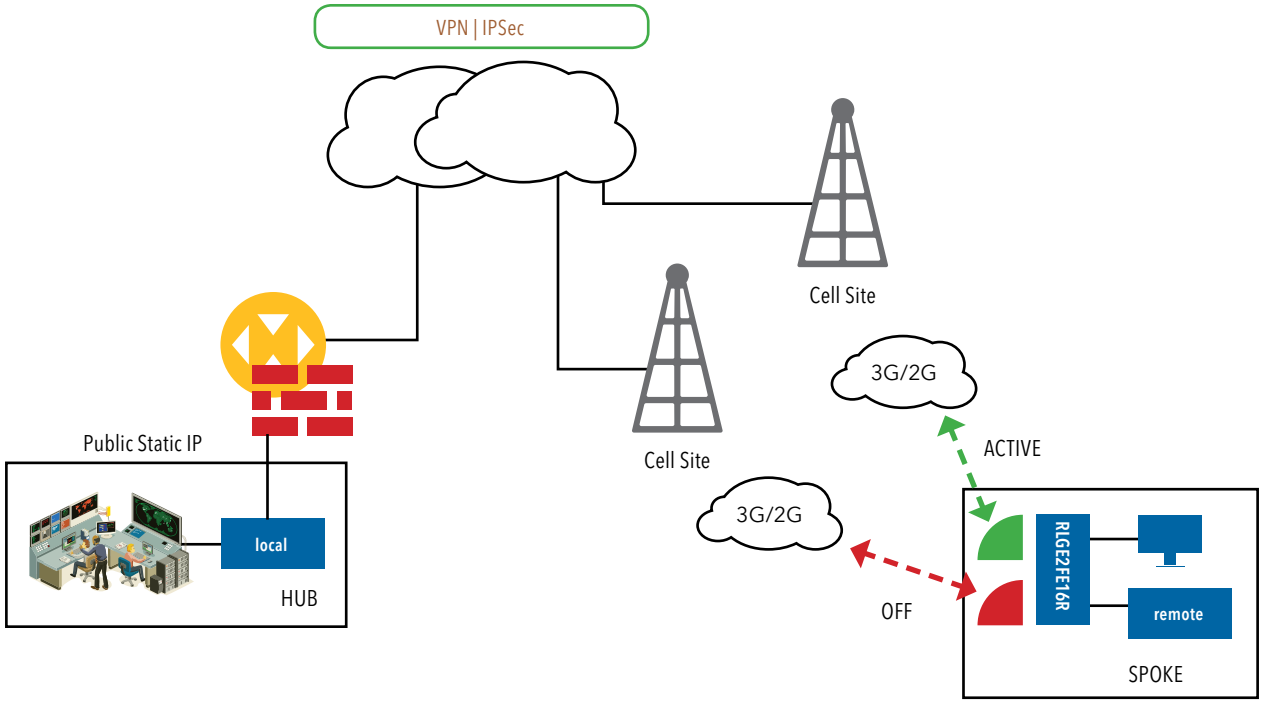


Figure 9 : Primary active

Backup between Interfaces (between Cellular or Physical interface)

A cellular link is by nature a high cost path and with a significant lower bandwidth then a physical channel. When the cellular link is to be used for backup to a physical link then resilient network protocols can determine the primary and backup paths.

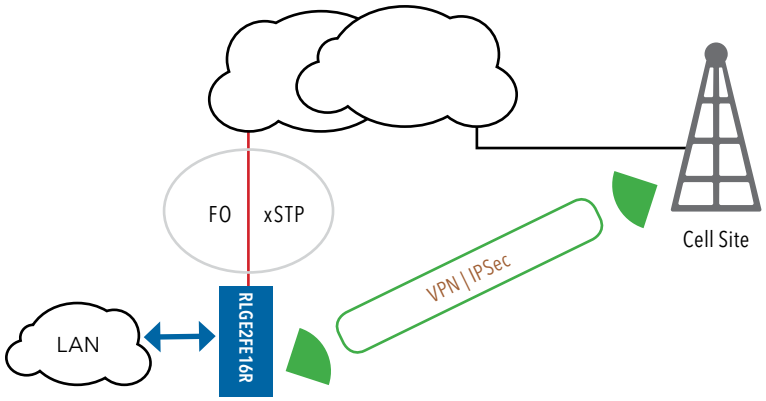


Figure 10 : L2 protection

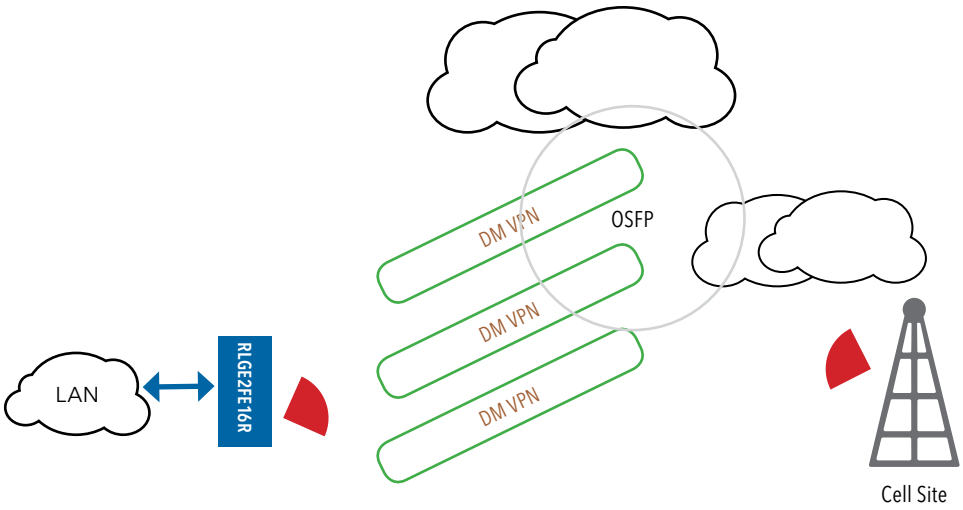


Figure 11 : L3 protection

Modem conditional reload

In case the modem is continuously unsuccessful in establishing a connection and retrieving an IP from the ISP, a reload can be trigger to the switch.

A configuration parameter "retry-threshold-reload" is available to be set between 0 (disabled) and 30, whereas values 1-30 represents the number of consecutives failures.

A typical flow is as follow:

» Once a SIM is in "CONNECTING…" and instead of reaching "CONNECTED" has reached "FAILED". Such attempt is approximately 2 minutes long (non configurable).

» The counter progresses with every such above condition and summarize for both SIMs together.

» The following states will reset the counter: "CONNECTED", "CONNECTED AS ALTERNATIVE","CONNECTED AS SECONDARY".

NOTE: The quality echo tests are applicable when the status of the SIM is "CONNECTED". At "connected" state, the "retry-threshold-reload" counter is cleared. This means the quality tests have no direct influence on this counter.

NOTE: In case of a single SIM card is used, the 'continuous-echo' test will result in action of 'cellular modem refresh' in case the test fails. If the modem is in 'connected' state but the echo test fails to meet the configured criteria (ping loss/ rtt..) the router will refresh the modem as attempt to recover.

Cellular Commands Hierarchy

+ root

+ application connect

  + Cellular

    + continuous-echo

    - {create | update} {name <>} {dest-ip-address <ip address>} [loss-threshold <50,10-99>] [num-of-requests <3,1-100>] [rtt-threshold < 5000msec(1,000-20,000)>] [interval (60sec<1-1440>)] [request-size (100bytes<64-1500>]

    - remove {dest-ip-address <ip address>} {name <> }

    - show-config

    - show-status

    + modem

    - power_down | power-up

    - send command at+cgsn

    - get {iccid| imei| model| version}

    + settings

    - update [quality check <0,time interval>] [backoff1 < 60sec,10-600>] [backoff2<300sec,10-600>] [default-route {yes|no}] [lcp-echo-interval<10sec,0-600>] [lcp-failure<4,1-64>] [preferred-sim {1|2|none}] [rssi-threshold-dbm<-100dbm ,-144 to -61>] [wait-to-restore <14400sec,120-86400>]

    - update retry-threshold-reload <0-30>

    - show

    + wan

    - update {sim-slot <slot(1-2>} {admin-status <enable | disable>} {apn-name <name>} [operator-name <name>] [pin <pin>] [user-name <name>] [password <password>] [radio-access-technology {auto |2G |3G |2Gthen3G |3Gthen2G | 4G | 4Gthen3Gthen2G | 4Gthen3G}] [flow-control {enable|disable}]

    - show

    - refresh

    - network {show}

- Connection {show}
- enable | disable
- show

+ nhrp

- hub {show}
- spoke update private-ip A.B.C.D remote-ip A.B.C.D
- show

Cellular Commands Description

Command	Description
Application connect	Enter the industrial application menu
Cellular	Enter the configuration mode for the Cellular application Enable: enable application Disable: disable application
continuous-echo	Configure ICMP traffic test to validate network connectivity to a remote host. the test sets optionally 2 triggers to be used by the application watch dog : round trip delay and percentage of lost ICMP messages sent. A test is determined by a configurable number of ICMP request following which the average of RRT is calculated. A sufficient trigger to a watchdog is one of these 2 conditions to be met.
Create | update	**name** : name of the test (text) **dest-ip-address** : IP address of a reachable (routable) host. Format aa.bb.cc.dd **rtt-threshold** : round trip threshold in msec. <1,000-20,000> **loss-threshold** : calculated percentage of ICMP requests which were not responded. <10-99> **interval** : time interval in seconds between ICMP messages sent. <1-1440>. **num-of-requests** : number of ICMP messages to send before calculating results of losses and rrd. <1-100>. **request-size** : icmp message packet size
remove	**name** : name of the test (text)
Show-config	Show configuration
Show-status	Show result of loss % and calculated round trip delay
Modem	**Power-up** : power the modem **Power-down** : shut the modem **Send command at+cgsn** : retrieve the IMEI identifier of the modem The modem must be enabled for these commands to take effect.

Command	Description
Settings update	**quality check**: define time interval in seconds for internal RSSI check of active SIM.<0-604800>. 0 – disable RSSI check. **backoff1** : minimum time to stay on a SIM after any fail over. < sec,10-600> **backoff2** : minimum time to stay on a SIM if "caveat" flag is set. This flag is set in case if there was already fail over in last 2 hours. < sec,10-600> **wait-to-restore** : maximum time allowed to stay on non-preferred SIM. default-route: setting the cellular interface to be the default gateway for the application IP interfaces. {yes | no} **lcp-echo-interval** : lcp protocol test of connectivity towards the connected ISP. 1 to 600 seconds interval between tests.0 –disable. **lcp-failure** : number of failed lcp echo tests. <1-64> **update retry-threshold-reload <0-30>** : sets a switch reload after a configurable number of failed attempts to establish "Connected" status of the cellular modem. Configuration which was not committed will not be saved after the reload.
Settings show	Show: show configured interval time.
Wan update	**Sim-slot**: location of SIM to be configured, 1 or 2. **Admin-status**: enable/disable SIM card. **Apn-name**: as given by the network provider. **operator-name** : operator name (text) **Pin**: as given by the network provider. **User-name**: as given by the network provider. **password**: as given by the network provider. Flow-control : enable | disable. **radio-access-technology** : preferred network to connect to. Auto – if 3G available it will be chosen over 2G. 3G – only 3G will be optional to connect to. 2G - only 2G will be optional to connect to. 2Gthen3G – 2G is preferred over 3G. 3Gthen2G - 3G is preferred over 2G. 4G – only 4G will be optional to connect to 4Gthen3Gthen2G –4G will be the preferred optional to connect. Fallback to 3G/2G is allowed. 4Gthen3 –4G will be the preferred optional to connect. Fallback to 3G is allowed.
Wan Show	Show configuration and status of SIM cards
Network show	Show connection time and RSSI per SIM card
Connection show	Show cellular connection status
Nhrp	Entering nhrp configuration
Hub	Show : display connected spokes list
Spoke update	Private IP: identifier in format of an IP address. Used for autorisation vs the hub. A.B.C.D Remote IP: Hub IP.
Spoke show	Show spoke configuration

Default State

The default state of the cellular modem is "disabled". The settings default state are as shown in below table.

```
[cellular/] settings show
+------------+-----------+---------+----------+----------+----------+----------+---------+-----------+-----------+
|  quality   |    dBm    | default | LCP echo | LCP echo | Backoff1 | Backoff2 | Wait to | Preferred |   Retry   |
| check(sec) | threshold |  route  | interval | failure  |  timer   |  timer   | restore |    SIM    | threshold |
|            |           |         |          |          |          |          |         |           |  reload   |
+============+===========+=========+==========+==========+==========+==========+=========+===========+===========+
|     0      |   -100    |   Yes   |    10    |    4     |    60    |   300    |  14400  |   none    |     0     |
+------------+-----------+---------+----------+----------+----------+----------+---------+-----------+-----------+
```

LED Indicators

The modem has a led indicator for each SIM slot to represent the SIM cad state.

Modem admin state	SIM admin state	SIM Operation state	LED
disable	N/A	N/A	OFF
enable	disable	N/A	OFF
	enable	Ready	ON
	enable	not present	Blink 1 Hz
	enable	Failed	Blink 1 Hz
	enable	PIN lock	Blink 1 Hz
	enable	PUK lock	Blink 1 Hz
	enable	connecting	ON
	enable	connected	ON
	enable	connected - secondary	ON
	enable	connected - alternative	ON
	enable	Connected and traffic	ON

Example for retrieving the IMEI

Below is an example of retrieving the IMEI identifier of the modem.

```
RLGE2FE16R# application connect
[/] cellular disable
[/] cellular modem power-up
Completed OK
[/] cellular modem send command at+cgsn
send : at+cgsn
reply : +cgsn
357524040483438
OK
[/]
```

Example: Sim Status

Below is a configuration example of 2 SIM cards and their permissible state status.

```
cellular wan update admin-status enable apn-name internetg sim-slot 1 operator-name
cellcom user-name guest password guest

cellular wan update admin-status enable apn-name internet.pelephone.net.il sim-slot 2
operator-name pelephone user-name pcl@3g password pcl


cellular enable


cellular refresh
```

```
[/] cellular network show
+------+---------+-------------+---------+----------+---------+--------+--------------+------------+
| slot |  oper   |    Last     | Changes | Failures |  Last   | Caveat |     RSSI     | Last RSSI  |
|      | status  | update(sec) |         |          | Failure |        |    [dBm]     | check(sec) |
+======+=========+=============+=========+==========+=========+========+==============+============+
|  1   | UNKNOWN |     16      |    7    |    0     |   N/A   |   No   |     -67      |     23     |
+------+---------+-------------+---------+----------+---------+--------+--------------+------------+
|  2   | UNKNOWN |     16      |    4    |    0     |   N/A   |   No   | not measured |    N/A     |
+------+---------+-------------+---------+----------+---------+--------+--------------+------------+
```

```
[/] cellular network show
+------+---------+-------------+---------+----------+---------+--------+--------------+------------+
| slot |  oper   |    Last     | Changes | Failures |  Last   | Caveat |     RSSI     | Last RSSI  |
|      | status  | update(sec) |         |          | Failure |        |    [dBm]     | check(sec) |
+======+=========+=============+=========+==========+=========+========+==============+============+
|  1   |  READY  |      9      |    8    |    0     |   N/A   |   No   |     -67      |     1      |
+------+---------+-------------+---------+----------+---------+--------+--------------+------------+
|  2   | UNKNOWN |     21      |    4    |    0     |   N/A   |   No   | not measured |    N/A     |
+------+---------+-------------+---------+----------+---------+--------+--------------+------------+
```

```
[/] cellular network show
+------+---------+-------------+---------+----------+---------+--------+--------+------------+
| slot |  oper   |    Last     | Changes | Failures |  Last   | Caveat |  RSSI  | Last RSSI  |
|      | status  | update(sec) |         |          | Failure |        | [dBm]  | check(sec) |
+======+=========+=============+=========+==========+=========+========+========+============+
|  1   |  READY  |     38      |    8    |    0     |   N/A   |   No   |  -67   |     30     |
+------+---------+-------------+---------+----------+---------+--------+--------+------------+
|  2   |  READY  |     15      |    5    |    0     |   N/A   |   No   |  -79   |     10     |
+------+---------+-------------+---------+----------+---------+--------+--------+------------+
```

```
[/] cellular network show
+------+---------------+-------------+---------+----------+---------+--------+--------+------------+
| slot |     oper      |    Last     | Changes | Failures |  Last   | Caveat |  RSSI  | Last RSSI  |
|      |    status     | update(sec) |         |          | Failure |        | [dBm]  | check(sec) |
+======+===============+=============+=========+==========+=========+========+========+============+
|  1   | CONNECTING... |      1      |    9    |    0     |   N/A   |   No   |  -67   |     31     |
+------+---------------+-------------+---------+----------+---------+--------+--------+------------+
|  2   |     READY     |     16      |    5    |    0     |   N/A   |   No   |  -79   |     12     |
+------+---------------+-------------+---------+----------+---------+--------+--------+------------+
```

```
[/] cellular network show
+------+------------+-------------+---------+----------+---------+--------+--------+------------+
| slot |    oper    |    Last     | Changes | Failures |  Last   | Caveat |  RSSI  | Last RSSI  |
|      |   status   | update(sec) |         |          | Failure |        | [dBm]  | check(sec) |
+======+============+=============+=========+==========+=========+========+========+============+
|  1   | CONNECTED! |     96      |   10    |    0     |   N/A   |   No   |  -67   |    132     |
+------+------------+-------------+---------+----------+---------+--------+--------+------------+
|  2   |   READY    |     117     |    5    |    0     |   N/A   |   No   |  -79   |    113     |
+------+------------+-------------+---------+----------+---------+--------+--------+------------+
```

```
[/] cellular connection show
+-----------+----------------+---------+--------+----------+--------+
| interface |    local ip    |   tx    |   tx   |    rx    |   rx   |
|           |                | packet  | error  | packets  | error  |
+===========+================+=========+========+==========+========+
|   ppp0    | 46.210.197.173 |    6    |   0    |    5     |   0    |
+-----------+----------------+---------+--------+----------+--------+
```

Example: Cellular Watch Dog

In below example we will configure a watchdog to cellular modem and see how the SIM status is changing due to the failed test of the watch dog.

An unreachable address of 10.10.10.10 is configured as the destination of the echo in order to provoke test failure and SIM status change.

Preliminary status, SIM card 1 is connected and received IP. Watchdog no configured.

```
[cellular/] network show
+------+------------+-------------+---------+----------+--------------------+--------+-------+------------+
| slot |    oper    |    Last     | Changes | Failures |        Last        | Caveat | RSSI  | Last RSSI  |
|      |   status   | update(sec) |         |          |      Failure       |        | [dBm] | check(sec) |
+======+============+=============+=========+==========+====================+========+=======+============+
|  1   | CONNECTED! |     20      |   22    |    2     | Cont. check failed |   No   |  -73  |     56     |
+------+------------+-------------+---------+----------+--------------------+--------+-------+------------+
|  2   |   READY    |     41      |   14    |    1     | Cont. check failed |  Yes   |  -79  |     37     |
+------+------------+-------------+---------+----------+--------------------+--------+-------+------------+
[cellular/] connection show
+-----------+---------------+---------+--------+----------+--------+
| interface |   local ip    |   tx    |   tx   |    rx    |   rx   |
|           |               | packet  | error  | packets  | error  |
+===========+===============+=========+========+==========+========+
|   ppp0    | 95.35.133.191 |    6    |   0    |    11    |   0    |
+-----------+---------------+---------+--------+----------+--------+
```

1. Configuration of a watchdog.

```
Application connect
[/] cellular continuous-echo
[cellular/continuous-echo/]
[cellular/continuous-echo/] create name destination _ 1 dest-ip-address 10.10.10.10 loss-threshold 20 num-of-requests 3 interval 2 request-size 64
Completed OK
```

```
[cellular/continuous-echo/] show-config
Cellular echo response diagnostics table:
+---------------+-------------+----------+----------+---------+-----------+-----------+
|      Name       |      IP       | interval |   number   | request |    loss     |     rtt
|
|                 |    address    |          |     of     |  size   | threshold | threshold
|
|                 |               |          | requests |         |           |
|
+===============+=============+==========+==========+=========+===========+===========+
| destination _ 1 | 10.10.10.10 |     2      |     3      |   64    |     20      |    5000
|
+---------------+-------------+----------+----------+---------+-----------+-----------+
```

2. Status of the watchdog

```
[cellular/continuous-echo/] show-status
Cellular echo response diagnostics table:
+---------------+------+------+------+---------+---------+----------+--------+------------+
|      Name       | last | last | last | highest | highest | interval | failed |     last
|
|                 | loss | avg  | max  |  loss   |   rtt   | counter  |        |
check     |
|                 |      | rtt  | rtt  |         |         |          |        |
(secs ago) |
+===============+======+======+======+=========+=========+==========+========+==========
==+
| destination _ 1 | 100  |  0   |  0   |    0    |    0    |    0     |  Yes   |
319      |
+---------------+------+------+------+---------+---------+----------+--------+------------+
```

Status of SIM card connection

```
[cellular/] network show
+------+-------------+-------------+---------+----------+--------------------+--------+-------+-------------+
| slot |    oper     |    Last     | Changes | Failures |        Last        | Caveat | RSSI  | Last RSSI   |
|      |   status    | update(sec) |         |          |      Failure       |        | [dBm] | check(sec)  |
+======+=============+=============+=========+==========+====================+========+=======+=============+
|  1   | CONNECTED!  |     256     |   22    |    2     | Cont. check failed |   No   |  -73  |     293     |
+------+-------------+-------------+---------+----------+--------------------+--------+-------+-------------+
|  2   |    READY    |     277     |   14    |    1     | Cont. check failed |  Yes   |  -79  |     273     |
+------+-------------+-------------+---------+----------+--------------------+--------+-------+-------------+
[cellular/] network show
+------+---------+-------------+---------+----------+--------------------+--------+-------+-------------+
| slot |  oper   |    Last     | Changes | Failures |        Last        | Caveat | RSSI  | Last RSSI   |
|      | status  | update(sec) |         |          |      Failure       |        | [dBm] | check(sec)  |
+======+=========+=============+=========+==========+====================+========+=======+=============+
|  1   | FAILED  |      1      |   23    |    3     | Cont. check failed |   No   |  -73  |     299     |
+------+---------+-------------+---------+----------+--------------------+--------+-------+-------------+
|  2   | READY   |     284     |   14    |    1     | Cont. check failed |  Yes   |  -79  |     280     |
+------+---------+-------------+---------+----------+--------------------+--------+-------+-------------+

[cellular/] network show
+------+--------------+-------------+---------+----------+--------------------+--------+-------+-------------+
| slot |     oper     |    Last     | Changes | Failures |        Last        | Caveat | RSSI  | Last RSSI   |
|      |    status    | update(sec) |         |          |      Failure       |        | [dBm] | check(sec)  |
+======+==============+=============+=========+==========+====================+========+=======+=============+
|  1   |    FAILED    |     64      |   23    |    3     | Cont. check failed |   No   |  -73  |     362     |
+------+--------------+-------------+---------+----------+--------------------+--------+-------+-------------+
|  2   | CONNECTING...|      6      |   15    |    1     | Cont. check failed |  Yes   |  -79  |     343     |
+------+--------------+-------------+---------+----------+--------------------+--------+-------+-------------+
[cellular/] network show
+------+---------------------------+-------------+---------+----------+--------------------+--------+-------+-------------+
| slot |           oper            |    Last     | Changes | Failures |        Last        | Caveat | RSSI  | Last RSSI   |
|      |          status           | update(sec) |         |          |      Failure       |        | [dBm] | check(sec)  |
+======+===========================+=============+=========+==========+====================+========+=======+=============+
|  1   |          FAILED           |     66      |   23    |    3     | Cont. check failed |   No   |  -73  |     364     |
+------+---------------------------+-------------+---------+----------+--------------------+--------+-------+-------------+
|  2   | CONNECTED-AS-ALTERNATIVE  |      1      |   16    |    1     | Cont. check failed |  Yes   |  -79  |     345     |
+------+---------------------------+-------------+---------+----------+--------------------+--------+-------+-------------+

[cellular/] connection show
+-----------+---------------+---------+--------+----------+--------+
| interface |   local ip    |   tx    |   tx   |    rx    |   rx   |
|           |               | packet  | error  | packets  | error  |
+===========+===============+=========+========+==========+========+
|   ppp0    | 10.166.187.235|    6    |   0    |    5     |   0    |
+-----------+---------------+---------+--------+----------+--------+
```

Adding a second test for the watchdog. This time the destination address is reachable.

```
[cellular/continuous-echo/] create name destination_2 dest-ip-address 80.74.102.38 loss-threshold 20 num-of-requests 3 interval 2 request-size 64
```

```
[cellular/continuous-echo/] show-config
Cellular echo response diagnostics table:
+---------------+-------------+----------+----------+---------+----------+-----------+
|     Name      |     IP      | interval |  number  | request |   loss   |    rtt    |
|               |   address   |          |    of    |  size   | threshold | threshold |
|               |             |          | requests |         |          |           |
+===============+=============+==========+==========+=========+==========+===========+
| destination_1 | 10.10.10.10 |    2     |    3     |   64    |    20    |   5000    |
+---------------+-------------+----------+----------+---------+----------+-----------+
| destination_2 | 80.74.102.38|    2     |    3     |   64    |    20    |   5000    |
+---------------+-------------+----------+----------+---------+----------+-----------+
```

In next screenshot we see that although the remote IP 80.74.102.38 is accessible, the echo request result did not meet the criteria of the watchdog set to 20% max loss.

```
--- 80.74.102.34 ping statistics ---
3 packets transmitted, 2 packets received, 33% packet loss
round-trip min/avg/max = 97.149/118.644/140.140 ms
Completed OK
```

The result of the failure will initiate testing again the sim1 as seen below.

```
[cellular/] network show
+------+--------------------------+-------------+---------+----------+--------------------+--------+-------+-------------+
| slot |          oper            |    Last     | Changes | Failures |        Last        | Caveat | RSSI  | Last RSSI   |
|      |         status           | update(sec) |         |          |      Failure       |        | [dBm] | check(sec)  |
+======+==========================+=============+=========+==========+====================+========+=======+=============+
|  1   | CONNECTED-AS-ALTERNATIVE |     229     |   25    |    3     | Cont. check failed |  Yes   |  -73  |    1001     |
+------+--------------------------+-------------+---------+----------+--------------------+--------+-------+-------------+
|  2   |          FAILED          |     295     |   18    |    2     | Cont. check failed |   No   |  -79  |     982     |
+------+--------------------------+-------------+---------+----------+--------------------+--------+-------+-------------+

[cellular/] connection show
+-----------+-----------------+---------+--------+----------+--------+
| interface |    local ip     |   tx    |   tx   |    rx    |   rx   |
|           |                 | packet  | error  | packets  | error  |
+===========+=================+=========+========+==========+========+
|   ppp0    | 109.253.99.232  |    7    |   0    |    6     |   0    |
+-----------+-----------------+---------+--------+----------+--------+

[cellular/] network show
+------+-------------+-------------+---------+----------+--------------------+--------+-------+-------------+
| slot |    oper     |    Last     | Changes | Failures |        Last        | Caveat | RSSI  | Last RSSI   |
|      |   status    | update(sec) |         |          |      Failure       |        | [dBm] | check(sec)  |
+======+=============+=============+=========+==========+====================+========+=======+=============+
|  1   | CONNECTED!  |     106     |   26    |    3     | Cont. check failed |   No   |  -73  |    1179     |
+------+-------------+-------------+---------+----------+--------------------+--------+-------+-------------+
|  2   |   FAILED    |     473     |   18    |    2     | Cont. check failed |   No   |  -79  |    1160     |
+------+-------------+-------------+---------+----------+--------------------+--------+-------+-------------+
```

VPN Setup Examples

L2 VPN over Layer 3 cloud

The following example will demonstrate proper configuration of L2 VPN over layer 3 cloud.

Concept:

Maintaining virtual LAN, layer 2 connectivity between two remote sites connected over layer 3 cloud.

The 2 PCs on the map are holding IP addresses with the same subnet. Following configuration will allow traffic between them to pass over the GRE tunnel as if they were connected at the same LAN.

Switch B will be configured so that the computer on side A will be able to manage it via SSH through the tunnel.

The spoke is set as terminal server to serve a locally connected serial remote. The PC (192.168.10.250) will be able to open a secure telnet connection to the spoke (over the encrypted tunnel) to control the remote remote.

The spoke is set as an IEC101/104 gateway to serve a locally connected IEC101 remote. The PC (192.168.10.250) will be able to open an IEC 104 connection to the spoke gateway (over the encrypted tunnel) to control the remote IEC 101 remote.

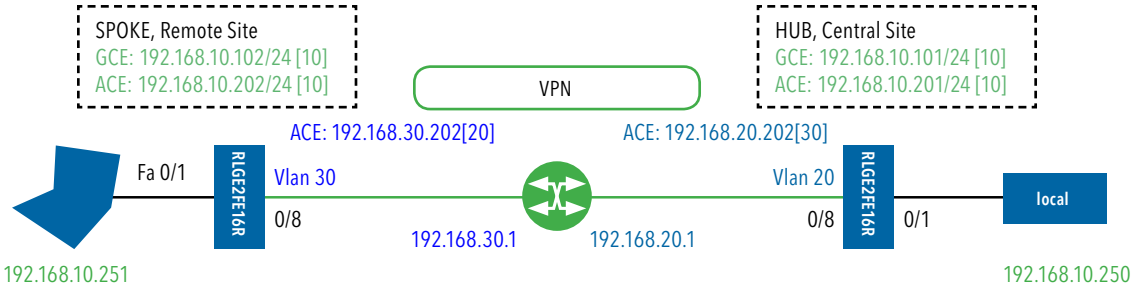
A serial tunneling service set between a local and remote. This service traffic is encrypted over the tunnel.

Guidelines:

- The proper usage of the ACE ports is of importance, port gigabitethernet 0/4 is to be added as tagged member to the customer service VLANs (vlan 10 at following example). By assigning this port, all traffic at the specified vlan will be send over the VPN.
- At both the hub and spoke, an ACE IP interface must be assigned as am 'application-host' type. This interface is used as the tunnel end point. Port gigabitethernet 0/3 is to be set as a tagged member at this ACE interface vlan (vlan 20 and 30 at following example).
- An additional ACE interface (type 'general') is set at the spoke to support the serial services: serial-tuneling, terminal-server, 101/104 gateway.
- An additional ACE interface (type 'general') is set at the HUB to support the serial-tuneling service.
- Port gigabitethernet 0/4 has a default state of disable mac-learning. When used in L2 VPN, this state must be changed to allow mac-learning.

Network drawing, part A

Establish the L2 VPN and IP traffic over it.



Configuration

Hub

1. Set host name (optional)

```
set host-name Hub
```

2. Create vlan 20 for network connection towards the router

```
config terminal
vlan 20
ports fast 0/8 gigabitethernet 0/3 untagged fastethernet 0/8 name network
exit
interface fastethernet 0/8
switchport pvid 20
alias VPN
exit
```

3. Create vlan 10 for access. Port giga 0/4 is added as a member in order to direct the incomng traffic at the access ports (0/1) to the vpn. port giga 0/3 is added for the later added serial services.

```
vlan 10
ports fastethernet 0/1 gigabitethernet 0/3-4 untagged fastethernet 0/1 name CE
exit
interface fastethernet 0/1
switchport pvid 10
alias SCADA
exit
```

4. Enable mac learning on Gigabitethernet 0/4

```
interface  gigabitethernet  0/4
switchport unicast-mac learning enable
exit
```

5. Remove default IP interface from vlan 1 (optional, to avoid conflicts)

```
interface vlan 1
shutdown
no ip address
exit
```

6. Create a GCE interface for management at vlan 10

```
interface vlan 10
ip address 192.168.10.101 255.255.255.0
no shutdown
exit
```

7. Disable RSTP

```
shutdown spanning-tree
no spanning-tree
end
write startup-cfg
```

8. Configure the tunnel, use an ACE interface of 'application-host' type:

```
RLGE2FE16R#application connect
[/]router interface create address-prefix 192.168.20.201/24 vlan 20 purpose application-host
description tunnel


router static
enable
configure terminal
ip route 192.168.30.0/24 192.168.20.1
write memory
exit
exit
[/]l2-vpn tunnel create  remote-address 192.168.30.202 name tunnel _ 1
```

9. Configure IPSec

```
ipsec isakmp update my-id Hub.ComNet.com
ipsec preshared create id Spoke1.ComNet.com key secretkey
ipsec preshared create id Hub.ComNet.com key secretkey
ipsec policy create protocol gre
ipsec isakmp update id-type fqdn
ipsec disable
ipsec enable
exit
write startup-cfg
```

Spoke

1. Set host name (optional)

```
set host-name Spoke
```

2. Create vlan 30 for network connection towards the router

```
config terminal
vlan 30
ports fast 0/8 gigabitethernet 0/3 untagged fastethernet 0/8 name network
exit
interface fastethernet 0/8
switchport pvid 30
alias VPN
exit
```

3. Create vlan 10 for access. Port giga 0/4 is added as a member in order to direct the incomng traffic at the access ports (0/1) to the vpn. port giga 0/3 is added for the later added serial services.

```
vlan 10
ports fastethernet 0/1 gigabitethernet 0/3-4 untagged fastethernet 0/1 name CE
exit
interface fastethernet 0/1
switchport pvid 10
alias SCADA
exit
```

4. Enable mac learning on Gigabitethernet 0/4

```
interface  gigabitethernet  0/4
switchport unicast-mac learning enable
exit
```

5. Remove default IP interface from vlan 1 (optional, to avoid conflicts)

```
interface vlan 1
shutdown
no ip address
exit
```

6. Create a GCE interface for management at vlan 10

```
interface vlan 10
ip address 192.168.10.102 255.255.255.0
no shutdown
exit
```

7. Disable RSTP

```
shutdown spanning-tree
no spanning-tree
end
write startup-cfg
```

8. Configure the tunnel, use an ACE interface of 'application-host' type:

```
RLGE2FE16R#application connect
 [/]router interface create address-prefix 192.168.30.202/24 vlan 30 purpose application-
host description tunnel
router static
enable
configure terminal
ip route 192.168.20.0/24 192.168.30.1
write memory
exit
exit
vpn l2 tunnel create remote-address 192.168.20.201 name tunnel _ 1
vpn l2 nhrp spoke update private-ip 192.168.30.202 remote-ip 192.168.20.201
[/]
```

9. Configure IPSec

```
ipsec isakmp update my-id Spoke1.ComNet.com
ipsec preshared create id Spoke1.ComNet.com key secretkey
ipsec preshared create id Hub.ComNet.com key secretkey
ipsec policy create protocol gre
ipsec isakmp update id-type fqdn
ipsec disable
ipsec enable
exit
write startup-cfg
```

Test the setup (shown at the hub)

1. Verify ping from ACE to ACE

```
[/] ping 192.168.30.202
PING 192.168.30.202 (192.168.30.202): 56 data bytes
64 bytes from 192.168.30.202: seq=0 ttl=63 time=0.460 ms
64 bytes from 192.168.30.202: seq=1 ttl=63 time=0.363 ms
```

2. Verify IPSec SA established

```
[/] ipsec show log
…
2015-05-04 17:49:05: INFO: IPsec-SA established: ESP/Transport 192.168.20.201[500]-
>192.168.30.202[500] spi=152943490(0x91dbb82)
2015-05-04 17:49:05: INFO: IPsec-SA established: ESP/Transport 192.168.20.201[500]-
>192.168.30.202[500] spi=167249243(0x9f8055b)
```

3. Verify ping from GCE to GCE

```
Hub# ping 192.168.10.102
Reply Received From :192.168.10.102, TimeTaken : 10 msecs
Reply Received From :192.168.10.102, TimeTaken : 3 msecs
Reply Received From :192.168.10.102, TimeTaken : 3 msecs
```

4. Verify ping between the PCs

Network drawing, part B

Based on part A of the setup, we will now add the serial services.

Spoke:

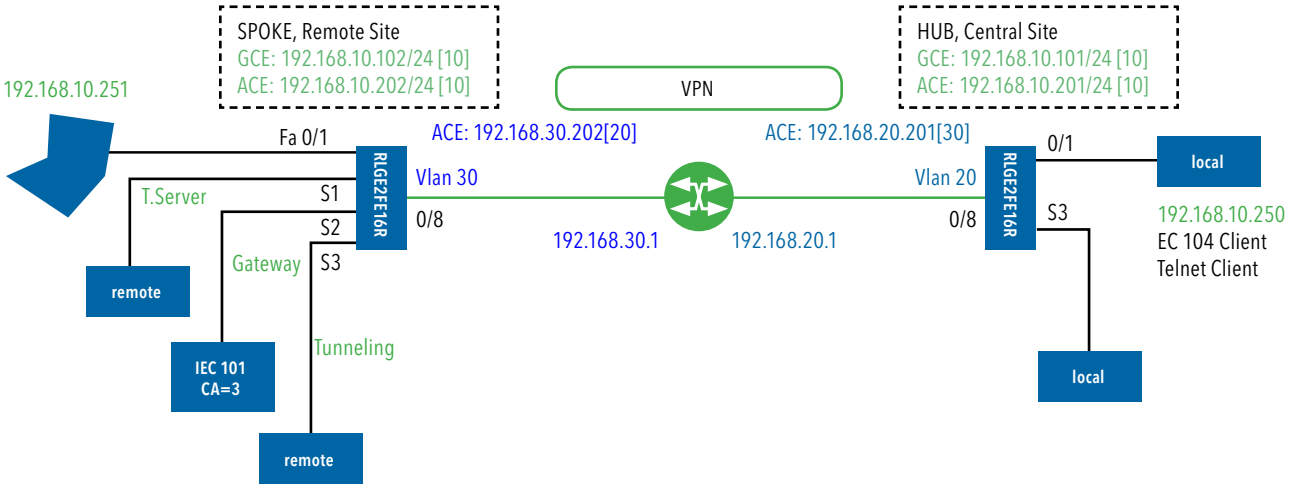
1. Terminal server (remote at port 1).

2. gateway 101/104 (remote at port 2).

3. Serial tunneling (remote at port 3).

Hub:

1. Serial tunneling (remote at port 3).



Configuration

Hub

1. Add an ACE interface at vlan 10 for the serial tunneling

```
application connect
router interface create address-prefix 192.168.10.201/24 vlan 10 purpose general description
serial
```

2. Configure the serial tunneling service pointing to the spoke ACE interface of vlan 10 as the remote end point

```
serial port create slot 1 port 3 baudrate 9600 parity no  stopbits 1 mode-of-operation
transparent
serial local-end-point create slot 1 port 3 service-id 3 position local application
serial-tunnel
serial remote-end-point create service-id 3 remote-address 192.168.10.202 position remote
connection-mode udp buffer-mode byte
```

Spoke

1. Add an ACE interface at vlan 10 for the serial services

```
application connect
router interface create address-prefix 192.168.10.202/24 vlan 10 purpose general
description serial
```

2. Configure the terminal server service

```
serial port create slot 1 port 1 baudrate 9600 parity no stopbits 1 mode-of-operation
transparent
serial local-end-point create slot 1 port 1 service-id 1  application terminal-server
terminal-server admin-status enable
terminal-server tcp-service create service-id 1 remote-address 192.168.10.202 telnet-port
2050
```

3. Configure the gateway service

```
serial port create slot 1 port 2 baudrate 9600 parity even  stopbits 1 mode-of-operation
transparent
serial local-end-point create slot 1 port 2 service-id 2 position remote application
iec101-gw
iec101-gw  config gw update mode balanced ip _ addr 192.168.10.202
iec101-gw config iec101 create slot 1 port 2 asdu _ addr 3 orig _ addr 0 link _ addr 1
```

4. Configure the serial tunneling service pointing to the hub ACE interface of vlan 10 as the remote end point

```
serial port create slot 1 port 3 baudrate 9600 parity no  stopbits 1 mode-of-operation
transparent
serial local-end-point create slot 1 port 3 service-id 3 position remote application
serial-tunnel
serial remote-end-point create service-id 3 remote-address 192.168.10.201 position local
connection-mode udp buffer-mode byte
```

Test the setup (shown at the hub)

1. Verify ping from the SCADA to the the spoke ACE vlan 10 interface

```
C:\Users\Eran>ping 192.168.10.202

Pinging 192.168.10.202 with 32 bytes of data:
Reply from 192.168.10.202: bytes=32 time=3ms TTL=64
Reply from 192.168.10.202: bytes=32 time=1ms TTL=64
Reply from 192.168.10.202: bytes=32 time=1ms TTL=64
```

2. Open telnet session from the SCADA to the spoke ACE vlan 10 interface with port 2050. The serial remote at serial port 1 should reply.

```
[/] terminal-server connections show
+-------+---------+--------+---------------+---------------+----------+-----------+
| index | service | telnet |     client    |     client    |  client  |  client   |
|       |    id   |  port  |   source IP   |    dest IP    | dest slot | dest port |
+=======+=========+========+===============+===============+==========+===========+
|   1   |    1    |  2050  | 192.168.10.250 | 192.168.10.202 |     1     |     1     |
+-------+---------+--------+---------------+---------------+----------+-----------+
```

3. Open IEC 104 session from the SCADA to the spoke ACE vlan 10 interface.

The serial IEC 101 remote at serial port 2 should reply.

The spoke should indicate the IEC 101 remote has a connection state UP

```
[/]iec101-gw show all
101-104 ROUTER
BALANCED MODE
IEC 104:
+---------------+-----------+-----------+----------+----+----+----+----+
|        IP     | ORIG. ADDR | CLOCK SYNC | TIME TAG | T0 | T1 | T2 | T3 |
+===============+===========+===========+==========+====+====+====+====+
| 192.168.10.202 |      0      |      n       |     n     | 30 | 15 | 10 | 20 |
| 192.168.10.250 |      0      |      n       |     n     | 30 | 15 | 10 | 20 |
+---------------+-----------+-----------+----------+----+----+----+----+
IEC 101:
+------+------+-------+----------+---------+-------------+----------+---------+---------+----
| SLOT | PORT | OP ST | LINK ADR | CMN ADR | CONV CMN ADR | LINK LEN | CMN LEN | COT
LEN | IOA LEN
+======+======+=======+==========+=========+=============+==========+=========+========
|  1   |  2   |  UP   |     1      |     3     |       0       |     2      |     2     |
2     |     3
```

```
+------+------+-------+----------+---------+-------------+----------+---------+---------+----
+------+------+-----------+------+---------+---------+---------+----------+---------+---------
| SLOT | PORT | ORIG. ADR | S CH | DIR BIT | TEST FR | GEN INT | TIME TAG | COT LEN |
IOA LEN | CMN
+======+======+===========+======+=========+=========+=========+==========+=========+===
|  1   |  2   |     0     |  y   |  AUTO   |    y    |    n    |    n     |    2    |
3    |
+------+------+-----------+------+---------+---------+---------+----------+---------+---------
[/]
```

4. Verify serial traffic between the local device at the hub (port 3) and remote device at the spoke (port 3) is ok. View the counters progressing.

```
[/]serial port show port 3 briefly
+-----+------+------+-----+-------------+------+------+--------+------+
| idx | slot | port | svc |     mode      | baud | data | parity | stop |
|     |      |      | id  |               | rate | bits |        | bits |
+=====+======+======+=====+=============+======+======+========+======+
|  1  |  1   |  3   |  3  | Transparent | 9600 |  8   |  None  |  1   |
+-----+------+------+-----+-------------+------+------+--------+------+
OctetsIn      : 52
OctetsOut     : 52
TxError       : 0
RxError       : 0
OctetsTotal   : 99
```

5. Verify ping between the PCs

Testing the setup

1. Ping is now possible between :

   i. The application IPs : 172.17.203.220 and 172.18.212.220

   ii. The PCs : 192.168.0.100 and 192.168.0.101.

2. SSH managemnt is possible from the PC 192.168.0.100 to the switch B at IP 192.168.0.102.

IPSec VPN over Layer 3 cloud

The following example will demonstrate proper configuration of IPSec-VPN over layer 3 cloud.

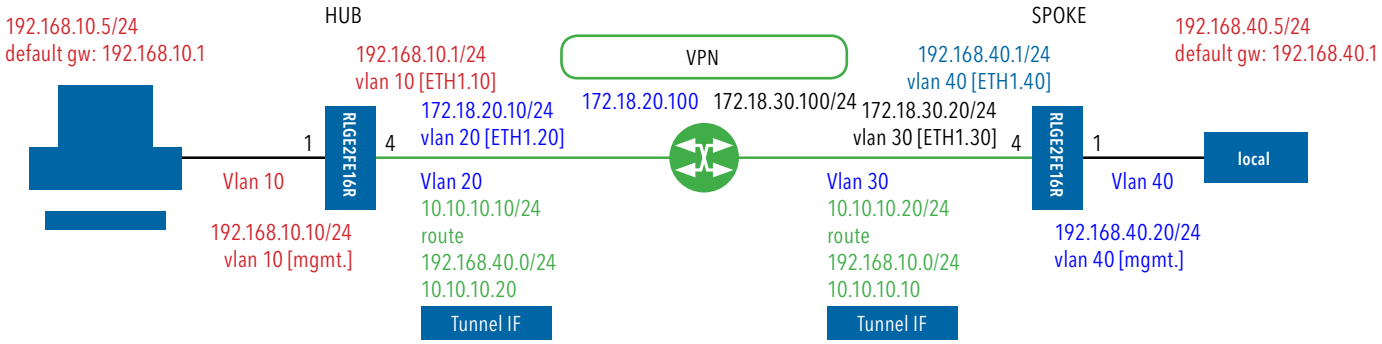
Concept:

Maintaining layer 3 connectivity between two remote sites connected over layer 3 cloud.

The 2 PCs on the map are holding IP addresses with different subnets. Following configuration will allow secure and routable traffic between them.

The Switches are configured so that the computers can remote manage them via SSH through the tunnel.

Network drawing



Configuration

ROUTER (RLGE2FE16R switch)

1. Create GCE IP Interfaces:

```
config terminal
interface vlan 20
ip address 172.18.20.100 255.255.255.0
no shutdown
exit
interface vlan 30
ip address 172.18.30.100 255.255.255.0
no shutdown
exit
```

2. Create vlans:

```
vlan 20
ports fastethernet 0/1
exit
vlan 30
ports fastethernet 0/2
exit
vlan 1
no ports fastethernet 0/1-2 untagged fastethernet 0/1-2
end
write startup-cfg
```

HUB

1. Set switch host name (not mandatory)

```
set host-name hub
```

2. Disable spanning tree and remove the ports to be used in the VPN from default vlan 1

```
config terminal
no spanning-tree
vlan 1
no ports fastethernet 0/1,0/4 gigabitethernet 0/3 untagged fastethernet 0/1,0/4
exit
```

3. Assign the user and network vlans and set PVID for the untagged ports

```
vlan 10
ports fastethernet 0/1 gigabitethernet 0/3 untagged fastethernet 0/1
exit
vlan 20
ports fastethernet 0/4 gigabitethernet 0/3
exit
interface fastethernet 0/1
switchport pvid 10
exit
interface fastethernet 0/4
switchport pvid 20
exit
```

4. Assign switch management IP interface (not mandatory)

```
interface vlan 10
ip address 192.168.10.10 255.255.255.0
no shut
exit
```

5. Assign static route so switch management will be routable over the VPN

```
ip route 192.168.0.0 255.255.0.0 192.168.10.1
end
write startup-cfg
```

6. Assign IP interface in the application which will route user traffic

```
application connect
router interface create address-prefix 192.168.10.1/24 vlan 10 purpose application-host
description user1
```

7. Assign IP interface in the application towards the WAN router

```
router interface create address-prefix 172.18.20.10/24 vlan 20 purpose general description
wan
```

```
8. Assign the IPSec tunnel
vpn ipsec tunnel create remote-address 172.18.30.20 address-prefix 10.10.10.10/24 lower-
```

```
layer-dev eth1.20 name test
```

9. Assign routes for the remote user network (192) and for the public network (172)

```
router static
enable
configure terminal
ip route 192.168.40.0/24 10.10.10.20   !remote user subnet via remote tunnel IF
ip route 172.18.30.0/24 172.18.20.100  !remote public IF via router connected IF
write
exit
exit
```

10. Configure IPSec

```
ipsec isakmp update dh-group modp1536
ipsec isakmp update pfs-group modp1536
ipsec isakmp update phase1-hash-algo md5
ipsec isakmp update phase1-encryption-algo 3des
ipsec isakmp update phase2-auth-algo hmac _ md5
ipsec isakmp update phase2-encryption-algo 3des
ipsec isakmp update ike-phase1-mode main
ipsec preshared create id 172.18.30.20 key 123456    !remote public ip
ipsec preshared create id 172.18.20.10 key 123456    !local public ip eth1.20
ipsec policy create protocol ipencap
ipsec enable
exit
write startup-cfg
```

SPOKE

1. Set switch host name (not mandatory)

```
set host-name spoke
```

2. Disable spanning tree and remove the ports to be used in the VPN from default vlan 1

```
config terminal
no spanning-tree

vlan 1
no ports fastethernet 0/1,0/4 gigabitethernet 0/3 untagged fastethernet 0/1,0/4
```

```
exit
```

3. Assign the user and network vlans and set PVID for the untagged ports

```
vlan 40
ports fastethernet 0/1 gigabitethernet 0/3 untagged fastethernet 0/1
exit
vlan 30
ports fastethernet 0/4 gigabitethernet 0/3
exit

interface fastethernet 0/1
switchport pvid 40
exit
interface fastethernet 0/4
switchport pvid 30
exit
```

4. Assign switch management IP interface (not mandatory)

```
interface vlan 40
shut
ip address 192.168.40.20 255.255.255.0
no shut
exit
```

5. Assign static route so switch management will be routable over the VPN

```
ip route 192.168.0.0 255.255.0.0 192.168.40.1
end
write startup-cfg
```

6. Assign IP interface in the application which will route user traffic

```
application connect


router interface create address-prefix 192.168.40.1/24 vlan 40 purpose application-host
description user1
```

7. Assign IP interface in the application towards the WAN router

```
router interface create address-prefix 172.18.30.20/24 vlan 30 purpose general description
wan
```

8. Assign the IPSec tunnel

```
vpn ipsec tunnel create remote-address 172.18.20.10 address-prefix 10.10.10.20/24 lower-
layer-dev eth1.30 name test
```

9. Assign routes for the remote user network (192) and for the public network (172)

```
router static
enable
configure terminal
ip route 192.168.10.0/24 10.10.10.10    !remote user subnet via remote tunnel IF
ip route 172.18.20.0/24 172.18.30.100   !remote public IF via router connected IF
write
exit
exit
```

10. Configure IPSec

```
ipsec isakmp update dh-group modp1536
ipsec isakmp update pfs-group modp1536
ipsec isakmp update phase1-hash-algo md5
ipsec isakmp update phase1-encryption-algo 3des
ipsec isakmp update phase2-auth-algo hmac _ md5
ipsec isakmp update phase2-encryption-algo 3des
ipsec isakmp update ike-phase1-mode main
ipsec preshared create id 172.18.20.10 key 123456     !remote public ip
ipsec preshared create id 172.18.30.20 key 123456     !local public ip eth1.30
ipsec policy create protocol ipencap
ipsec enable
exit
write startup-cfg
```

Test

1. Ping is now possible between :

```
The application IPs : 172.18.20.10 and 172.18.30.20
The switch interfaces : 192.168.10.10 and 192.168.40.20.
The PCs : 192.168.10.5  and 192.168.40.5.
SSH managemnt is possible from the PCs to the switch IPs.
```

L2 VPN over Cellular Setup

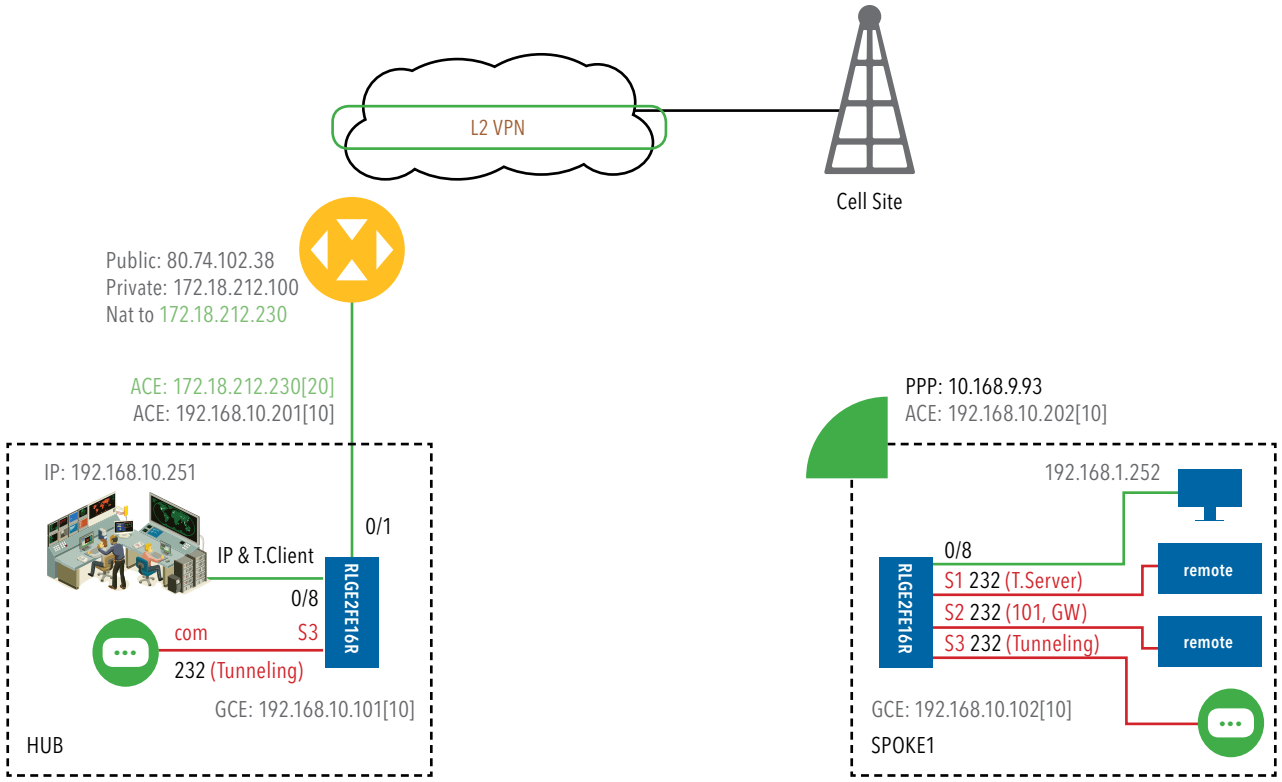
Following network demonstrates a Spoke – Hub topology.

The Spoke is equipped with a SIM card allowing it to connect to the ISP.

Implementation concepts:

1. The ISPs should provide the Spoke, following SIM card authentication, with a routable IP address. At below example the valid IP 10.168.9.93 was issued to the Spoke SIM card by the ISP Orange.
2. At the Hub side, a static, routable address should be assigned to the switch ACE interface. The ACE interface must be 'application-host' type. At below example the hub is located behind a NAT router. The NAT is holding a public address 80.74.102.38 and has a local route to the ACE interface of the hub over subnet 172.18.212.x. Since the hub is not directly routable with the spoke, the NAT router must be set to forward incoming traffic at its public interface towards the hub interface (172.18.212.230).
3. As the hub is located behind a NAT router, a default gateway should be assigned at the application interface (172.18.212.100).
4. At the spoke, an ACE interface should be assigned for proper registration via the Hub. This IP (192.168.10.202 in below example) will be used as well for serial services. The cellular modem settings should be set for it to act as the default gateway.
5. IPSec must be configured to ensure secure traffic and proper NAT traversal.
6. Between the hub and the spoke there will be created a layer 2 tunnel using the NHRP protocol .traffic between the 2 remote LANs (e.g., the two PCs) will be directed through the tunnel. The 2 remote PCs should be members of the same VLAN and should hold IP addresses of the same subnet. In below example vlan 10 and subnet 192.168.10.xx/24 are configured for both remote PCs.
7. The proper usage of the ACE ports is of importance, port gigabitethernet 0/4 is to be added as tagged member to the customer service VLANs (VLAN 10 at following example). By assigning this port, all traffic at the specified VLAN will be send over the VPN.
8. Port gigabitethernet 0/4 has a default state of disable mac-learning. When used in L2 VPN, this state must be changed to allow mac-learning.
9. At the hub, which is connected to the network over an Ethernet port, an ACE IP interface must be assigned as am 'application-host' type. This interface is used as the tunnel end point. Port gigabitethernet 0/3 is to be set as a tagged member at this ACE interface VLAN (VLAN 20 at following example).
10. At the hub, a second ACE interface us required, as the source of the serial tunneling service.

Network drawing



L2 VPN , RLGE2FE16R cellular spoke - RLGE2FE16R hub

Spoke

1. Set host name (optional)

```
set host-name Spoke1
```

2. Disable spanning tree

```
config terminal
shutdown spanning-tree
no spanning-tree
```

3. Enable mac learning on the application port gigabiethernet 0/4

```
interface gigabitethernet 0/4
switchport unicast-mac learning enable
exit
```

4. Create vlan 10 to direct UNI traffic from the PC to the tunnel.

```
port  gigabitethernet 0/4 must be a tagged member at this vlan.
Port gigabitethernet 0/3 is added as well as an ACE interface at vlan 10 will be created for the serial services.
vlan 10
ports fastethernet 0/8 gigabitethernet 0/3-4 untagged fastethernet 0/8 name LAN
exit
interface fastethernet 0/8
switchport pvid 10
exit
interface vlan 10
ip address 192.168.10.102 255.255.255.0
no shutdown
end
```

5. Remove gigabitethernet 0/4 from default vlan 1, to avoid unintentional traffic to be sent over the vpn.

```
config terminal
vlan 1
no ports gigabitethernet 0/4
end
write startup-cfg
```

6. Enabling cellular application mode

```
application connect
cellular settings update default-route yes
```

7. Set the properties of the SIM

```
cellular wan update admin-status enable apn-name uinternet sim-slot 1 operator-name orange user-name orange password orange


cellular enable
```

8. Create an ACE interface

```
router interface create address-prefix 192.168.10.202/24 vlan 10 purpose application-host
```

9. NHRP configuration

```
[/] vpn l2 nhrp spoke update private-ip 192.168.10.202 remote-ip 80.74.102.38
 exit
```

10. IPSec configuration

```
ipsec isakmp update my-id RTU1.ComNet.com
ipsec preshared create id HUB.ComNet.com key secretkey
ipsec preshared create id RTU1.ComNet.com key secretkey
ipsec isakmp update id-type fqdn
ipsec policy create protocol gre
ipsec enable
exit
write startup-cfg
```

Hub

1. Set host name (optional)

```
set host-name Hub
```

2. Disable spanning tree

```
config terminal
shutdown spanning-tree
no spanning-tree
```

3. Enable mac learning on the application port gigabiethernet 0/4

```
interface gigabitethernet 0/4
switchport unicast-mac learning enable
exit
```

4. Create vlan 10 to direct UNI traffic from the PC to the tunnel.

```
port  gigabitethernet 0/4 must be a tagged member at this vlan. Port gigabitethernet 0/3
is added as well as an ACE interface at vlan 10 will be created for the serial services.
Create vlan 20 for the networking towards the cloud. Port gigabitethernet 0/3 must be a
tagged member at this vlan.
vlan 20
ports fastethernet 0/1 gigabitethernet 0/3 untagged fastethernet 0/1 name WAN
exit
vlan 10
ports fastethernet 0/8 gigabitethernet 0/3-4 untagged fastethernet 0/8 name LAN
```

```
exit
interface fastethernet 0/8
no shutdown
switchport pvid 10
exit
interface fastethernet 0/1
no shutdown
switchport pvid 20
exit
interface vlan 10
shutdown
ip address 192.168.10.101 255.255.255.0
no shutdown
end
write startup-cfg
```

5. Remove gigabitethernet 0/4 from default vlan 1, to avoid unintentional traffic to be sent over the vpn.

```
config terminal
vlan 1
no ports gigabitethernet 0/4
end
write startup-cfg
```

6. Crate ACE interface for the networking, must be an 'application-host type as it is used for the tunnel establishment.

```
router interface create address-prefix 172.18.212.230/24 vlan 20 purpose application-host
```

7. Create an ACE interface to e used for serial services over the tunnel

```
router interface create address-prefix 192.168.10.201/24 vlan 10 purpose general
description serial _ services
```

8. Set route over the cloud

```
router static
enable
configure terminal
ip route 0.0.0.0/0  172.18.212.100
write memory
exit
exit
```

9. IPSec configuration

```
ipsec isakmp update my-id HUB.ComNet.com
ipsec preshared create id HUB.ComNet.com key secretkey
ipsec preshared create id RTU1.ComNet.com key secretkey
ipsec isakmp update id-type fqdn
ipsec policy create protocol gre
ipsec enable
exit
write startup-cfg
```

Testing the setup

1. Verify the cellular connection has established at the spoke.

```
[/] cellular connection show
+-----------+-------------+---------+--------+----------+--------+
| interface | local ip    |    tx   |   tx   |    rx    |   rx   |
|           |             |  packet |  error |  packets |  error |
+===========+=============+=========+========+==========+========+
|    ppp0   | 10.168.9.93 |    39   |    0   |    31    |    0   |
+-----------+-------------+---------+--------+----------+--------+
```

2. Verify connectivity between the spoke cellular interface and the hub public IP by pinging from the spoke ACE towards 80.74.102.38

3. Verify ipsec sa has established (below is spoke show example)

```
[/] ipsec show sa
10.168.9.93[4500] 80.74.102.38[4500]
         esp-udp mode=transport spi=73136673(0x045bfa21) reqid=0(0x00000000)
         E: 3des-cbc  0dce56ef 01a70616 de752007 81f87ca8 1c94aeae f20ac6b8
         A: hmac-md5  245e4944 f9b7d574 ba920299 3d728001
         seq=0x00000000 replay=4 flags=0x00000000 state=mature
         created: May  5 15:25:36 2015   current: May  5 15:38:42 2015
         diff: 786(s)    hard: 86400(s)  soft: 69120(s)
         last: May  5 15:25:45 2015      hard: 0(s)      soft: 0(s)
         current: 11548(bytes)   hard: 0(bytes)  soft: 0(bytes)
         allocated: 152  hard: 0 soft: 0
         sadb _ seq=1 pid=7567 refcnt=0
80.74.102.38[4500] 10.168.9.93[4500]
         esp-udp mode=transport spi=81643941(0x04ddc9a5) reqid=0(0x00000000)
```

```
        E: 3des-cbc  e0d98c2e d34f30d9 1df9544c 45147ae1 27e7aa38 f06994c3
        A: hmac-md5  610ed4cd edd50ea7 191d108e 4f11457c
        seq=0x00000000 replay=4 flags=0x00000000 state=mature
        created: May  5 15:25:36 2015   current: May  5 15:38:42 2015
        diff: 786(s)    hard: 86400(s)  soft: 69120(s)
        last: May  5 15:25:58 2015      hard: 0(s)      soft: 0(s)
        current: 129799(bytes)  hard: 0(bytes)  soft: 0(bytes)
        allocated: 621  hard: 0 soft: 0
        sadb _ seq=0 pid=7567 refcnt=0
```

4. Check the tunnel settings at the spoke

```
[/] l2-vpn tunnel show
    name                  remote       idx      ucastrx    ucasttx    mcastrx    mcasttx
err
   access                   N/A          4         75         69          1        554
0
   nhrpSpoke        80.74.102.38       13         69         75        554          1
0
Total: 2 interfaces
MAC learning is disabled
Tunnel Spanning Tree Mode is set to : normal
Tunnel ICMP send-fragmentation-needed is set to : enabled

[/] l2-vpn nhrp spoke show
+--------------+-------------+
| private ip   |  remote ip  |
+==============+=============+
| 192.168.10.202 | 80.74.102.38  |
+--------------+-------------+
```

5. Verify the tunnel is established at the hub

```
[/]   l2-vpn nhrp hub show
+--------------+---------------+
| private ip   |   remote ip   |
+==============+===============+
| 192.168.10.202 | 2.54.0.232    |
+--------------+---------------+
```

6. Check pinging between the GCE interfaces

```
Hub# ping 192.168.10.102
Reply Received From :192.168.10.102, TimeTaken : 243 msecs
Reply Received From :192.168.10.102, TimeTaken : 123 msecs
Reply Received From :192.168.10.102, TimeTaken : 117 msecs
```

Adding Terminal server service

Spoke

1. Create the serial port and terminal server service

```
application connect
serial port create slot 1 port 1 baudrate 9600 parity no stopbits 1 mode-of-operation
transparent
serial local-end-point create slot 1 port 1 service-id 1  application terminal-server
```

2. Create the terminal server service

```
terminal-server admin-status enable
terminal-server tcp-service create service-id 1 remote-address 192.168.10.202 telnet-port
2050
```

Testing the setup

1. From the IP station at the hub (.251) verify ping connectivity to the spoke ACE vlan 10 interface (used for terminal server).

```
C:\Users>ping 192.168.10.202

Pinging 192.168.10.202 with 32 bytes of data:
Reply from 192.168.10.202: bytes=32 time=1915ms TTL=64
Reply from 192.168.10.202: bytes=32 time=134ms TTL=64
Reply from 192.168.10.202: bytes=32 time=118ms TTL=64
```

2. Open telnet session with port 2050 towards the terminal server (spoke ACE vlan 10 interface). The connected serial device should reply.

3. Verify the telnet connection state

```
[/] terminal-server connections show
+---------+--------------+---------------+---------------+---------------+
| service |    telnet    |     telnet    |  client's IP  | client's port |
|   id    | server's port |  server's IP  |               |               |
+=========+==============+===============+===============+===============+
|    1    |     2050     | 192.168.10.202 | 192.168.10.251 |     64530     |
+---------+--------------+---------------+---------------+---------------+
```

Adding an IEC 101/104 service

Spoke

1. Create the serial port and gateway service

```
application connect
serial port create slot 1 port 2 baudrate 9600 parity even  stopbits 1 mode-of-operation transparent
serial local-end-point create slot 1 port 2 service-id 2 application iec101-gw
```

2. Set the gateway IEC 104 properties

```
iec101-gw  config gw update mode balanced ip _ addr 192.168.10.202
```

3. Configure the gateway IEC 101 properties to be in line with the IEC101 RTU settings.

```
iec101-gw config iec101 create slot 1 port 2 asdu _ addr 3 orig _ addr 0 link _ addr 1 link _ addr 10 link _ address _ field _ length 2 common _ address _ field _ length 2  ioa _ len 3 orig _ addr _ participate y
```

Testing the setup

1. From the IP station at the hub (.251) verify ping connectivity to the spoke ACE vlan 10 interface (used for terminal server).

```
C:\Users>ping 192.168.10.202

Pinging 192.168.10.202 with 32 bytes of data:
Reply from 192.168.10.202: bytes=32 time=1915ms TTL=64
Reply from 192.168.10.202: bytes=32 time=134ms TTL=64
Reply from 192.168.10.202: bytes=32 time=118ms TTL=64
```

2. Open IEC 104 session from the IEC104 Client (the IP station at the hub) towards the gateway (the spoke vlan 10 ACE interface).

3. Verify the connection state

```
[/] iec101-gw show all
101-104 ROUTER
BALANCED MODE
IEC 104:
+---------------+-----------+-----------+----------+----+----+----+----+
|        IP     | ORIG. ADDR | CLOCK SYNC | TIME TAG | T0 | T1 | T2 | T3 |
+===============+============+============+==========+====+====+====+====+
```

```
| 192.168.10.202 |      0       |      n       |     n    | 30 | 15 | 10 | 20 |
| 192.168.10.251 |      0       |      n       |     n    | 30 | 15 | 10 | 20 |
+----------------+--------------+--------------+----------+----+----+----+----+

IEC 101:
+------+------+-------+----------+---------+-------------+----------+---------+---------+----
| SLOT | PORT | OP ST | LINK ADR | CMN ADR | CONV CMN ADR | LINK LEN | CMN LEN | COT
LEN | IOA LEN |
+======+======+=======+==========+=========+==============+==========+=========+========
|  1   |  2   |  UP   |    1     |    3    |      0       |    2     |    2    |
2    |    3    |
+------+------+-------+----------+---------+-------------+----------+---------+---------+----
+------+------+-----------+------+---------+---------+---------+----------+---------+---------
| SLOT | PORT | ORIG. ADR | S CH | DIR BIT | TEST FR | GEN INT | TIME TAG | COT LEN |
IOA LEN | CMN (UB) | LINK (UB) |
+======+======+===========+======+=========+=========+=========+==========+=========+===
|  1   |  2   |    0      |  y   |  AUTO   |    y    |    n    |    n     |    2    |
3   |  3   |     1     |
+------+------+-----------+------+---------+---------+---------+----------+---------+---------
```

Adding serial tunneling service

Hub

1. Create the serial port and transparent serial tunneling service

```
application connect
serial port create slot 1 port 3 mode-of-operation transparent
serial local-end-point create slot 1 port 3 service-id 3 application serial-tunnel
position local
serial remote-end-point create remote-address 192.168.10.202 service-id 3  position remote
exit
write startup-cfg
```

Spoke

2. Create the serial port and transparent serial tunneling service

```
application connect
serial port create slot 1 port 3 baudrate 9600 parity no  stopbits 1 mode-of-operation
transparent
serial local-end-point create slot 1 port 3 service-id 3 position remote application
serial-tunnel
serial remote-end-point create service-id 3 remote-address 192.168.10.201 position local
```

```
connection-mode udp buffer-mode byte
exit
write startup-cfg
```

Testing the setup

1. Verify connectivity between the hub and spoke ACE interfaces 192.168.10.x. From hub:

```
[/] ping 192.168.10.202
PING 192.168.10.202 (192.168.10.202): 56 data bytes
64 bytes from 192.168.10.202: seq=0 ttl=64 time=137.089 ms
64 bytes from 192.168.10.202: seq=1 ttl=64 time=174.828 ms
64 bytes from 192.168.10.202: seq=2 ttl=64 time=160.599 ms
```

2. Initiate traffic between the serial devices (hub local device at serial port 3, spoke remote device at serial port 3).

3. Verify the serial counters at hub and spoke

```
[/]serial port show port 3 briefly
+-----+------+------+-----+-------------+------+------+--------+------+
| idx | slot | port | svc |     mode      | baud | data | parity | stop |
|     |      |      | id  |               | rate | bits |        | bits |
+=====+======+======+=====+=============+======+======+========+======+
|  1  |  1   |  3   |  3  | Transparent | 9600 |  8   |  None  |  1   |
+-----+------+------+-----+-------------+------+------+--------+------+
OctetsIn      : 52
OctetsOut     : 52
TxError       : 0
RxError       : 0
OctetsTotal   : 99
```

DM-VPN over Cellular Setup

Below network demonstrates a Spoke – Hub topology.

Implementation concepts:

1. The spoke will retrieve via PPP an IP from the cellular ISP. In below example the valid IP 212.8.101.10 was issued to the Spoke from the ISP "Cellcom".
2. At the Hub side, a static, Public address should be assigned to the switch application interface. In below example the hub is located behind a NAT router. The NAT, holding a public address 80.74.102.38 should route all traffic designated to it to the application interface of the hub 172.18.212.230.
3. As the hub is located behind a NAT router, a default gateway should be assigned at the application interface (172.18.212.100).
4. As this is layer 3 service, the users behind the spoke and hub are in different vlans and different subnets.
5. Routing the users (SCADA & PC) IP traffic is done by creating ip interfaces in the application. For each user subnet (using unique vlan), an ip interface will be created in the application in the same subnet and will be called ETH1.<vlan id>. in below example at the spoke: PC subnet is on vlan 40 and subnet 192.168.40.x. port gigabitethernet 0/3 must be tagged at vlan 40. ip interface 192.168.40.10 is created and is called ETH1.40. This interface will route the user traffic towards the network.
6. At both the spokes and the hub, private ip interfaces for the tunnel end point will be created. See interfaces of 10.10.10.x in below example
7. IPSec must be configured to ensure secure traffic and proper NAT traversal.
8. Ip connectivity is established between the user stations (SCADA & PC) 192.168.10.11 and 192.168.40.11.
9. At the second part of the example a terminal server service is configured between 192.168.10.11 and the serial device connected at RS-232 port 1 of the spoke.
10. At the third part of the example a transparent serial tunneling service is configured between the SCADA (connected via its com port to the switch RS-232 port 4 at the hub) and the serial device connected at the spoke (RS-232 port 4).

Network drawing

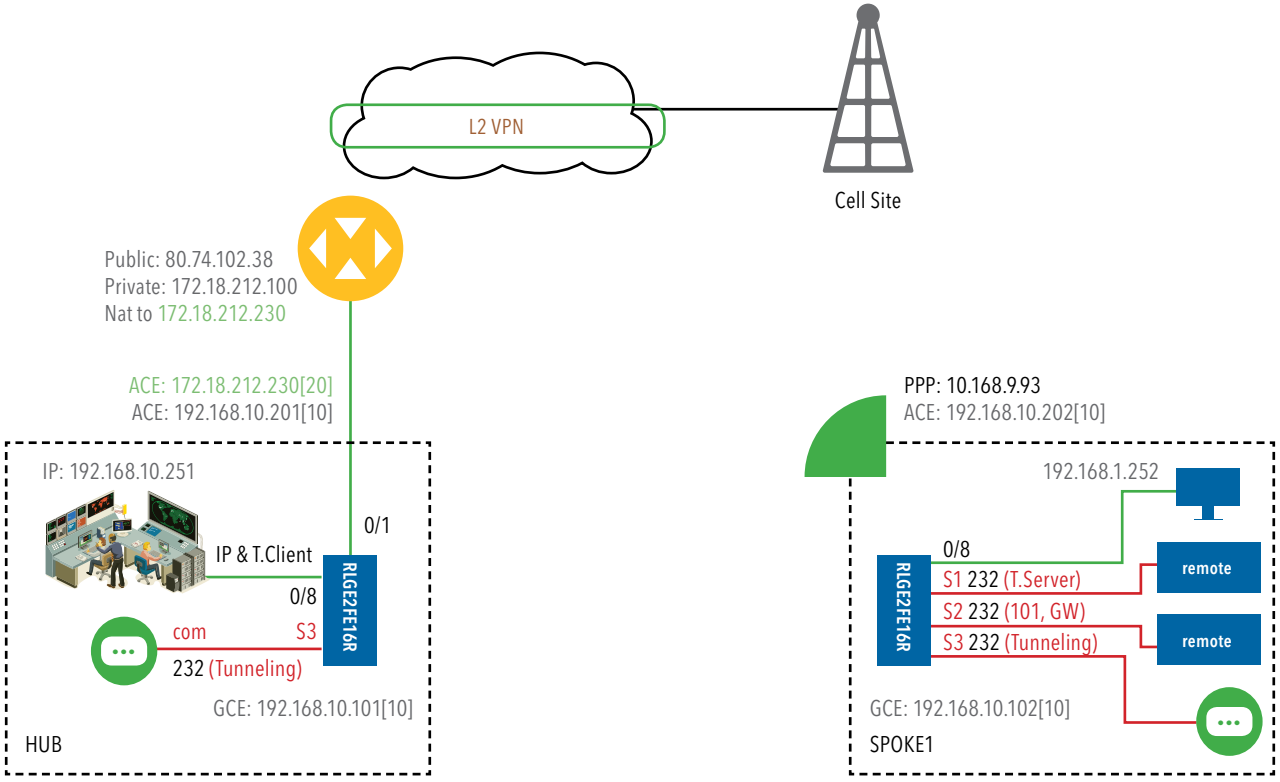


Figure 13 : L3 VPN, cellular spoke - RLGE2FE16R hub

Configuration

Spoke

1. Create vlan UNI 40 to direct traffic from the PC to the application. port gigabitethernet 0/3 must be a tagged member at this vlan. Interface 192.168.40.1 will allow management to the switch over this vlan via the tunnel.

```
set host-name spoke
config terminal
vlan 40
 ports fastethernet 0/1  gigabitethernet 0/3 untagged fastethernet 0/1
 exit
 interface fastethernet 0/1
 description UNI
 switchport pvid 40
 exit
 interface vlan 40
 shutdown
 ip address 192.168.40.1 255.255.255.0
 no shut
 exit
 ip route 0.0.0.0 0.0.0.0 192.168.40.10 1
 end
write startup-cfg
```

2. Set the cellular configuration and SIM settings

```
application connect
cellular settings update default-route yes
cellular wan update sim-slot 1 admin-status enable operator-name cellcom apn-name
internetg user-name guest password guest
cellular enable
```

3. Create an ip interface ETH1.40 to route user subnet 192.168.40.x/24

```
[/] router interface create address-prefix 192.168.40.10/24 vlan 40 purpose application-host
```

4. Create an mGRE private interface for tunnel end. This interface will use the PPP of the cellular as its lower layer.

```
[/]vpn gre tunnel create address-prefix 10.10.10.20/24 lower-layer-dev ppp0 name mgre1 key
10.0.0.0
```

5. Describe the tunnel remote end private interface behind the hub public address.

```
[/]vpn gre nhrp map create multipoint-gre-name mgre1 protocol-address-prefix 10.10.10.10/24
nbma-address 80.74.102.38
```

6. Describe the tunnel remote end private interface behind the hub public address.

```
[/]vpn gre nhrp enable
```

7. assign static route to the remote user subnet behind the hub via the tunnel remote end

```
[/]router static
enable
configure terminal
ip route 192.168.10.0/24 10.10.10.10
write
exit
exit
```

8. IPSec configuration

```
RLGE2FE16R#application connect
ipsec isakmp update my-id RTU1.ComNet.com
ipsec preshared create id HUB.ComNet.com key secretkey
ipsec preshared create id RTU1.ComNet.com key secretkey
ipsec isakmp update id-type fqdn
ipsec policy create protocol gre
ipsec disable
ipsec enable
exit
```

Hub

1. Create vlan UNI 10 to direct traffic from the PC to the application. Port gigabitethernet 0/3 must be a tagged member at this vlan. Interface 192.168.10.1 will allow management to the switch over this vlan via the tunnel. vlan 20 will be towards the router.

```
set host-name hub
config terminal
vlan 10
 ports fastethernet 0/1  gigabitethernet 0/3 untagged fastethernet 0/1
 exit
 vlan 20
 ports fastethernet 0/8  gigabitethernet 0/3 untagged fastethernet 0/8
 exit
 interface fastethernet 0/1
 description UNI
 switchport pvid 10
 exit
 interface fastethernet 0/8
 alias NNI
 switchport pvid 20
 exit
 interface vlan 10
 shutdown
 ip address 192.168.10.1 255.255.255.0
 no shut
 exit
  ip route 0.0.0.0 0.0.0.0 192.168.10.10 1
   end
write startup-cfg
```

2. Create an IP interface ETH.20 in the subnet of the router

```
[/]router interface create address-prefix 172.18.212.230/24 vlan 20 purpose application-host
[/]
```

3. Create an ip interface ETH.10 to route user subnet 192.168.10.x/24

```
[/]router interface create address-prefix 192.168.10.10/24 vlan 10 purpose general
```

4. Create an mgre private interface for tunnel end. This interface will use the interface ETH.20 of towards the router as its lower layer.

```
[/]vpn gre tunnel create address-prefix 10.10.10.10/24 lower-layer-dev eth1.20 name mgre1
key 10.0.0.0 holding-time 120
```

5. Enable nhrp

```
[/]vpn gre nhrp enable
```

6. Assign static route to the remote user subnet 192.168.40.x behind the spoke via the tunnel remote end 10.10.10.20

```
[/]router static
enable
configure terminal
ip route 192.168.40.0/24 10.10.10.20
ip route 0.0.0.0/0  172.18.212.100
write
exit
exit
```

7. IPSec configuration

```
application connect
ipsec isakmp update my-id HUB.ComNet.com
ipsec preshared create id HUB.ComNet.com key secretkey
ipsec preshared create id RTU1.ComNet.com key secretkey
ipsec isakmp update id-type fqdn
ipsec policy create protocol gre
ipsec disable
ipsec enable
exit
```

Testing the setup

1. Use show commands to check configuration

2. Spoke

```
RLGE2FE16R(spoke)#Show vlan
[]router interface show
[]cellular show
[]cellular wan show
[]cellular Connection show
[]ipsec show
```

3. Hub

```
3700(hub)#Show vlan
[]router interface show
```

4. Make sure both the IP of the hub and the one of the spoke are each accessible from the internet. Using a PC connected to the internet send ping commands. Ping 'public ip of the spoke'.

```
ping 80.74.102.38.
```

5. Send traffic between the SCADA and RTU.

Adding a terminal server service

Spoke

1. Create the serial port

```
application connect
serial port create slot 1 port 1
serial local-end-point create slot 1 port 1 service-id 1 application terminal-server
```

2. Create the terminal server service

```
Application connect


terminal-server admin-status enable
terminal-server telnet-service create service-id 1 telnet-port 2050 remote-address
192.168.40.10
```

Testing the setup

1. From the hub station 192.168.10.11 ping to the remote application interface 192.168.40.10.

2. Open a telnet session towards address 192.168.40.10 with port 2050.

3. The serial port will respond

Adding a transparent serial tunneling service

Hub

1. Create the serial port and transparent serial tunneling service

```
application connect
[]serial port create slot 1 port 4 mode-of-operation transparent
[]serial local-end-point create slot 1 port 4 service-id 2 application
  serial-tunnel position local
[]serial remote-end-point create remote-address 192.168.40.10 service-id 2
  position remote
```

Spoke

2. Create the serial port and transparent serial tunneling service

```
application connect
[]serial port create slot 1 port 4 mode-of-operation transparent
[]serial local-end-point create slot 1 port 4 service-id 2 application
  serial-tunnel position remote
[]serial remote-end-point create remote-address 192.168.10.10 service-id 2
  position local
```

Testing the setup:

From the SCADA send serial traffic over its COM port. The remote serial device at the spoke will respond.

ComNet Customer Service
Customer Care is ComNet Technology's global service center, where our professional staff is ready to answer your questions at any time.
Email ComNet Global Service Center: customercare@comnet.net

comnet
Communication Networks

3 CORPORATE DRIVE | DANBURY, CT 06810 | USA
T: 203.796.5300 | F: 203.796.5303 | TECH SUPPORT: 1.888.678.9427 | INFO@COMNET.NET
8 TURNBERRY PARK ROAD | GILDERSOME | MORLEY | LEEDS, UK LS27 7LE
T: +44 (0)113 307 6400 | F: +44 (0)113 253 7462 | INFO-EUROPE@COMNET.NET

© 2016 Communications Networks Corporation. All Rights Reserved. "ComNet" and the "ComNet Logo" are registered trademarks of Communication Networks, LLC.