ISG50

CLI Reference Guide

Version 2.30
5/2012
Edition 3

DEFAULT LOGIN	
User Name	**admin**
Password	**1234**

ZyXEL

www.zyxel.com

About This CLI Reference Guide

Intended Audience

This manual is intended for people who want to configure the ISG50 via Command Line Interface (CLI). You should have at least a basic knowledge of TCP/IP networking concepts and topology. Generally, it is organized by feature as outlined in the web configurator.

Note: This guide is intended as a command reference for a series of products. Therefore many commands or command options in this guide may not be available in your product. See your User's Guide for a list of supported features and details about feature implementation.

Please refer to www.zyxel.com or your product's CD for product specific User Guides and product certifications.

How To Use This Guide

1 Read Chapter 1 on page 19 for how to access and use the CLI (Command Line Interface).

2 Read Chapter 2 on page 33 to learn about the CLI user and privilege modes.

3 Subsequent chapters are arranged by menu item as defined in the web configurator. Read each chapter carefully for detailed information on that menu item.

Note: Some features cannot be configured in both the web configurator and CLI.

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this User's Guide.

Warnings tell you about things that could harm you or your device.

Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The ISG50 may be referred to as the "ISG50", the "device", the "system" or the "product" in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".

Icons Used in Figures

Figures in this User's Guide may use the following generic icons. The ISG50 icon is not an exact representation of your device.

ISG50 	Computer 	Notebook computer 
Server 	Firewall 	Telephone 
Switch 	Router 	

Contents Overview

Introduction **17**

Command Line Interface 19
User and Privilege Modes 33

Reference **37**

Object Reference 39
Status 41
Registration 45
Interfaces 51
Trunks 79
Route 85
Routing Protocol 93
Zones 97
DDNS 101
Virtual Servers 105
HTTP Redirect 111
ALG 113
IP/MAC Binding 115
Firewall 117
IPSec VPN 125
PBX 133
User/Group 269
Addresses 277
Services 281
Schedules 285
AAA Server 287
Authentication Objects 294
Certificates 297
ISP Accounts 303
System 307
System Remote Management 314
File Manager 325
Logs 339
Reports and Reboot 345
Session Timeout 351
Diagnostics 353
Packet Flow Explore 355
Maintenance Tools 359

Watchdog Timer 365

Table of Contents

About This CLI Reference Guide 3

Document Conventions 4

Contents Overview 5

Table of Contents 7

Part I: Introduction 17

Chapter 1
Command Line Interface 19

1.1 Overview 19
1.1.1 The Configuration File 19
1.2 Accessing the CLI 19
1.2.1 Console Port 20
1.2.2 Web Configurator Console 20
1.2.3 Telnet 23
1.2.4 SSH (Secure SHell) 23
1.3 How to Find Commands in this Guide 23
1.4 How Commands Are Explained 24
1.4.1 Background Information (Optional) 24
1.4.2 Command Input Values (Optional) 24
1.4.3 Command Summary 24
1.4.4 Command Examples (Optional) 24
1.4.5 Command Syntax 24
1.4.6 Changing the Password 25
1.5 CLI Modes 25
1.6 Shortcuts and Help 26
1.6.1 List of Available Commands 26
1.6.2 List of Sub-commands or Required User Input 27
1.6.3 Entering Partial Commands 27
1.6.4 Entering a ? in a Command 27
1.6.5 Command History 27
1.6.6 Navigation 28
1.6.7 Erase Current Command 28
1.6.8 The no Commands 28
1.7 Input Values 28
1.8 Ethernet Interfaces 31

1.9 Saving Configuration Changes 31
1.10 Logging Out 31

Chapter 2
User and Privilege Modes 33

2.1 User And Privilege Modes 33
2.1.1 Debug Commands 34

Part II: Reference 37

Chapter 3
Object Reference 39

3.1 Object Reference Commands 39
3.1.1 Object Reference Command Example 40

Chapter 4
Status 41

Chapter 5
Registration 45

5.1 myZyXEL.com overview 45
5.2 Registration Commands 45
5.2.1 Command Examples 46
5.3 Country Code 47

Chapter 6
Interfaces 51

6.1 Interface Overview 51
6.1.1 Types of Interfaces 51
6.1.2 Relationships Between Interfaces 53
6.2 Interface General Commands Summary 54
6.2.1 Basic Interface Properties and IP Address Commands 54
6.2.2 DHCP Setting Commands 57
6.2.3 Interface Parameter Command Examples 61
6.2.4 RIP Commands 61
6.2.5 OSPF Commands 62
6.2.6 Connectivity Check (Ping-check) Commands 64
6.3 Ethernet Interface Specific Commands 65
6.3.1 MAC Address Setting Commands 65
6.3.2 Port Grouping Commands 66
6.4 Virtual Interface Specific Commands 67
6.4.1 Virtual Interface Command Examples 68

6.5 PPPoE/PPTP Specific Commands 68
6.5.1 PPPoE/PPTP Interface Command Examples 69
6.6 Cellular Interface Specific Commands 69
6.6.1 Cellular Status 72
6.6.2 Cellular Interface Command Examples 74
6.7 USB Storage Specific Commands 75
6.7.1 USB Storage General Commands Example 76
6.8 VLAN Interface Specific Commands 76
6.8.1 VLAN Interface Command Examples 77
6.9 Bridge Specific Commands 77
6.9.1 Bridge Interface Command Examples 78

Chapter 7
Trunks 79

7.1 Trunks Overview 79
7.2 Trunk Scenario Examples 79
7.3 Trunk Commands Input Values 80
7.4 Trunk Commands Summary 80
7.5 Trunk Command Examples 81
7.6 Link Sticking Commands Summary 83
7.7 Link Sticking Command Example 84

Chapter 8
Route 85

8.1 Policy Route 85
8.2 Policy Route Commands 85
8.2.1 Assured Forwarding (AF) PHB for DiffServ 88
8.2.2 Policy Route Command Example 89
8.3 IP Static Route 90
8.4 Static Route Commands 90
8.4.1 Static Route Commands Example 91

Chapter 9
Routing Protocol 93

9.1 Routing Protocol Overview 93
9.2 Routing Protocol Commands Summary 93
9.2.1 RIP Commands 94
9.2.2 General OSPF Commands 94
9.2.3 OSPF Area Commands 95
9.2.4 Virtual Link Commands 95
9.2.5 Learned Routing Information Commands 96
9.2.6 show ip route Command Example 96

Chapter 10
Zones 97

10.1 Zones Overview 97
10.2 Zone Commands Summary 98
10.2.1 Zone Command Examples 99

Chapter 11
DDNS 101

11.1 DDNS Overview 101
11.2 DDNS Commands Summary 102

Chapter 12
Virtual Servers 105

12.1 Virtual Server Overview 105
12.1.1 1:1 NAT and Many 1:1 NAT 105
12.2 Virtual Server Commands Summary 105
12.2.1 Virtual Server Command Examples 108
12.2.2 Tutorial - How to Allow Public Access to a Server 108

Chapter 13
HTTP Redirect 111

13.1 HTTP Redirect Overview 111
13.1.1 Web Proxy Server 111
13.2 HTTP Redirect Commands 111
13.2.1 HTTP Redirect Command Examples 112

Chapter 14
ALG 113

14.1 ALG Introduction 113
14.2 ALG Commands 114
14.3 ALG Commands Example 114

Chapter 15
IP/MAC Binding 115

15.1 IP/MAC Binding Overview 115
15.2 IP/MAC Binding Commands 115
15.3 IP/MAC Binding Commands Example 116

Chapter 16
Firewall 117

16.1 Firewall Overview 117
16.2 Firewall Commands 118
16.2.1 Firewall Sub-Commands 120

16.2.2 Firewall Command Examples 121
16.3 Session Limit Commands 122

Chapter 17
IPSec VPN 125

17.1 IPSec VPN Overview 125
17.2 IPSec VPN Commands Summary 126
17.2.1 IKE SA Commands 127
17.2.2 IPSec SA Commands (except Manual Keys) 129
17.2.3 IPSec SA Commands (for Manual Keys) 131
17.2.4 VPN Concentrator Commands 131
17.2.5 SA Monitor Commands 132

Chapter 18
PBX 133

18.1 PBX Overview 133
18.2 PBX Brute Force Attack Prevention Commands 134
18.2.1 PBX Brute Force Attack Prevention Command Examples 134
18.3 PBX Monitor Commands 135
18.3.1 PBX Monitor Command Examples 135
18.4 PBX CDR Commands 136
18.4.1 PBX CDR Command Examples 138
18.5 Global PBX Commands 140
18.5.1 Global PBX Command Examples 141
18.6 Feature Code PBX Commands 142
18.6.1 Feature Code PBX Command Examples 143
18.7 E-mail PBX Commands 144
18.7.1 E-mail PBX Command Examples 145
18.8 QoS PBX Commands 146
18.8.1 QoS PBX Command Examples 146
18.9 Voice Interface Commands 147
18.9.1 PSTN Voice Interface Commands 147
18.9.2 PSTN Voice Interface Command Examples 148
18.9.3 ISDN Voice Interface Commands 149
18.9.4 ISDN Voice Interface Command Examples 150
18.10 Extension Management Commands 151
18.10.1 Authority Group Commands 151
18.10.2 Authority Group Command Examples 152
18.10.3 Authority TAPI Commands 153
18.10.4 Authority TAPI Command Examples 154
18.10.5 PBX Extension Commands 155
18.10.6 PBX Extension Command Examples 158
18.11 Group Access Code Commands 176

18.11.1 Group Access Code Command Examples 176
18.12 Click To Talk Commands 177
18.12.1 Click To Talk Command Examples 178
18.13 Outbound Line Management Commands 179
18.13.1 SIP Trunk and Trusted Peer Commands 179
18.13.2 SIP Trunk and Trusted Peer Command Examples 185
18.13.3 FXO Commands 188
18.13.4 FXO Command Examples 189
18.13.5 BRI Commands 190
18.13.6 BRI Command Examples 192
18.14 Auto Attendant Commands 194
18.14.1 Auto Attendant Command Examples 200
18.15 LCR Commands 213
18.15.1 LCR Command Examples 214
18.16 Group Management Commands 216
18.16.1 Group Management Command Examples 217
18.17 Call Service Commands 218
18.17.1 Call Service Command Examples 221
18.18 Call Recording Commands 227
18.18.1 Call Recording Command Examples 228
18.19 Meet-me Conference Commands 229
18.19.1 Meet-me Conference Command Examples 230
18.20 Paging Group Commands 231
18.20.1 Paging Group Command Examples 232
18.21 ACD Commands 233
18.21.1 ACD Command Examples 238
18.22 Sound File Commands 243
18.22.1 Sound File Command Examples 243
18.23 Auto Provision Commands 244
18.23.1 Auto Provision Command Examples 246
18.24 Voice Mail Configuration Commands 246
18.24.1 Voice Mail Configuration Command Examples 247
18.25 Phonebook Commands 248
18.25.1 Phonebook Command Examples 251
18.26 Office Hour Commands 254
18.26.1 Office Hour Command Examples 255
18.27 PBX Diagnostics Commands 259
18.27.1 PBX Diagnostics Command Examples 259

Chapter 19
User/Group 269

19.1 User Account Overview 269
19.1.1 User Types 269

19.2 User/Group Commands Summary 270
19.2.1 User Commands 270
19.2.2 User Group Commands 271
19.2.3 User Setting Commands 271
19.2.4 Force User Authentication Commands 273
19.2.5 Additional User Commands 275

Chapter 20
Addresses 277

20.1 Address Overview 277
20.2 Address Commands Summary 277
20.2.1 Address Object Commands 278
20.2.2 Address Group Commands 279

Chapter 21
Services 281

21.1 Services Overview 281
21.2 Services Commands Summary 281
21.2.1 Service Object Commands 281
21.2.2 Service Group Commands 282

Chapter 22
Schedules 285

22.1 Schedule Overview 285
22.2 Schedule Commands Summary 285
22.2.1 Schedule Command Examples 286

Chapter 23
AAA Server 287

23.1 AAA Server Overview 287
23.2 Authentication Server Command Summary 287
23.2.1 ad-server Commands 287
23.2.2 ldap-server Commands 288
23.2.3 radius-server Commands 289
23.2.4 radius-server Command Example 289
23.2.5 aaa group server ad Commands 289
23.2.6 aaa group server ldap Commands 291
23.2.7 aaa group server radius Commands 292
23.2.8 aaa group server Command Example 293

Chapter 24
Authentication Objects 294

24.1 Authentication Objects Overview 294

24.2 aaa authentication Commands 294
24.2.1 aaa authentication Command Example 295
24.3 test aaa Command 296
24.3.1 Test a User Account Command Example 296

Chapter 25
Certificates 297

25.1 Certificates Overview 297
25.2 Certificate Commands 297
25.3 Certificates Commands Input Values 297
25.4 Certificates Commands Summary 298
25.5 Certificates Commands Examples 301

Chapter 26
ISP Accounts 303

26.1 ISP Accounts Overview 303
26.1.1 PPPoE and PPTP Account Commands 303
26.1.2 Cellular Account Commands 304

Chapter 27
System 307

27.1 System Overview 307
27.2 Customizing the WWW Login Page 307
27.3 Host Name Commands 310
27.4 Time and Date 310
27.4.1 Date/Time Commands 310
27.5 Console Port Speed 311
27.6 DNS Overview 311
27.6.1 Domain Zone Forwarder 311
27.6.2 DNS Commands 312
27.6.3 DNS Command Example 313
27.7 SNAT Overview 313

Chapter 28
System Remote Management 314

28.1 Remote Management Overview 314
28.1.1 Remote Management Limitations 314
28.1.2 System Timeout 314
28.2 Common System Command Input Values 315
28.3 HTTP/HTTPS Commands 315
28.3.1 HTTP/HTTPS Command Examples 317
28.4 SSH 317
28.4.1 SSH Implementation on the ISG50 317

28.4.2 Requirements for Using SSH 317
28.4.3 SSH Commands 318
28.4.4 SSH Command Examples 318
28.5 Telnet 319
28.6 Telnet Commands 319
28.6.1 Telnet Commands Examples 319
28.7 Configuring FTP 320
28.7.1 FTP Commands 320
28.7.2 FTP Commands Examples 321
28.8 SNMP 321
28.8.1 Supported MIBs 321
28.8.2 SNMP Traps 321
28.8.3 SNMP Commands 322
28.8.4 SNMP Commands Examples 323
28.9 ICMP Filter 323
28.10 Language Commands 324

Chapter 29
File Manager 325

29.1 File Directories 325
29.2 Configuration Files and Shell Scripts Overview 325
29.2.1 Comments in Configuration Files or Shell Scripts 326
29.2.2 Errors in Configuration Files or Shell Scripts 327
29.2.3 ISG50 Configuration File Details 327
29.2.4 Configuration File Flow at Restart 328
29.3 File Manager Commands Input Values 328
29.4 File Manager Commands Summary 329
29.5 File Manager Command Example 330
29.6 FTP File Transfer 330
29.6.1 Command Line FTP File Upload 330
29.6.2 Command Line FTP Configuration File Upload Example 331
29.6.3 Command Line FTP File Download 331
29.6.4 Command Line FTP Configuration File Download Example 332
29.7 ISG50 File Usage at Startup 332
29.8 Notification of a Damaged Recovery Image or Firmware 333
29.9 Restoring the Recovery Image 334
29.10 Restoring the Firmware 336

Chapter 30
Logs 339

30.1 Log Commands Summary 339
30.1.1 Log Entries Commands 339
30.1.2 System Log Commands 340

30.1.3 Debug Log Commands 341
30.1.4 E-mail Profile Commands 342
30.1.5 Console Port Logging Commands 343

Chapter 31
Reports and Reboot 345

31.1 Report Commands Summary 345
31.1.1 Report Commands 345
31.1.2 Report Command Examples 346
31.1.3 Session Commands 346
31.2 Email Daily Report Commands 347
31.2.1 Email Daily Report Example 348
31.3 Reboot 349

Chapter 32
Session Timeout 351

Chapter 33
Diagnostics 353

33.1 Diagnostics 353
33.2 Diagnosis Commands 353
33.3 Diagnosis Commands Example 353

Chapter 34
Packet Flow Explore 355

34.1 Packet Flow Explore 355
34.2 Packet Flow Explore Commands 355
34.3 Packet Flow Explore Commands Example 356

Chapter 35
Maintenance Tools 359

35.0.1 Command Examples 361

Chapter 36
Watchdog Timer 365

36.1 Hardware Watchdog Timer 365
36.2 Software Watchdog Timer 365
36.3 Application Watchdog 366
36.3.1 Application Watchdog Commands Example 367

List of Commands (Alphabetical) 369

PART I
Introduction

1

Command Line Interface

This chapter describes how to access and use the CLI (Command Line Interface).

Note: This guide covers the configuration commands. See the User's Guide for background information on features.

1.1 Overview

If you have problems with your ISG50, customer support may request that you issue some of these commands to assist them in troubleshooting.

Use of undocumented commands or misconfiguration can damage the ISG50 and possibly render it unusable.

1.1.1 The Configuration File

When you configure the ISG50 using either the CLI (Command Line Interface) or the web configurator, the settings are saved as a series of commands in a configuration file on the ISG50. You can store more than one configuration file on the ISG50. However, only one configuration file is used at a time.

You can perform the following with a configuration file:

- Back up ISG50 configuration once the ISG50 is set up to work in your network.
- Restore ISG50 configuration.
- Save and edit a configuration file and upload it to multiple ISG50s (of the same model) in your network to have the same settings.

Note: You may also edit a configuration file using a text editor.

1.2 Accessing the CLI

You can access the CLI using a terminal emulation program on a computer connected to the console port, from the web configurator or access the ISG50 using Telnet or SSH (Secure SHell).

Note: The ISG50 might force you to log out of your session if reauthentication time, lease time, or idle timeout is reached. See Chapter 19 on page 269 for more information about these settings.

1.2.1 Console Port

The default settings for the console port are as follows.

Table 1 Managing the ISG50: Console Port

SETTING	VALUE
Speed	115200 bps
Data Bits	8
Parity	None
Stop Bit	1
Flow Control	Off

When you turn on your ISG50, it performs several internal tests as well as line initialization. You can view the initialization information using the console port.

- Garbled text displays if your terminal emulation program's speed is set lower than the ISG50's.
- No text displays if the speed is set higher than the ISG50's.
- If changing your terminal emulation program's speed does not get anything to display, restart the ISG50.
- If restarting the ISG50 does not get anything to display, contact your local customer support.

Figure 1 Console Port Power-on Display

```
FLASH: AMD 16M
product: ISG

BootModule Version: V1.12 | 05/17/2010 16:58:00
DRAM: Size = 512 Mbytes
```

After the initialization, the login screen displays.

Figure 2 Login Screen

```
Welcome to ISG50-PSTN

Username:
```

Enter the user name and password at the prompts.

Note: The default login username is **admin** and password is **1234**. The username and password are case-sensitive.

1.2.2 Web Configurator Console

Note: Before you can access the CLI through the web configurator, make sure your computer supports the Java Runtime Environment. You will be prompted to download and install the Java plug-in if it is not already installed.

When you access the CLI using the web console, your computer establishes a SSH (Secure SHell) connection to the ISG50. Follow the steps below to access the web console.

1 Log into the web configurator.

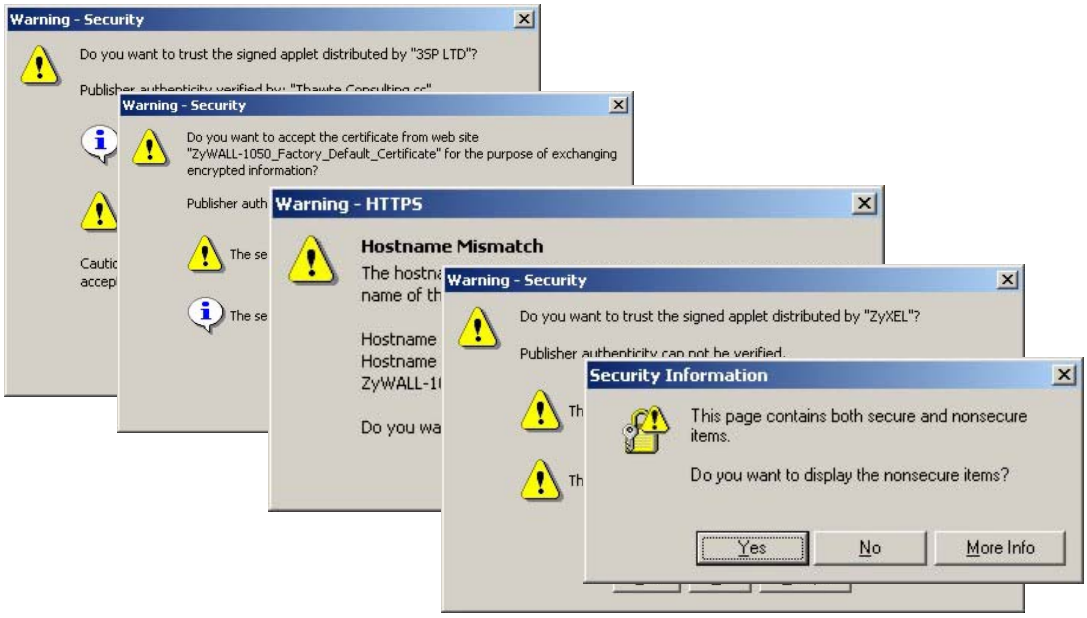
2 Click the **Console** icon in the top-right corner of the web configurator screen.

3 If the Java plug-in is already installed, skip to step 4.

Otherwise, you will be prompted to install the Java plug-in. If the prompt does not display and the screen remains gray, you have to download the setup program.

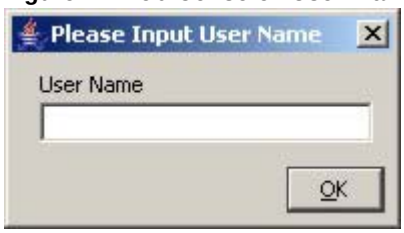
4 The web console starts. This might take a few seconds. One or more security screens may display. Click **Yes** or **Always**.

Figure 3 Web Console: Security Warnings



Finally, the **User Name** screen appears.

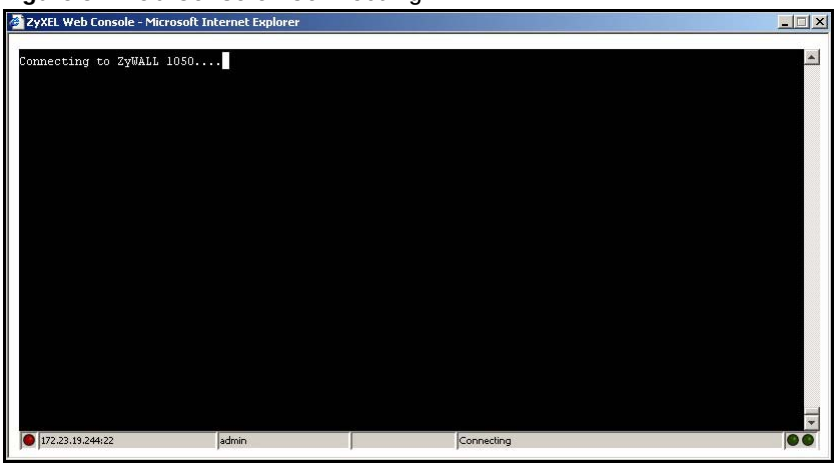
Figure 4 Web Console: User Name



5 Enter the user name you want to use to log in to the console. The console begins to connect to the ISG50.

Note: The default login username is **admin**. It is case-sensitive.

Figure 5 Web Console: Connecting



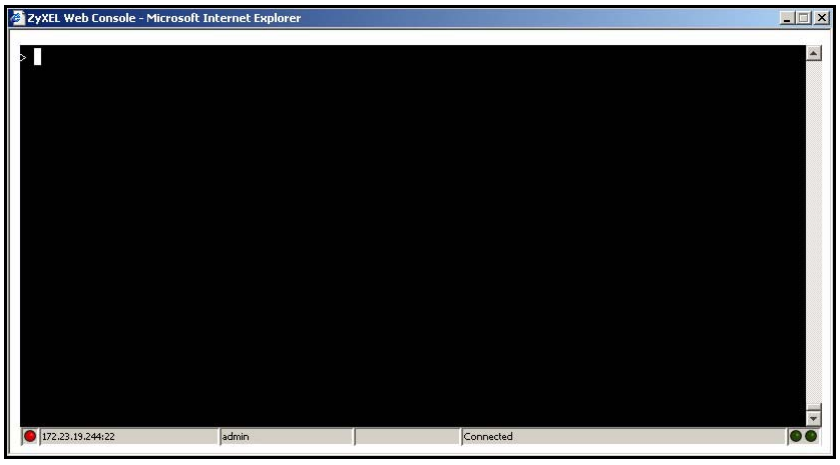
Then, the **Password** screen appears.

Figure 6 Web Console: Password



6 Enter the password for the user name you specified earlier, and click **OK**. If you enter the password incorrectly, you get an error message, and you may have to close the console window and open it again. If you enter the password correctly, the console screen appears.

Figure 7 Web Console



7 To use most commands in this User's Guide, enter `configure terminal`. The prompt should change to `Router(config)#`.

1.2.3 Telnet

Use the following steps to Telnet into your ISG50.

1 If your computer is connected to the ISG50 over the Internet, skip to the next step. Make sure your computer IP address and the ISG50 IP address are on the same subnet.

2 In Windows, click **Start** (usually in the bottom left corner) and **Run**. Then type `telnet` and the ISG50's IP address. For example, enter `telnet 192.168.1.1` (the default management IP address).

3 Click **OK**. A login screen displays. Enter the user name and password at the prompts.

Note: The default login username is **admin** and password is **1234**. The username and password are case-sensitive.

1.2.4 SSH (Secure SHell)

You can use an SSH client program to access the CLI. The following figure shows an example using a text-based SSH client program. Refer to the documentation that comes with your SSH program for information on using it.

Note: The default login username is **admin** and password is **1234**. The username and password are case-sensitive.

Figure 8 SSH Login Example

```
C:\>ssh2 admin@192.168.1.1
Host key not found from database.
Key fingerprint:
xolor-takel-fipef-zevit-visom-gydog-vetan-bisol-lysob-cuvun-muxex
You can get a public key's fingerprint by running
% ssh-keygen -F publickey.pub
on the keyfile.
Are you sure you want to continue connecting (yes/no)? yes

Host key saved to C:/Documents and Settings/user/Application Data/SSH/
hostkeys/
ey_22_192.168.1.1.pub
host key for 192.168.1.1, accepted by user Tue Aug 09 2005 07:38:28
admin's password:
Authentication successful.
```

1.3 How to Find Commands in this Guide

You can simply look for the feature chapter to find commands. In addition, you can use the List of Commands (Alphabetical) at the end of the guide. This section lists the commands in alphabetical order that they appear in this guide.

If you are looking at the CLI Reference Guide electronically, you might have additional options (for example, bookmarks or **Find...**) as well.

1.4 How Commands Are Explained

Each chapter explains the commands for one keyword. The chapters are divided into the following sections.

1.4.1 Background Information (Optional)

Note: See the User's Guide for background information about most features.

This section provides background information about features that you cannot configure in the web configurator. In addition, this section identifies related commands in other chapters.

1.4.2 Command Input Values (Optional)

This section lists common input values for the commands for the feature in one or more tables

1.4.3 Command Summary

This section lists the commands for the feature in one or more tables.

1.4.4 Command Examples (Optional)

This section contains any examples for the commands in this feature.

1.4.5 Command Syntax

The following conventions are used in this User's Guide.

- A command or keyword in courier new must be entered literally as shown. Do not abbreviate.
- Values that you need to provide are in *italics*.
- Required fields that have multiple choices are enclosed in curly brackets {}.
- A range of numbers is enclosed in angle brackets <>.
- Optional fields are enclosed in square brackets [].
- The | symbol means OR.

For example, look at the following command to create a TCP/UDP service object.

```
service-object object-name {tcp | udp} {eq <1..65535> | range <1..65535> <1..65535>}
```

1. Enter service-object exactly as it appears.
2. Enter the name of the object where you see *object-name.*
3. Enter tcp or udp, depending on the service object you want to create.
4. Finally, do one of the following.
   - Enter eq exactly as it appears, followed by a number between 1 and 65535.

- Enter `range` exactly as it appears, followed by two numbers between 1 and 65535.

1.4.6 Changing the Password

It is highly recommended that you change the password for accessing the ISG50. See Section 19.2 on page 270 for the appropriate commands.

1.5 CLI Modes

You run CLI commands in one of several modes.

Table 2 CLI Modes

	USER	PRIVILEGE	CONFIGURATION	SUB-COMMAND
What **Guest** users can do	Unable to access	Unable to access	Unable to access	Unable to access
What **User** users can do	• Look at (but not run) available commands	Unable to access	Unable to access	Unable to access
What **Limited-Admin** users can do	• Look at system information (like **Status** screen) • Run basic diagnostics	• Look at system information (like **Status** screen) • Run basic diagnostics	Unable to access	Unable to access
What **Admin** users can do	• Look at system information (like **Status** screen) • Run basic diagnostics	• Look at system information (like **Status** screen) • Run basic diagnostics	• Configure simple features (such as an address object) • Create or remove complex parts (such as an interface)	• Configure complex parts (such as an interface) in the ISG50
How you enter it	Log in to the ISG50	Type **enable** in **User** mode	Type **configure terminal** in **User** or **Privilege** mode	Type the command used to create the specific part in **Configuration** mode

What the prompt looks like	`Router>`	`Router#`	`Router(config)#`	(varies by part)
				`Router(zone)#`
				`Router(config-if-ge)#`
				`...`

How you exit it	Type **exit**	Type **disable**	Type **exit**	Type **exit**

See Chapter 19 on page 269 for more information about the user types. **User** users can only log in, look at (but not run) the available commands in **User** mode, and log out. **Limited-Admin** users can look at the configuration in the web configurator and CLI, and they can run basic diagnostics in the CLI. **Admin** users can configure the ISG50 in the web configurator or CLI.

At the time of writing, there is not much difference between **User** and **Privilege** mode for admin users. This is reserved for future use.

1.6 Shortcuts and Help

1.6.1 List of Available Commands

A list of valid commands can be found by typing ? or [TAB] at the command prompt. To view a list of available commands within a command group, enter <command> ? or <command> [TAB].

Figure 9 Help: Available Commands Example 1

```
Router> ?
<cr>
apply
atse
clear
configure
------------------[Snip]--------------------
shutdown
telnet
test
traceroute
write
Router>
```

Figure 10 Help: Available Command Example 2

```
Router> show ?
aaa
access-page
account
ad-server
address-object
alg
app
app-watch-dog
apply
arp
arp-table
arpseal
boot
bridge
bwm
ca
clock
comport
conn
connectivity-check
connlimit
console                     Console
corefile
--More--
```

1.6.2 List of Sub-commands or Required User Input

To view detailed help information for a command, enter <command> <sub command> ?.

Figure 11 Help: Sub-command Information Example

```
Router(config)# ip telnet server ?
;
<cr>
port
rule
|
Router(config)# ip telnet server
```

Figure 12 Help: Required User Input Example

```
Router(config)# ip telnet server port ?
<1..65535>
Router(config)# ip telnet server port
```

1.6.3 Entering Partial Commands

The CLI does not accept partial or incomplete commands. You may enter a unique part of a command and press [TAB] to have the ISG50 automatically display the full command.

For example, if you enter **config** and press [TAB] , the full command of **configure** automatically displays.

If you enter a partial command that is not unique and press [TAB], the ISG50 displays a list of commands that start with the partial command.

Figure 13 Non-Unique Partial Command Example

```
Router# c [TAB]
clear      configure  copy
Router# co [TAB]
configure  copy
```

1.6.4 Entering a ? in a Command

Typing a ? (question mark) usually displays help information. However, some commands allow you to input a ?, for example as part of a string. Press [CTRL+V] on your keyboard to enter a ? without the ISG50 treating it as a help query.

1.6.5 Command History

The ISG50 keeps a list of commands you have entered for the current CLI session. You can use any commands in the history again by pressing the up (↑) or down (↓) arrow key to scroll through the previously used commands and press [ENTER].

1.6.6 Navigation

Press [CTRL]+A to move the cursor to the beginning of the line. Press [CTRL]+E to move the cursor to the end of the line.

1.6.7 Erase Current Command

Press [CTRL]+U to erase whatever you have currently typed at the prompt (before pressing [ENTER]).

1.6.8 The no Commands

When entering the no commands discribed in this document, you may not need to type the whole command. For example, with the "[no] mss <536..1452>" command, you use "mss 536" to specify the MSS value. But to disable the MSS setting, you only need to type "no mss" instead of "no mss 536".

1.7 Input Values

You can use the ? or [TAB] to get more information about the next input value that is required for a command. In some cases, the next input value is a string whose length and allowable characters may not be displayed in the screen. For example, in the following example, the next input value is a string called <description>.

```
Router# configure terminal
Router(config)# interface wan1
Router(config-if-wan1)# description
<description>
```

The following table provides more information about input values like <description>.

Table 3 Input-Value Formats for Strings in CLI Commands

TAG	# VALUES	LEGAL VALUES
***	1	*
all	--	ALL
authentication key	Used in IPSec SA	
	32-40 16-20	"0x" or "0X" + 32-40 hexadecimal values alphanumeric or ;|`~!@#$%^&*()_+\\{}':,./<>=-
	Used in MD5 authentication keys for RIP/OSPF and text authentication key for RIP	
	0-16	alphanumeric or _-
	Used in text authentication keys for OSPF	
	0-8	alphanumeric or _-
certificate name	1-31	alphanumeric or ;`~!@#$%^&()_+[\]{}',.=-
community string	0-63	alphanumeric or .- first character: alphanumeric or -

Table 3 Input-Value Formats for Strings in CLI Commands (continued)

TAG	# VALUES	LEGAL VALUES
connection_id	1+	alphanumeric or -_:
contact	1-61	alphanumeric, spaces, or '()+,/:=?;!*#@$_%-.
country code	0 or 2	alphanumeric
custom signature file name	0-30	alphanumeric or _-. first character: letter
description	Used in keyword criteria for log entries	
	1-64	alphanumeric, spaces, or '()+,/:=?;!*#@$_%-.
	Used in other commands	
	1-61	alphanumeric, spaces, or '()+,/:=?;!*#@$_%-
distinguished name	1-511	alphanumeric, spaces, or .@=,_-
domain name	Used in ip dns server	
	0-247	alphanumeric or .- first character: alphanumeric or -
	Used in domainname, ip dhcp pool, and ip domain	
	0-254	alphanumeric or ._- first character: alphanumeric or -
email	1-63	alphanumeric or .@_-
e-mail	1-64	alphanumeric or .@_-
encryption key	16-64 8-32	“0x” or “0X” + 16-64 hexadecimal values alphanumeric or ;|`~!@#$%^&*()_+\\{}':,./<>=-
file name	0-31	alphanumeric or _-
filter extension	1-256	alphanumeric, spaces, or '()+,/:=?;!*#@$_%.-
fqdn	Used in ip dns server	
	0-252	alphanumeric or .- first character: alphanumeric or -
	Used in ip ddns, time server, VPN, certificates, and interface ping check	
	0-254	alphanumeric or .- first character: alphanumeric or -
full file name	0-256	alphanumeric or _/.-
hostname	Used in hostname command	
	0-63	alphanumeric or .-_ first character: alphanumeric or -
	Used in other commands	
	0-252	alphanumeric or .- first character: alphanumeric or -
import configuration file	1-26+”.conf”	alphanumeric or ;`~!@#$%^&()_+[]{}',.=- add “.conf” at the end
import shell script	1-26+”.zysh”	alphanumeric or ;`~!@#$%^&()_+[]{}',.=- add “.zysh” at the end
initial string	1-64	alphanumeric, spaces, or '()+,/:=!*#@$_%-.&
isp account password	0-63	alphanumeric or `~!@#$%^&*()_\-+={}|\;:'<,>./

Table 3 Input-Value Formats for Strings in CLI Commands (continued)

TAG	# VALUES	LEGAL VALUES
isp account username	0-30	alphanumeric or -_@$./
key length	--	512, 768, 1024, 1536, 2048
license key	25	“S-” + 6 upper-case letters or numbers + “-” + 16 upper-case letters or numbers
mac address	--	aa:bb:cc:dd:ee:ff (hexadecimal)
mail server fqdn		lower-case letters, numbers, or -.
name	1-31	alphanumeric or _-
notification message	1-81	alphanumeric, spaces, or '()+,/:=?;!*#@$_%-
password: less than 15 chars	1-15	alphanumeric or `~!@#$%^&*()_\-+={}|\;:'<,>./
password: less than 8 chars	1-8	alphanumeric or ;/?:@&=+$\.-_!~*'()%,#$
password	Used in user and ip ddns	
	1-63	alphanumeric or `~!@#$%^&*()_-+={}|\;:'<,>./
	Used in e-mail log profile SMTP authentication	
	1-63	alphanumeric or `~!@#$%^&*()_-+={}|\;:'<>./
	Used in registration	
	6-20	alphanumeric or .@_-
phone number	1-20	numbers or ,+
preshared key	16-64	“0x” or “0X” + 16-64 hexadecimal values alphanumeric or ;|`~!@#$%^&*()_+\{}':,./<>=-
profile name	0-30	alphanumeric or _- first character: letters or _-
proto name	1-16	lower-case letters, numbers, or -
protocol name	0-30	alphanumeric or _- first character: letters or _-
quoted string less than 127 chars	1-255	alphanumeric, spaces, or ;/?:@&=+$\.-_!~*'()%,
quoted string less than 63 chars	1-63	alphanumeric, spaces, or ;/?:@&=+$\.-_!~*'()%
quoted string	0+	alphanumeric, spaces, or punctuation marks enclosed in double quotation marks (“) must put a backslash (\) before double quotation marks that are part of input value itself
service name	0-63	alphanumeric or -_@$./
spi	2-8	hexadecimal
string less than 15 chars	1-15	alphanumeric or -_
string: less than 63 chars	1-63	alphanumeric or `~!@#$%^&*()_-+={}|\;:'<,>./
string	1+	alphanumeric or -_@
subject	1-61	alphanumeric, spaces, or '()+,./:=?;!*#@$_%-

Table 3 Input-Value Formats for Strings in CLI Commands (continued)

TAG	# VALUES	LEGAL VALUES
system type	0-2	hexadecimal
timezone [-+]*hh*	--	-12 through +12 (with or without “+”)
url	1-511	alphanumeric or '()+,/:.=?;!*#@$_%-
user name	Used in VPN extended authentication	
	1-31	alphanumeric or _-
	Used in other commands	
	0-30	alphanumeric or _- first character: letters or _-
username	6-20	alphanumeric or .@_- registration
user name	1+	alphanumeric or -_. logging commands
user@domainname	1-80	alphanumeric or .@_-
vrrp group name: less than 15 chars	1-15	alphanumeric or _-
week-day sequence, i.e. 1=first,2=second	1	1-4
xauth method	1-31	alphanumeric or _-
xauth password	1-31	alphanumeric or ;|`~!@#$%^&*()_+\{}':,./<>=-
mac address	0-12 (even number)	hexadecimal for example: aa aabbcc aabbccddeeff

1.8 Ethernet Interfaces

How you specify an Ethernet interface depends on the ISG50 model. Use *gex*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your ISG50 model.

1.9 Saving Configuration Changes

Use the `write` command to save the current configuration to the ISG50.

Note: Always save the changes before you log out after each management session. All unsaved changes will be lost after the system restarts.

1.10 Logging Out

Enter the `exit` or `end` command in configure mode to go to privilege mode.

Enter the `exit` command in user mode or privilege mode to log out of the CLI.

2

User and Privilege Modes

This chapter describes how to use these two modes.

2.1 User And Privilege Modes

This is the mode you are in when you first log into the CLI. (Do not confuse ‘user mode’ with types of user accounts the ISG50 uses. See Chapter 19 on page 269 for more information about the user types. ‘User’ type accounts can only run ‘exit’ in this mode. However, they may need to log into the device in order to be authenticated for ‘user-aware’ policies, for example a firewall rule that a particular user is exempt from or a VPN tunnel that only certain people may use.)

Type ‘enable’ to go to ‘privilege mode’. No password is required. All commands can be run from here except those marked with an asterisk. Many of these commands are for trouble-shooting purposes, for example the htm (hardware test module) and debug commands. Customer support may ask you to run some of these commands and send the results if you need assistance troubleshooting your device.

For admin logins, all commands are visible in ‘user mode’ but not all can be run there. The following table displays which commands can be run in ‘user mode’. All commands can be run in ‘privilege mode’.

The `htm` and `psm` commands are for ZyXEL’s internal manufacturing process.

Table 4 User (U) and Privilege (P) Mode Commands

COMMAND	MODE	DESCRIPTION
`apply`	P	Applies a configuration file.
`atse`	U/P	Displays the seed code
`clear`	U/P	Clears system or debug logs or DHCP binding.
`configure`	U/P	Use ‘configure terminal’ to enter configuration mode.
`copy`	P	Copies configuration files.
`debug (*)`	U/P	For support personnel only! The device needs to have the debug flag enabled.
`delete`	P	Deletes configuration files.
`details`	P	Performs diagnostic commands.
`diag`	P	Provided for support personnel to collect internal system information. It is not recommended that you use these.
`diag-info`	P	Has the ISG50 create a new diagnostic file.
`dir`	P	Lists files in a directory.

Table 4 User (U) and Privilege (P) Mode Commands (continued)

COMMAND	MODE	DESCRIPTION
disable	U/P	Goes from privilege mode to user mode
enable	U/P	Goes from user mode to privilege mode
exit	U/P	Goes to a previous mode or logs out.
htm	U/P	Goes to htm (hardware test module) mode for testing hardware components. You may need to use the htm commands if your customer support Engineer asks you to during troubleshooting. Note: These commands are for ZyXEL's internal manufacturing process.
interface	U/P	Dials or disconnects an interface.
no packet-trace	U/P	Turns of packet tracing.
nslookup	U/P	Resolves an IP address to a host name and vice-versa.
packet-trace	U/P	Performs a packet trace.
ping	U/P	Pings an IP address or host name.
psm	U/P	Goes to psm (product support module) mode for setting product parameters. You may need to use the htm commands if your customer support Engineer asks you to during troubleshooting. Note: These commands are for ZyXEL's internal manufacturing process.
reboot	P	Restarts the device.
release	P	Releases DHCP information from an interface.
rename	P	Renames a configuration file.
renew	P	Renews DHCP information for an interface.
run	P	Runs a script.
setenv	U/P	Turns stop-on-error on (terminates booting if an error is found in a configuration file) or off (ignores configuration file errors and continues booting).
show	U/P	Displays command statistics. See the associated command chapter in this guide.
shutdown	P	Writes all d data to disk and stops the system processes. It does not turn off the power.
telnet	U/P	Establishes a connection to the TCP port number 23 of the specified host name or IP address.
test aaa	U/P	Tests whether the specified user name can be successfully authenticated by an external authentication server.
traceroute	P	Traces the route to the specified host name or IP address.
write	P	Saves the current configuration to the ISG50. All unsaved changes are lost after the ISG50 restarts.

Subsequent chapters in this guide describe the configuration commands. User/privilege mode commands that are also configuration commands (for example, 'show') are described in more detail in the related configuration command chapter.

2.1.1 Debug Commands

Debug commands marked with an asterisk (*) are not available when the debug flag is on and are for ZyXEL service personnel use only. The debug commands follow a syntax that is Linux-based, so

if there is a Linux equivalent, it is displayed in this chapter for your reference. You must know a command listed here well before you use it. Otherwise, it may cause undesired results.

Table 5 Debug Commands

COMMAND SYNTAX	DESCRIPTION	LINUX COMMAND EQUIVALENT
debug alg	ALG debug commands	
debug ca (*)	Certificate debug commands	
debug force-auth (*)	Authentication policy debug commands	
debug gui (*)	Web Configurator releated debug commands	
debug hardware (*)	Hardware debug commands	
debug interface	Interface debug commands	
debug interface ifconfig [interface]	Shows system interfaces detail	> ifconfig [interface]
debug interface-group	Port grouping debug commands	
debug ip dns	DNS debug commands	
debug ip virtual-server	Virtual Server (NAT) debug commands.	
debug ipsec	IPSec VPN debug commands	
debug logging	System logging debug commands	
debug manufacture	Manufacturing related debug commands	
debug myzyxel server (*)	Myzyxel.com debug commands	
debug network arpignore (*)	Enable/Display the ignoring of ARP responses for interfaces which don't own the IP address	cat /proc/sys/net/ipv4/conf/*/arp_ignore
debug no myzyxel server (*)	Set the myZyXEL.com registration/update server to the official site	
debug pbx tapi dump {on|off}	Sets whether or not the ISG50 displays the debug messages about TAPI on the console.	
debug policy-route (*)	Policy route debug commands	
debug service-register	Service registration debug commands	
debug show myzyxel server status	Myzyxel.com debug commands	
debug show ipset	Lists the ISG50‘s received cards	
debug show myzyxel server status	Myzyxel.com debug commands	
debug [cmdexec|corefile|ip|kernel|mac-id-rewrite|observer|switch|system|zyinetpkt|zysh-ipt-op] (*)	ZLD internal debug commands	
debug update server (*)	Update server debug command	

PART II
Reference

3

Object Reference

This chapter describes how to use object reference commands.

3.1 Object Reference Commands

The object reference commands are used to see which configuration settings reference a specfic object. You can use this table when you want to delete an object because you have to remove references to the object first.

Table 6 `show reference` Commands

COMMAND	DESCRIPTION
`show reference object username [username]`	Displays which configuration settings reference the specified user object.
`show reference object address [profile]`	Displays which configuration settings reference the specified address object.
`show reference object service [profile]`	Displays which configuration settings reference the specified service object.
`show reference object schedule [profile]`	Displays which configuration settings reference the specified schedule object.
`show reference object interface [interface_name | virtual_interface_name]`	Displays which configuration settings reference the specified interface or virtual interface object.
`show reference object aaa authentication [default | auth_method]`	Displays which configuration settings reference the specified AAA authentication object.
`show reference object ca category {local|remote} [cert_name]`	Displays which configuration settings reference the specified authentication method object.
`show reference object account pppoe [profile]`	Displays which configuration settings reference the specified PPPoE account object.
`show reference object account pptp [profile]`	Displays which configuration settings reference the specified PPTP account object.
`show reference object crypto map [crypto_name]`	Displays which configuration settings reference the specified VPN connection object.
`show reference object isakmp policy [isakmp_name]`	Displays which configuration settings reference the specified VPN gateway object.
`show reference object zone [profile]`	Displays which configuration settings reference the specified zone object.
`show reference object-group username [username]`	Displays which configuration settings reference the specified user group object.
`show reference object-group address [profile]`	Displays which configuration settings reference the specified address group object.

Table 6 show reference Commands (continued)

COMMAND	DESCRIPTION
show reference object-group service [*profile*]	Displays which configuration settings reference the specified service group object.
show reference object-group interface [*profile*]	Displays which configuration settings reference the specified trunk object.
show reference object-group aaa ad [*group_name*]	Displays which configuration settings reference the specified AAA AD group object.
show reference object-group aaa ldap [*group_name*]	Displays which configuration settings reference the specified AAA LDAP group object.
show reference object-group aaa radius [*group_name*]	Displays which configuration settings reference the specified AAA RADIUS group object.

3.1.1 Object Reference Command Example

This example shows how to check which configuration is using an address object named LAN1_SUBNET. For the command output, firewall rule 3 named LAN1-to-Device is using the address object.

```
Router(config)# show reference object address LAN1_SUBNET

LAN1_SUBNET References:
Category
Rule Priority        Rule Name
Description
================================================================================
Firewall
3                    N/A
LAN1-to-Device
Router(config)#
```

4

Status

This chapter explains some commands you can use to display information about the ISG50's current operational state.

Table 7 Status Show Commands

COMMAND	DESCRIPTION
`show boot status`	Displays details about the ISG50's startup state.
`show comport status`	Displays whether the console port is on or off.
`show cpu status`	Displays the CPU utilization.
`show disk`	Displays the disk utilization.
`show extension-slot`	Displays the status of the USB ports and the names of any connected devices.
`show fan-speed`	Displays the current fan speed.
`show led status`	Displays the status of the **SYS** LED on the ISG50.
`show mac`	Displays the ISG50's MAC address.
`show mem status`	Displays what percentage of the ISG50's memory is currently being used.
`show ram-size`	Displays the size of the ISG50's on-board RAM.
`show serial-number`	Displays the serial number of this ISG50.
`show socket listen`	Displays the ISG50's listening ports
`show socket open`	Displays the ports that are open on the ISG50.
`show system uptime`	Displays how long the ISG50 has been running since it last restarted or was turned on.
`show version`	Displays the ISG50's model, firmware and build information.

Here are examples of the commands that display the CPU and disk utilization.

```
Router(config)# show cpu status
CPU utilization: 0 %
CPU utilization for 1 min: 0 %
CPU utilization for 5 min: 1 %
```

Here are examples of the commands that display the fan speed, MAC address, memory usage, RAM size, and serial number.

```
Router(config)# show fan-speed
FAN1(F00)(rpm): limit(hi)=6500, limit(lo)=1400, max=6006, min=6006, avg=6006
Router(config)# show mac
MAC address: 00:13:49:00:00:01-00:13:49:00:00:05
Router(config)# show mem status
memory usage: 28%
Router(config)# show ram-size
ram size: 512MB
Router(config)# show serial-number
serial number: Z34131340 80-009-011001AA
```

Here is an example of the command that displays the listening ports.

```
Router(config)# show socket listen
No.   Proto Local_Address         Foreign_Address       State
================================================================================
1     tcp   0.0.0.0:2601          0.0.0.0:0             LISTEN
2     tcp   0.0.0.0:2602          0.0.0.0:0             LISTEN
3     tcp   127.0.0.1:10443       0.0.0.0:0             LISTEN
4     tcp   0.0.0.0:2604          0.0.0.0:0             LISTEN
5     tcp   0.0.0.0:80            0.0.0.0:0             LISTEN
6     tcp   127.0.0.1:8085        0.0.0.0:0             LISTEN
7     tcp   1.1.1.1:53            0.0.0.0:0             LISTEN
8     tcp   172.23.37.205:53      0.0.0.0:0             LISTEN
9     tcp   10.0.0.8:53           0.0.0.0:0             LISTEN
10    tcp   172.23.37.240:53      0.0.0.0:0             LISTEN
11    tcp   192.168.1.1:53        0.0.0.0:0             LISTEN
12    tcp   127.0.0.1:53          0.0.0.0:0             LISTEN
13    tcp   0.0.0.0:21            0.0.0.0:0             LISTEN
14    tcp   0.0.0.0:22            0.0.0.0:0             LISTEN
15    tcp   127.0.0.1:953         0.0.0.0:0             LISTEN
16    tcp   0.0.0.0:443           0.0.0.0:0             LISTEN
17    tcp   127.0.0.1:1723        0.0.0.0:0             LISTEN
```

Here is an example of the command that displays the open ports.

```
Router(config)# show socket open
No.   Proto Local_Address         Foreign_Address       State
==========================================================================
1     tcp   172.23.37.240:22      172.23.37.10:1179     ESTABLISHED
2     udp   127.0.0.1:64002       0.0.0.0:0
3     udp   0.0.0.0:520           0.0.0.0:0
4     udp   0.0.0.0:138           0.0.0.0:0
5     udp   0.0.0.0:138           0.0.0.0:0
6     udp   0.0.0.0:138           0.0.0.0:0
7     udp   0.0.0.0:138           0.0.0.0:0
8     udp   0.0.0.0:138           0.0.0.0:0
9     udp   0.0.0.0:138           0.0.0.0:0
10    udp   0.0.0.0:138           0.0.0.0:0
11    udp   0.0.0.0:32779         0.0.0.0:0
12    udp   192.168.1.1:4500      0.0.0.0:0
13    udp   1.1.1.1:4500          0.0.0.0:0
14    udp   10.0.0.8:4500         0.0.0.0:0
15    udp   172.23.37.205:4500    0.0.0.0:0
16    udp   172.23.37.240:4500    0.0.0.0:0
17    udp   127.0.0.1:4500        0.0.0.0:0
18    udp   127.0.0.1:63000       0.0.0.0:0
19    udp   127.0.0.1:63001       0.0.0.0:0
20    udp   127.0.0.1:63002       0.0.0.0:0
21    udp   0.0.0.0:161           0.0.0.0:0
22    udp   127.0.0.1:63009       0.0.0.0:0
23    udp   192.168.1.1:1701      0.0.0.0:0
24    udp   1.1.1.1:1701          0.0.0.0:0
25    udp   10.0.0.8:1701         0.0.0.0:0
26    udp   172.23.37.205:1701    0.0.0.0:0
27    udp   172.23.37.240:1701    0.0.0.0:0
28    udp   127.0.0.1:1701        0.0.0.0:0
29    udp   127.0.0.1:63024       0.0.0.0:0
30    udp   127.0.0.1:30000       0.0.0.0:0
31    udp   1.1.1.1:53            0.0.0.0:0
32    udp   172.23.37.205:53      0.0.0.0:0
33    udp   10.0.0.8:53           0.0.0.0:0
34    udp   172.23.37.240:53      0.0.0.0:0
35    udp   192.168.1.1:53        0.0.0.0:0
36    udp   127.0.0.1:53          0.0.0.0:0
37    udp   0.0.0.0:67            0.0.0.0:0
38    udp   127.0.0.1:63046       0.0.0.0:0
39    udp   127.0.0.1:65097       0.0.0.0:0
40    udp   0.0.0.0:65098         0.0.0.0:0
41    udp   192.168.1.1:500       0.0.0.0:0
42    udp   1.1.1.1:500           0.0.0.0:0
43    udp   10.0.0.8:500          0.0.0.0:0
44    udp   172.23.37.205:500     0.0.0.0:0
45    udp   172.23.37.240:500     0.0.0.0:0
46    udp   127.0.0.1:500         0.0.0.0:0
```

Here are examples of the commands that display the system uptime and model, firmware, and build information.

```
Router> show system uptime
system uptime: 04:18:00
Router> show version
ZyXEL Communications Corp.
model           : ISG50-PSTN
firmware version: ISG50-PSTN-2.21-2011-06-30-04-00
BM version      : 1.12
build date      : 2011-06-30 05:14:42
```

This example shows the current LED states on the ISG50. The **SYS** LED light is on and green.

```
Router> show led status
sys: green
```

5

Registration

This chapter introduces myzyxel.com and shows you how to register the ISG50 using commands.

5.1 myZyXEL.com overview

myZyXEL.com is ZyXEL's online services center where you can register your ISG50 and manage subscription services available for the ISG50. To use a subscription service, you have to register the ISG50 and activate the corresponding service at myZyXEL.com (through the ISG50).

Note: You need to create a myZyXEL.com account before you can register your device and activate the services at myZyXEL.com.

You can directly create a myZyXEL.com account, register your ISG50 and activate a service using the **Registration** screen. Alternatively, go to http://www.myZyXEL.com with the ISG50's serial number and LAN MAC address to register it. Refer to the web site's on-line help for details.

Note: To activate a service on a ISG50, you need to access myZyXEL.com via that ISG50.

Subscription Services Available on the ISG50

Purchase and enter a license key to use subscription services such as call recording, additional extension numbers, and smartphone application support. You can try a free trial of the call recording and smartphone application support services. See the respective User's Guide chapters for more information about these features.

5.2 Registration Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 8 Input Values for General Registration Commands

LABEL	DESCRIPTION
user_name	The user name of your myZyXEL.com account. You must use six to 20 alphanumeric characters (and the underscore). Spaces are not allowed.
password	The password for the myZyXEL.com account. You must use six to 20 alphanumeric characters (and the underscore). Spaces are not allowed.

The following table describes the commands available for registration. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 9 Command Summary: Registration

COMMAND	DESCRIPTION
`device-register checkuser user_name`	Checks if the user name exists in the myZyXEL.com database.
`device-register username user_name password password [e-mail user@domainname] [country-code country_code] [reseller-name name] [reseller-mail email-address] [reseller-phone phone-number] [vat vat-number]`	Registers the device with an existing account or creates a new account and registers the device at one time. *country_code*: see Table 10 on page 47
`service-register checkexpire`	Gets information of all service subscriptions from myZyXEL.com and updates the status table.
`service-register service-type standard license-key key_value`	Activates a standard service subscription with the license key.
`service-register service-type trial service {call-recording|smartphone}`	Activates the call recording or smartphone service trial.
`show device-register status`	Displays whether the device is registered and account information.
`show service-register server-type`	Displays the type of the register server to which your ISG50 is connected.
`show service-register status all`	Displays service license information.

5.2.1 Command Examples

The following commands allow you to register your device with an existing account or create a new account and register the device at one time, and activate a trial service subscription.

```
Router# configure terminal
Router(config)# device-register username alexctsui password 123456
Router(config)# service-register service-type trial service call-recording
```

The following command displays the account information and whether the device is registered.

```
Router# configure terminal
Router(config)# show device-register status
username               : example
password               : 123456
device register status : yes
expiration self check  : no
```

The following command displays the service registration status and type and how many days remain before the service expires.

```
Router(config)# show service-register status all
Service              Status       Type                    Count Expiration
=============================================================================
Call Recording       Not Licensed None                    N/A   0
Extension            Licensed     Standard                25    N/A
Smartphone           Not Licensed None                    N/A   0
```

The following command displays the seller details you have entered on the ISG50.

```
Router# configure terminal
Router(config)# show service-register reseller-info
seller’s name: ABC
seller’s e-mail: abc@example.com
seller’s contact number: 12345678
vat number:
```

5.3 Country Code

The following table displays the number for each country.

Table 10 Country Codes

COUNTRY CODE	COUNTRY NAME	COUNTRY CODE	COUNTRY NAME
001	Afghanistan	002	Albania
003	Algeria	004	American Samoa
005	Andorra	006	Angola
007	Anguilla	008	Antarctica
009	Antigua & Barbuda	010	Argentina
011	Armenia	012	Aruba
013	Ascension Island	014	Australia
015	Austria	016	Azerbaijan
017	Bahamas	018	Bahrain
019	Bangladesh	020	Barbados
021	Belarus	022	Belgium
023	Belize	024	Benin
025	Bermuda	026	Bhutan
027	Bolivia	028	Bosnia and Herzegovina
029	Botswana	030	Bouvet Island
031	Brazil	032	British Indian Ocean Territory
033	Brunei Darussalam	034	Bulgaria
035	Burkina Faso	036	Burundi
037	Cambodia	038	Cameroon

Table 10 Country Codes (continued)

COUNTRY CODE	COUNTRY NAME	COUNTRY CODE	COUNTRY NAME
039	Canada	040	Cape Verde
041	Cayman Islands	042	Central African Republic
043	Chad	044	Chile
045	China	046	Christmas Island
047	Cocos (Keeling) Islands	048	Colombia
049	Comoros	050	Congo, Democratic Republic of the
051	Congo, Republic of	052	Cook Islands
053	Costa Rica	054	Cote d'Ivoire
055	Croatia/Hrvatska	056	Cyprus
057	Czech Republic	058	Denmark
059	Djibouti	060	Dominica
061	Dominican Republic	062	East Timor
063	Ecuador	064	Egypt
065	El Salvador	066	Equatorial Guinea
067	Eritrea	068	Estonia
069	Ethiopia	070	Falkland Islands (Malvina)
071	Faroe Islands	072	Fiji
073	Finland	074	France
075	France (Metropolitan)	076	French Guiana
077	French Polynesia	078	French Southern Territories
079	Gabon	080	Gambia
081	Georgia	082	Germany
083	Ghana	084	Gibraltar
085	Great Britain	086	Greece
087	Greenland	088	Grenada
089	Guadeloupe	090	Guam
091	Guatemala	092	Guernsey
093	Guinea	094	Guinea-Bissau
095	Guyana	096	Haiti
097	Heard and McDonald Islands	098	Holy See (City Vatican State)
099	Honduras	100	Hong Kong
101	Hungary	102	Iceland
103	India	104	Indonesia
105	Ireland	106	Isle of Man
107	Italy	108	Jamaica
109	Japan	110	Jersey
111	Jordan	112	Kazakhstan
113	Kenya	114	Kiribati
115	Korea, Republic of	116	Kuwait
117	Kyrgyzstan	118	Lao People's Democratic Republic

Table 10 Country Codes (continued)

COUNTRY CODE	COUNTRY NAME	COUNTRY CODE	COUNTRY NAME
119	Latvia	120	Lebanon
121	Lesotho	122	Liberia
123	Liechtenstein	124	Lithuania
125	Luxembourg	126	Macau
127	Macedonia, Former Yugoslav Republic	128	Madagascar
129	Malawi	130	Malaysia
131	Maldives	132	Mali
133	Malta	134	Marshall Islands
135	Martinique	136	Mauritania
137	Mauritius	138	Mayotte
139	Mexico	140	Micronesia, Federal State of
141	Moldova, Republic of	142	Monaco
143	Mongolia	144	Montserrat
145	Morocco	146	Mozambique
147	Namibia	148	Nauru
149	Nepal	150	Netherlands
151	Netherlands Antilles	152	New Caledonia
153	New Zealand	154	Nicaragua
155	Niger	156	Nigeria
157	Niue	158	Norfolk Island
159	Northern Mariana Islands	160	Norway
161	Not Determined	162	Oman
163	Pakistan	164	Palau
165	Panama	166	Papua New Guinea
167	Paraguay	168	Peru
169	Philippines	170	Pitcairn Island
171	Poland	172	Portugal
173	Puerto Rico	174	Qatar
175	Reunion Island	176	Romania
177	Russian Federation	178	Rwanda
179	Saint Kitts and Nevis	180	Saint Lucia
181	Saint Vincent and the Grenadines	182	San Marino
183	Sao Tome and Principe	184	Saudi Arabia
185	Senegal	186	Seychelles
187	Sierra Leone	188	Singapore
189	Slovak Republic	190	Slovenia
191	Solomon Islands	192	Somalia
193	South Africa	194	South Georgia and the South Sandwich Islands
185	Spain	196	Sri Lanka

Table 10 Country Codes (continued)

COUNTRY CODE	COUNTRY NAME	COUNTRY CODE	COUNTRY NAME
197	St Pierre and Miquelon	198	St. Helena
199	Suriname	200	Svalbard and Jan Mayen Islands
201	Swaziland	202	Sweden
203	Switzerland	204	Taiwan
205	Tajikistan	206	Tanzania
207	Thailand	208	Togo
209	Tokelau	210	Tonga
211	Trinidad and Tobago	212	Tunisia
213	Turkey	214	Turkmenistan
215	Turks and Caicos Islands	216	Tuvalu
217	US Minor Outlying Islands	218	Uganda
219	Ukraine	220	United Arab Emirates
221	United Kingdom	222	United States
223	Uruguay	224	Uzbekistan
225	Vanuatu	226	Venezuela
227	Vietnam	228	Virgin Islands (British)
229	Virgin Islands (USA)	230	Wallis And Futuna Islands
231	Western Sahara	232	Western Samoa
233	Yemen	234	Yugoslavia
235	Zambia	236	Zimbabwe

6

Interfaces

This chapter shows you how to use interface-related commands.

6.1 Interface Overview

In general, an interface has the following characteristics.

- An interface is a logical entity through which (layer-3) packets pass.
- An interface is bound to a physical port or another interface.
- Many interfaces can share the same physical port.
- An interface is bound to at most one zone.
- Many interface can belong to the same zone.
- Layer-3 virtualization (IP alias, for example) is a kind of interface.

Some characteristics do not apply to some types of interfaces.

6.1.1 Types of Interfaces

You can create several types of interfaces in the ISG50. The types supported vary by ISG50 model.

- **Port groups** create a hardware connection between physical ports at the layer-2 (data link, MAC address) level.
- **Ethernet interfaces** are the foundation for defining other interfaces and network policies. RIP and OSPF are also configured in these interfaces.
- **VLAN interfaces** receive and send tagged frames. The ISG50 automatically adds or removes the tags as needed. Each VLAN can only be associated with one Ethernet interface.
- **Bridge interfaces** create a software connection between Ethernet or VLAN interfaces at the layer-2 (data link, MAC address) level. Unlike port groups, bridge interfaces can take advantage of some security features in the ISG50. You can also assign an IP address and subnet mask to the bridge.
- **PPPoE/PPTP interfaces** support Point-to-Point Protocols (PPP). ISP accounts are required for PPPoE/PPTP interfaces.
- **Cellular interfaces** are for 3G WAN connections via a connected 3G device.
- **Virtual interfaces** (IP alias) provide additional routing information in the ISG50. There are three types: **virtual Ethernet interfaces**, **virtual VLAN interfaces**, and **virtual bridge interfaces**.
- **Trunks** manage load balancing between interfaces.

Port groups and trunks have a lot of characteristics that are specific to each type of interface. These characteristics are listed in the following tables and discussed in more detail farther on.

Table 11 Characteristics of Ethernet, VLAN, Bridge, PPPoE/PPTP, and Virtual Interfaces

CHARACTERISTICS	ETHERNET	VLAN	BRIDGE	PPPOE/PPTP	VIRTUAL
Name*	gex	vlanx	brx	pppx	**
IP Address Assignment					
static IP address	Yes	Yes	Yes	Yes	Yes
DHCP client	Yes	Yes	Yes	Yes	No
routing metric	Yes	Yes	Yes	Yes	Yes
Interface Parameters					
bandwidth restrictions	Yes	Yes	Yes	Yes	Yes
packet size (MTU)	Yes	Yes	Yes	Yes	No
data size (MSS)	Yes	Yes	Yes	Yes	No
traffic prioritization	Yes	Yes	Yes	Yes	No
DHCP					
DHCP server	Yes	Yes	Yes	No	No
DHCP relay	Yes	Yes	Yes	No	No
Ping Check	Yes	Yes	Yes	Yes	No

* - The format of interface names is strict. Each name consists of 2-4 letters (interface type), followed by a number (*x*, limited by the maximum number of each type of interface). For example, Ethernet interface names are ge1, ge2, ge3, ...; VLAN interfaces are vlan0, vlan1, vlan2, ...; and so on.

** - The names of virtual interfaces are derived from the interfaces on which they are created. For example, virtual interfaces created on Ethernet interface ge1 are called ge1:1, ge1:2, and so on. Virtual interfaces created on VLAN interface vlan2 are called vlan2:1, vlan2:2, and so on. You cannot specify the number after the colon(:) in the web configurator; it is a sequential number. You can specify the number after the colon if you use the CLI to set up a virtual Interface Parameters

Table 12 Cellular Interface Characteristics

CHARACTERISTICS	CELLULAR
Name*	cellular*x*
Configurable Zone	Yes**
IP Address Assignment	
Static IP address	Yes
DHCP client	Yes
Routing metric	Yes
Interface Parameters	
Bandwidth restrictions	Yes
Packet size (MTU)	Yes
Data size (MSS)	Yes
DHCP	
DHCP server	No
DHCP relay	No
Connectivity Check	Yes

* - Each name consists of letters (interface type), followed by a number (*x*). For most interfaces, x is limited by the

maximum number of the type of interface.

** - Cellular interfaces can be added to the WAN zone or no zone.

6.1.2 Relationships Between Interfaces

In the ISG50, interfaces are usually created on top of other interfaces. Only Ethernet interfaces are created directly on top of the physical ports (or port groups). The relationships between interfaces are explained in the following table.

Table 13 Relationships Between Different Types of Interfaces

INTERFACE	REQUIRED PORT / INTERFACE
port group	physical port
Ethernet interface	physical port port group
VLAN interface	Ethernet interface
bridge interface	Ethernet interface* VLAN interface*
PPPoE/PPTP interface	Ethernet interface* VLAN interface* bridge interface
virtual interface (virtual Ethernet interface) (virtual VLAN interface) (virtual bridge interface)	 Ethernet interface* VLAN interface* bridge interface
trunk	Ethernet interface Cellular interface VLAN interface bridge interface PPPoE/PPTP interface

* - You cannot set up a PPPoE/PPTP interface, virtual Ethernet interface, or virtual VLAN interface if the underlying interface is a member of a bridge. You also cannot add an Ethernet interface or VLAN interface to a bridge if the member interface has a virtual interface or PPPoE/PPTP interface on top of it.

6.2 Interface General Commands Summary

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 14 Input Values for General Interface Commands

LABEL	DESCRIPTION
interface_name	The name of the interface. Ethernet interface: Use ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your ISG50 model. virtual interface on top of Ethernet interface: add a colon (:) and the number of the virtual interface. For example: ge*x*:*y*, *x* = 1 - N, *y* = 1 - 4 VLAN interface: vlan*x*, *x* = 0 - 4094 virtual interface on top of VLAN interface: vlan*x*:*y*, *x* = 0 - 4094, *y* = 1 - 4 bridge interface: br*x*, *x* = 0 - N, where N depends on the number of bridge interfaces your ISG50 model supports. virtual interface on top of bridge interface: br*x*:*y*, *x* = the number of the bridge interface, *y* = 1 - 4 PPPoE/PPTP interface: ppp*x*, *x* = 0 - N, where N depends on the number of PPPoE/PPTP interfaces your ISG50 model supports.
profile_name	The name of the DHCP pool. You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
domain_name	Fully-qualified domain name. You may up to 254 alphanumeric characters, dashes (-), or periods (.), but the first character cannot be a period.

The following sections introduce commands that are supported by several types of interfaces. See Section 6.6 on page 69 for the unique commands for each type of interface.

6.2.1 Basic Interface Properties and IP Address Commands

This table lists basic properties and IP address commands.

Table 15 interface General Commands: Basic Properties and IP Address Assignment

COMMAND	DESCRIPTION
`show interface {ethernet | vlan | bridge | ppp} status`	Displays the connection status of the specified type of interfaces.
`show interface {`*`interface_name`*` | ethernet | vlan | bridge | ppp | virtual ethernet | virtual vlan | virtual bridge | all}`	Displays information about the specified interface, specified type of interfaces, or all interfaces. See Section 6.6.1 on page 72 for all possible cellular status description.
`show interface send statistics interval`	Displays the interval for how often the ISG50 refreshes the sent packet statistics for the interfaces.
`show interface summary all`	Displays basic information about the interfaces.
`show interface summary all status`	Displays the connection status of the interfaces.
`[no] interface `*`interface_name`	Creates the specified interface if necessary and enters sub-command mode. The `no` command deletes the specified interface.

Table 15 interface General Commands: Basic Properties and IP Address Assignment (continued)

COMMAND	DESCRIPTION
[no] description *description*	Specifies the description for the specified interface. The no command clears the description. *description*: You can use alphanumeric and ()+/ :=?!*#@$_%- characters, and it can be up to 60 characters long.
[no] downstream <0..1048576>	This is reserved for future use. Specifies the downstream bandwidth for the specified interface. The no command sets the downstream bandwidth to 1048576.
exit	Leaves the sub-command mode.
[no] ip address dhcp	Makes the specified interface a DHCP client; the DHCP server gives the specified interface its IP address, subnet mask, and gateway. The no command makes the IP address static IP address for the specified interface. (See the next command to set this IP address.)
[no] ip address *ip subnet_mask*	Assigns the specified IP address and subnet mask to the specified interface. The no command clears the IP address and the subnet mask.
[no] ip gateway *ip*	Adds the specified gateway using the specified interface. The no command removes the gateway.
ip gateway *ip* metric <0..15>	Sets the priority (relative to every gateway on every interface) for the specified gateway. The lower the number, the higher the priority.
[no] metric <0..15>	Sets the PPPoE/PPTP or cellular interface's priority relative to other interfaces. The lower the number, the higher the priority.
[no] mss <536..1460>	Specifies the maximum segment size (MSS) the interface is to use. MSS is the largest amount of data, specified in bytes, that the interface can handle in a single, unfragmented piece. The no command has the interface use its default MSS.
[no] mtu <576..1500>	Specifies the Maximum Transmission Unit, which is the maximum number of bytes in each packet moving through this interface. The ISG50 divides larger packets into smaller fragments. The no command resets the MTU to 1500.
[no] shutdown	Deactivates the specified interface. The no command activates it.
traffic-prioritize {tcp-ack|content-filter|dns|ipsec-vpn} bandwidth <0..1048576> priority <1..7> [maximize-bandwidth-usage];	Applies traffic priority when the interface sends TCP-ACK traffic, traffic for resolving domain names, or encrypted traffic for an IPSec VPN tunnel. It also sets how much bandwidth the traffic can use and can turn on maximize bandwidth usage.
traffic-prioritize {tcp-ack|content-filter|dns|ipsec-vpn} deactivate	Turns off traffic priority settings for when the interface sends the specified type of traffic.
[no] upstream <0..1048576>	Specifies the upstream bandwidth for the specified interface. The no command sets the upstream bandwidth to 1048576.
interface reset {*interface_name*|*virtual_interface_name*|all}	Resets the interface statistics TxPkts (transmitted packets) and RxPkts (received packets) counts to 0. You can use the show interface summary all status command to see the interface statistics.

Table 15 interface General Commands: Basic Properties and IP Address Assignment (continued)

COMMAND	DESCRIPTION
`interface send statistics interval <15..3600>`	Sets how often the ISG50 sends interface statistics to external servers. For example, syslog server and Vantage Report server.
`show interface-name`	Displays all PPP and Ethernet interface system name and user-defined name mappings.
`interface-name {`*`ppp_interface`* `|` *`ethernet_interface`*`} `*`user_defined_name`*	Specifies a name for a PPP or an Ethernet interface. It can use alphanumeric characters, hyphens, and underscores, and it can be up to 11 characters long. *`ppp_interface`* | *`ethernet_interface`*: This must be the system name of a PPP or an Ethernet interface. Use the `show interface-name` command to see the system name of interfaces. *`user_defined_name`*: • This name cannot be one of the follows: "ethernet", "ppp", "vlan", "bridge", "virtual", "cellular", "tunnel", "status", "summary", "all" • This name cannot begin with one of the follows either: "ge", "ppp", "vlan", "br", "cellular", "tunnel".
`interface-rename `*`old_user_defined_name new_user_defined_name*	Modifies the user-defined name of a PPP or an Ethernet interface.

6.2.1.1 Basic Interface Properties Command Examples

The following commands make Ethernet interface ge1 a DHCP client.

```
Router# configure terminal
Router(config)# interface ge1
Router(config-if)# ip address dhcp
Router(config-if)# exit
```

This example shows how to modify the name of interface ge4 to “VIP”. First you have to check the interface system name (ge4 in this example) on the ISG50. Then change the name and display the result.

```
Router> show interface-name
No.  System Name     User Defined Name
================================================================================
====
1    ge1             wan1
2    ge2             wan2
3    ge3             lan1
4    ge4             lan2
5    ge5             dmz
Router> configure terminal
Router(config)# interface-name ge4 VIP
Router(config)# show interface-name
No.  System Name     User Defined Name
================================================================================
1    ge1             wan1
2    ge2             wan2
3    ge3             lan1
4    ge4             VIP
5    ge5             dmz
Router(config)#
```

This example shows how to restart an interface. You can check all interface names on the ISG50. Then use either the system name or user-defined name of an interface (ge5 or dmz in this example) to restart it.

```
Router(config)# show interface-name
No.  System Name     User Defined Name
================================================================================
====
1    ge1             wan1
2    ge2             wan2
3    ge3             lan1
4    ge4             lan2
5    ge5             dmz
Router> configure terminal
Router(config)# interface reset ge4
Router(config)# interface reset dmz
Router(config)#
```

6.2.2 DHCP Setting Commands

This table lists DHCP setting commands. DHCP is based on DHCP pools. Create a DHCP pool if you want to assign a static IP address to a MAC address or if you want to specify the starting IP address and pool size of a range of IP addresses that can be assigned to DHCP clients. There are different

commands for each configuration. Afterwards, in either case, you have to bind the DHCP pool to the interface.

Table 16 interface Commands: DHCP Settings

COMMAND	DESCRIPTION
`show ip dhcp pool [profile_name]`	Shows information about the specified DHCP pool or about all DHCP pools.
`ip dhcp pool rename profile_name profile_name`	Renames the specified DHCP pool from the first *profile_name* to the second *profile_name*.
`[no] ip dhcp pool profile_name`	Creates a DHCP pool if necessary and enters sub-command mode. You can use the DHCP pool to create a static entry or to set up a range of IP addresses to assign dynamically. About the sub-command settings: • If you use the `host` command, the ISG50 treats this DHCP pool as a static DHCP entry. • If you do not use the `host` command and use the `network` command, the ISG50 treats this DHCP pool as a pool of IP addresses. • If you do not use the `host` command or the `network` command, the DHCP pool is not properly configured and cannot be bound to any interface. The `no` command removes the specified DHCP pool.
`show`	Shows information about the specified DHCP pool.
	Use the following commands if you want to create a static DHCP entry. If you do not use the `host` command, the commands that are not in this section have no effect, but you can still set them.
`[no] host ip`	Specifies the static IP address the ISG50 should assign. Use this command, along with `hardware-address`, to create a static DHCP entry. Note: The IP address must be in the same subnet as the interface to which you plan to bind the DHCP pool. When this command is used, the ISG50 treats this DHCP pool like a static entry, regardless of the `network` setting. The `no` command clears this field.
`[no] hardware-address mac_address`	Reserves the DHCP pool for the specified MAC address. Use this command, along with `host`, to create a static DHCP entry. The `no` command clears this field.
`[no] client-identifier mac_address`	Specifies the MAC address that appears in the DHCP client list. The `no` command clears this field.
`[no] client-name host_name`	Specifies the host name that appears in the DHCP client list. The `no` command clears this field. *host_name*: You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
	Use the following commands if you want to create a pool of IP addresses. These commands have no effect if you use the `host` command. You can still set them, however.

Table 16 interface Commands: DHCP Settings (continued)

COMMAND	DESCRIPTION
network IP/<1..32> network *ip mask* no network	Specifies the IP address and subnet mask of the specified DHCP pool. The subnet mask can be written in w.x.y.z format or in /<1..32> format. Note: The DHCP pool must have the same subnet as the interface to which you plan to bind it. The no command clears these fields.
[no] default-router *ip*	Specifies the default gateway DHCP clients should use. The no command clears this field.
[no] description *description*	Specifies a description for the DHCP pool for identification. The no command removes the description.
[no] domain-name *domain_name*	Specifies the domain name assigned to DHCP clients. The no command clears this field.
[no] starting-address *ip* pool-size <1..65535>	Sets the IP start address and maximum pool size of the specified DHCP pool. The final pool size is limited by the subnet mask. Note: You must specify the network number first, and the start address must be in the same subnet. The no command clears the IP start address and maximum pool size.
[no] first-dns-server {*ip* | *interface_name* {1st-dns | 2nd-dns | 3rd-dns}}	Sets the first DNS server to the specified IP address, the specified interface's first, second, or third DNS server, or the ISG50 itself. The no command resets the setting to its default value.
[no] second-dns-server {*ip* | *interface_name* {1st-dns | 2nd-dns | 3rd-dns}}	Sets the second DNS server to the specified IP address, the specified interface's first, second, or third DNS server, or the ISG50 itself. The no command resets the setting to its default value.
[no] third-dns-server {*ip* | *interface_name* {1st-dns | 2nd-dns | 3rd-dns}}	Sets the third DNS server to the specified IP address, the specified interface's first, second, or third DNS server, or the ISG50 itself. The no command resets the setting to its default value.
[no] first-wins-server *ip*	Specifies the first WINS server IP address to assign to the remote users. The no command removes the setting.
[no] second-wins-server *ip*	Specifies the second WINS server IP address to assign to the remote users. The no command removes the setting.
[no] lease {<0..365> [<0..23> [<0..59>]] | infinite}	Sets the lease time to the specified number of days, hours, and minutes or makes the lease time infinite. The no command resets the first DNS server setting to its default value.
interface *interface_name*	Enters sub-command mode.
[no] ip dhcp-pool *profile_name*	Binds the specified interface to the specified DHCP pool. You have to remove any DHCP relays first. The no command removes the binding.
[no] ip helper-address *ip*	Creates the specified DHCP relay. You have to remove the DHCP pool first, if the DHCP pool is bound to the specified interface. The no command removes the specified DHCP relay.

Table 16 interface Commands: DHCP Settings (continued)

COMMAND	DESCRIPTION
release dhcp *interface-name*	Releases the TCP/IP configuration of the specified interface. The interface must be a DHCP client. This command is available in privilege mode, not configuration mode.
renew dhcp *interface-name*	Renews the TCP/IP configuration of the specified interface. The interface must be a DHCP client. This command is available in privilege mode, not configuration mode.
show ip dhcp binding [*ip*]	Displays information about DHCP bindings for the specified IP address or for all IP addresses.
clear ip dhcp binding {*ip* | *}	Removes the DHCP bindings for the specified IP address or for all IP addresses.

6.2.2.1 DHCP Setting Command Examples

The following example uses these commands to configure DHCP pool DHCP_TEST.

```
Router# configure terminal
Router(config)# ip dhcp pool DHCP_TEST
Router(config-ip-dhcp-pool)#  network 192.168.1.0 /24
Router(config-ip-dhcp-pool)#  domain-name zyxel.com
Router(config-ip-dhcp-pool)#  first-dns-server 10.1.5.1
Router(config-ip-dhcp-pool)#  second-dns-server ge1 1st-dns
Router(config-ip-dhcp-pool)#  third-dns-server 10.1.5.2
Router(config-ip-dhcp-pool)#  default-router 192.168.1.1
Router(config-ip-dhcp-pool)#  lease 0 1 30
Router(config-ip-dhcp-pool)#  starting-address 192.168.1.10 pool-size 30
Router(config-ip-dhcp-pool)#  hardware-address 00:0F:20:74:B8:18
Router(config-ip-dhcp-pool)#  client-identifier 00:0F:20:74:B8:18
Router(config-ip-dhcp-pool)#  client-name TWtester1
Router(config-ip-dhcp-pool)# exit
Router(config)#  interface ge1
Router(config-if)# ip dhcp-pool DHCP_TEST
Router(config-if)# exit
Router(config)# show ip dhcp server status
binding interface : ge1
  binding pool    : DHCP_TEST
```

6.2.3 Interface Parameter Command Examples

This table shows an example of each interface type's sub-commands. The sub-commands vary for different interface types.

Table 17 Examples for Different Interface Parameters

ETHERNET	VIRTUAL INTERFACE	PPPOE/PPTP
Router(config)# interface wan1 Router(config-if-wan1)# description downstream exit ip mac mss mtu no ping-check property shutdown traffic-prioritize type upstream use-defined-mac	Router(config)# interface wan1:1 Router(config-if-vir)# description downstream exit ip no shutdown upstream	Router(config)# interface wan1_ppp Router(config-if-ppp)# account bind connectivity description downstream exit local-address metric mss mtu no ping-check remote-address shutdown traffic-prioritize upstream
CELLULAR	**VLAN**	**BRIDGE**
Router(config)# interface cellular1 Router(config-if-cellular)# account band budget connectivity description device downstream exit local-address metric mtu no pin ping-check remote-address shutdown traffic-prioritize upstream	Router(config)# interface vlan1 Router(config-if-vlan)# description downstream exit ip mss mtu no ping-check port shutdown traffic-prioritize upstream vlan-id	Router(config)# interface br0 Router(config-if-brg)# description downstream exit ip join mss mtu no ping-check shutdown traffic-prioritize upstream

6.2.4 RIP Commands

This table lists the commands for RIP settings.

Table 18 interface Commands: RIP Settings

COMMAND	DESCRIPTION
`router rip`	Enters sub-command mode.
`[no] network` *`interface_name`*	Enables RIP for the specified interface. The no command disables RIP for the specified interface.
`[no] passive-interface` *`interface_name`*	Sets the RIP direction of the specified interface to in-only. The no command makes RIP bi-directional in the specified interface.

Table 18 interface Commands: RIP Settings (continued)

COMMAND	DESCRIPTION
[no] outonly-interface *interface_name*	Sets the RIP direction of the specified interface to out-only. The no command makes RIP bi-directional in the specified interface.
interface *interface_name*	Enters sub-command mode.
[no] ip rip {send | receive} version <1..2>	Sets the send or receive version to the specified version number. The no command sets the send or received version to the current global setting for RIP. See Chapter 9 on page 93 for more information about routing protocols.
[no] ip rip v2-broadcast	Enables RIP-2 packets using subnet broadcasting. The no command uses multi-casting.
show rip {global | interface {all | *interface_name*}}	Displays RIP settings.

6.2.5 OSPF Commands

This table lists the commands for OSPF settings.

Table 19 interface Commands: OSPF Settings

COMMAND	DESCRIPTION
router ospf	Enters sub-command mode.
[no] network *interface_name* area *ip*	Makes the specified interface part of the specified area. The no command removes the specified interface from the specified area, disabling OSPF in this interface.
[no] passive-interface *interface_name*	Sets the OSPF direction of the specified interface to in-only. The no command makes OSPF bi-directional in the specified interface.
interface *interface_name*	Enters sub-command mode.
[no] ip ospf priority <0..255>	Sets the priority of the specified interface to the specified value. The no command sets the priority to 1.
[no] ip ospf cost <1..65535>	Sets the cost to route packets through the specified interface. The no command sets the cost to 10.
no ip ospf authentication	Disables authentication for OSPF in the specified interface.
ip ospf authentication	Enables text authentication for OSPF in the specified interface.
ip ospf authentication message-digest	Enables MD5 authentication for OSPF in the specified interface.
ip ospf authentication same-as-area	To exchange OSPF routing information with peer border routers, you must use the same authentication method that they use. This command makes OSPF authentication in the specified interface follow the settings in the corresponding area.
[no] ip ospf authentication-key *password*	Sets the simple text password for OSPF text authentication in the specified interface. The no command clears the text password. *password*: 1-8 alphanumeric characters or underscores
ip ospf message-digest-key <1..255> md5 *password*	Sets the ID and password for OSPF MD5 authentication in the specified interface. *password*: 1-16 alphanumeric characters or underscores

Table 19 interface Commands: OSPF Settings (continued)

COMMAND	DESCRIPTION
`no ip ospf message-digest-key`	Clears the ID and password for OSPF MD5 authentication in the specified interface.
`[no] ip ospf hello-interval <1..65535>`	Sets the number of seconds between “hello” messages to peer routers. These messages let peer routers know the ISG50 is available. The `no` command sets the number of seconds to 10. See `ip ospf dead-interval` for more information.
`[no] ip ospf dead-interval <1..65535>`	Sets the number of seconds the ISG50 waits for “hello” messages from peer routers before it assumes the peer router is not available and deletes associated routing information. The `no` command sets the number of seconds to 40. See `ip ospf hello-interval` for more information.
`[no] ip ospf retransmit-interval <1..65535>`	Sets the number of seconds the ISG50 waits for an acknowledgment in response to a link state advertisement before it re-sends the advertisement. Link state advertisements (LSA) are used to share the link state and routing information between routers.

6.2.6 Connectivity Check (Ping-check) Commands

Use these commands to have an interface regularly check the connection to the gateway you specified to make sure it is still available. You specify how often the interface checks the connection, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the ISG50 stops routing to the gateway. The ISG50 resumes routing to the gateway the first time the gateway passes the connectivity check.

This table lists the ping-check commands

Table 20 interface Commands: Ping Check

COMMAND	DESCRIPTION
show ping-check [*interface_name* | status]	Displays information about ping check settings for the specified interface or for all interfaces. status: displays the current connectivity check status for any interfaces upon which it is activated.
show ping-check [*interface_name*]	Displays information about ping check settings for the specified interface or for all interfaces.
[no] connectivity-check continuous-log activate	Use this command to have the ISG50 logs connectivity check result continously. The no command disables the setting.
show connectivity-check continuous-log status	Displays the continuous log setting about connectivity check.
interface *interface_name*	Enters sub-command mode.
[no] ping-check activate	Enables ping check for the specified interface. The no command disables ping check for the specified interface.
ping-check {*domain_name* | *ip* | default-gateway}	Specifies what the ISG50 pings for the ping check; you can specify a fully-qualified domain name, IP address, or the default gateway for the interface.
ping-check {*domain_name* | *ip* | default-gateway} period <5..30>	Specifies what the ISG50 pings for the ping check and sets the number of seconds between each ping check.
ping-check {*domain_name* | *ip* | default-gateway} timeout <1..10>	Specifies what the ISG50 pings for the ping check and sets the number of seconds the ISG50 waits for a response.
ping-check {*domain_name* | *ip* | default-gateway} fail-tolerance <1..10>	Specifies what the ISG50 pings for the ping check and sets the number of times the ISG50 times out before it stops routing through the specified interface.
ping-check {*domain_name* | *ip* | default-gateway} method {icmp | tcp}	Sets how the ISG50 checks the connection to the gateway. icmp: ping the gateway you specify to make sure it is still available. tcp: perform a TCP handshake with the gateway you specify to make sure it is still available.
ping-check {*domain_name* | *ip* | default-gateway} port <1..65535>	Specifies the port number to use for a TCP connectivity check.

6.2.6.1 Connectivity Check Command Example

The following commands show you how to set the WAN1 interface to use a TCP handshake on port 8080 to check the connection to IP address 1.1.1.2

```
Router# configure terminal
Router(config)# interface wan1
Router(config-if-wan1)# ping-check 1.1.1.2 method tcp port 8080
Router(config-if-wan1)# exit
Router(config)# show ping-check
Interface: wan1
Check Method: tcp
IP Address: 1.1.1.2
Period: 30
Timeout: 5
Fail Tolerance: 5
Activate: yes
Port: 8080
Router(config)#
```

6.3 Ethernet Interface Specific Commands

This section covers commands that are specific to Ethernet interfaces.

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 21 Input Values for Ethernet Interface Commands

LABEL	DESCRIPTION
interface_name	The name of the Ethernet interface. Use ge*x*, *x* = 1~N, where N equals the highest numbered Ethernet interface for your ISG50 model.

6.3.1 MAC Address Setting Commands

This table lists the commands you can use to set the MAC address of an interface.

Table 22 interface Commands: MAC Setting

COMMAND	DESCRIPTION
interface *interface_name*	Enters sub-command mode.
no mac	Has the interface use its default MAC address.
mac *mac*	Specifies the MAC address the interface is to use.

Table 22 interface Commands: MAC Setting (continued)

COMMAND	DESCRIPTION
type {internal|external|general}	Sets which type of network you will connect this interface. The ISG50 automatically adds default route and SNAT settings for traffic it routes from internal interfaces to external interfaces; for example LAN to WAN traffic. internal: Set this to connect to a local network. Other corresponding configuration options: DHCP server and DHCP relay. The ISG50 automatically adds default SNAT settings for traffic flowing from this interface to an external interface. external: Set this to connect to an external network (like the Internet). This interface is automatically added to the default WAN trunk. general: Set this if you want to manually configure a policy route to add routing and SNAT settings for the interface.
no use-defined-mac	Has the interface use its default MAC address.
use-defined-mac	Has the interface use a MAC address that you specify.

6.3.2 Port Grouping Commands

This section covers commands that are specific to port grouping.

Note: In CLI, representative interfaces are also called representative ports.

Table 23 Basic Interface Setting Commands

COMMAND	DESCRIPTION
show port-grouping	Displays which physical ports are assigned to each representative interface.
port-grouping *representative_interface* port <1..*x*>	Adds the specified physical port to the specified representative interface. *representative_interface*: ge*x* <1..*x*> where *x* equals the highest numbered port for your ISG50 model.
no port <1..*x*>	Removes the specified physical port from its current representative interface and adds it to its default representative interface (for example, port *x* --> ge*x*).
port status Port<1..*x*>	Enters a sub-command mode to configure the specified port's settings.
[no] duplex <full | half>	Sets the port's duplex mode. The no command returns the default setting.
exit	Leaves the sub-command mode.
[no] negotiation auto	Sets the port to use auto-negotiation to determine the port speed and duplex. The no command turns off auto-negotiation.
[no] speed <100,10>	Sets the Ethernet port's connection speed in Mbps. The no command returns the default setting.

Table 23 Basic Interface Setting Commands (continued)

COMMAND	DESCRIPTION
show port setting	Displays the Ethernet port negotiation, duplex, and speed settings.
show port status	Displays statistics for the Ethernet ports.

6.3.2.1 Port Grouping Command Examples

The following commands add physical port 5 to representative interface ge1.

```
Router# configure terminal
Router(config)# show port-grouping
No. Representative Name  Port1 Port2 Port3 Port4 Port5
=========================================================
1   ge1                  yes   no    no    no    no
2   ge2                  no    yes   no    no    no
3   ge3                  no    no    yes   no    no
4   ge4                  no    no    no    yes   no
5   ge5                  no    no    no    no    yes
Router(config)# port-grouping ge1
Router(config-port-grouping)# port 5
Router(config-port-grouping)# exit
Router(config)# show port-grouping
No. Representative Name  Port1 Port2 Port3 Port4 Port5
=========================================================
1   ge1                  yes   no    no    no    yes
2   ge2                  no    yes   no    no    no
3   ge3                  no    no    yes   no    no
4   ge4                  no    no    no    yes   no
5   ge5                  no    no    no    no    no
```

The following commands set port 1 to use auto-negotiation auto and port 2 to use a 10 Mbps connection speed and half duplex.

```
Router(config)# port status Port1
Router(config-port-status)# negotiation auto
Router(config-port-status)# exit
Router(config)# port status Port2
Router(config-port-status)# duplex half
Router(config-port-status)# speed 10
Router(config-port-status)# exit
Router(config)# exit
```

6.4 Virtual Interface Specific Commands

Virtual interfaces use many of the general interface commands discussed at the beginning of Section 6.2 on page 54. There are no additional commands for virtual interfaces.

6.4.1 Virtual Interface Command Examples

The following commands set up a virtual interface on top of Ethernet interface ge1. The virtual interface is named ge1:1 with the following parameters: IP 1.2.3.4, subnet 255.255.255.0, gateway 4.6.7.8, upstream bandwidth 345, downstream bandwidth 123, and description “I am vir interface”.

```
Router# configure terminal
Router(config)# interface ge1:1
Router(config-if-vir)# ip address 1.2.3.4 255.255.255.0
Router(config-if-vir)# ip gateway 4.6.7.8
Router(config-if-vir)# upstream 345
Router(config-if-vir)# downstream 123
Router(config-if-vir)# description I am vir interface
Router(config-if-vir)# exit
```

6.5 PPPoE/PPTP Specific Commands

This section covers commands that are specific to PPPoE/PPTP interfaces. PPPoE/PPTP interfaces also use many of the general interface commands discussed at the beginning of Section 6.2 on page 54.

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 24 Input Values for PPPoE/PPTP Interface Commands

LABEL	DESCRIPTION
interface_name	PPPoE/PPTP interface: ppp*x*, *x* = 0 - N, where N depends on the number of PPPoE/PPTP interfaces your ISG50 model supports.
profile_name	The name of the ISP account. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

This table lists the PPPoE/PPTP interface commands.

Table 25 interface Commands: PPPoE/PPTP Interfaces

COMMAND	DESCRIPTION
`interface dial` *interface_name*	Connects the specified PPPoE/PPTP interface.
`interface disconnect` *interface_name*	Disconnects the specified PPPoE/PPTP interface.
`interface` *interface_name*	Creates the specified interface if necessary and enters sub-command mode.
`[no] account` *profile_name*	Specifies the ISP account for the specified PPPoE/PPTP interface. The no command clears the ISP account field.
`[no] bind` *interface_name*	Specifies the base interface for the PPPoE/PPTP interface. The no command removes the base interface.
`[no] connectivity {nail-up | dial-on-demand}`	Specifies whether the specified PPPoE/PPTP interface is always connected (nail-up) or connected only when used (dial-on-demand). The no command sets it to dial-on-demand.

Table 25 interface Commands: PPPoE/PPTP Interfaces (continued)

COMMAND	DESCRIPTION
[no] local-address *ip*	Specifies a static IP address for the specified PPPoE/PPTP interface. The no command makes the PPPoE/PPTP interface a DHCP client; the other computer assigns the IP address.
[no] remote-address *ip*	Specifies the IP address of the PPPoE/PPTP server. If the PPPoE/PPTP server is not available at this IP address, no connection is made. The no command lets the ISG50 get the IP address of the PPPoE/PPTP server automatically when it establishes the connection.
[no] mss <536..1452>	Specifies the maximum segment size (MSS) the interface can use. MSS is the largest amount of data, specified in bytes, that the interface can handle in a single, unfragmented piece. The no command has the ISG50 use its default MSS setting.
mtu <576..1492>	Sets the Maximum Transmission Unit in bytes.
show interface ppp system-default	Displays system default PPP interfaces (non-deletable) that come with the ISG50.
show interface ppp user-define	Displays all PPP interfaces that were manually configured on the ISG50.

6.5.1 PPPoE/PPTP Interface Command Examples

The following commands show you how to configure PPPoE/PPTP interface ppp0 with the following characteristics: base interface ge1, ISP account **Hinet**, local address 1.1.1.1, remote address 2.2.2.2, MTU 1200, upstream bandwidth 345, downstream bandwidth 123, description “I am ppp0”, and dialed only when used.

```
Router# configure terminal
Router(config)# interface ppp0
Router(config-if-ppp)# account Hinet
Router(config-if-ppp)# bind ge1
Router(config-if-ppp)# local-address 1.1.1.1
Router(config-if-ppp)# remote-address 2.2.2.2
Router(config-if-ppp)# mtu 1200
Router(config-if-ppp)# upstream 345
Router(config-if-ppp)# downstream 123
Router(config-if-ppp)# connectivity dial-on-demand
Router(config-if-ppp)# description I am ppp0
Router(config-if-ppp)# exit
```

The following commands show you how to connect and disconnect ppp0.

```
Router# interface dial ppp0
Router# interface disconnect ppp0
```

6.6 Cellular Interface Specific Commands

Use a 3G (Third Generation) cellular device with the ISG50 for wireless broadband Internet access.

Use these commands to add, edit, dial, disconnect, or delete cellular interfaces. When you add a new cellular interface, make sure you enter the account. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 26 Cellular Interface Commands

COMMAND	DESCRIPTION
`[no] interface` *`interface_name`*	Creates the specified interface if necessary and enters sub-command mode. The `no` command deletes the specified interface.
`[no] account` *`profile_name`*	Specifies the ISP account for the specified cellular interface. The `no` command clears the ISP account field.
`[no] band {auto|wcdma|gsm}`	Sets (or clears) the cellular band that the cellular interface uses. `auto` has the ISG50 always use the fastest network that is in range. `gsm` has this interface only use a 2.5G or 2.75G network (respectively). If you only have a GSM network available to you, you may want to use this so the ISG50 does not spend time looking for a WCDMA network. `wcdma` has this interface only use a 3G or 3.5G network (respectively). You may want to use this if you want to make sure the interface does not use the GSM network.
`[no] network-selection {auto|home}`	Home network is the network to which you are originally subscribed. `Home` has the 3G device connect only to the home network. If the home network is down, the ISG50's 3G Internet connection is also unavailable. `Auto` is the default setting and allows the 3G device to connect to a network to which you are not subscribed when necessary, for example when the home network is down or another 3G base station's signal is stronger. This is recommended if you need continuous Internet connectivity. If you select this, you may be charged using the rate of a different network.
`[no] budget active`	Sets a monthly limit for the user account of the installed 3G card. You can set a limit on the total traffic and/or call time. The ISG50 takes the actions you specified when a limit is exceeded during the month. Use the no command to disable budget control.
`[no] budget time active <1..672>`	Sets the amount of time (in hours) that the 3G connection can be used within one month. If you change the value, the ISG50 resets the statistics. Use the no command to disable time budget control.

Table 26 Cellular Interface Commands (continued)

COMMAND	DESCRIPTION
[no] budget data active {download-upload|download|upload} <1..100000>	Sets how much downstream and/or upstream data (in Mega bytes) can be transmitted via the 3G connection within one month. download: set a limit on the downstream traffic (from the ISP to the ISG50). upload: set a limit on the upstream traffic (from the ISG50 to the ISP). download-upload: set a limit on the total traffic in both directions. If you change the value, the ISG50 resets the statistics. Use the no command to disable data budget control.
budget reset-day <0..31>	Sets the date on which the ISG50 resets the budget every month. If the date you selected is not available in a month, such as 30th or 31th, the ISG50 resets the budget on the last day of the month.
budget reset-counters	Resets the time and data budgets immediately. The count starts over with the 3G connection's full configured monthly time and data budgets. This does not affect the normal monthly budget restart.
budget {log|log-alert}[recursive <1..65535>]	Sets the ISG50 to create a log (log) or an alert log (log-alert) when the time or data limit is exceeded. You can also specify how often (from 1 to 65535 minutes) to generate a log or an alert.
no budget log [recursive]	Sets the ISG50 to not create a log when the time or data limit is exceeded. Specify recursive to have the ISG50 only create a log one time when the time or data limit is exceeded.
budget new-connection {allow|disallow}	Sets to permit (allow) or drop/block (disallow) new 3G connections when the time or data limit is exceeded.
budget current-connection {keep|drop}	Sets to maintain the existing 3G connection (keep) or disconnect it (drop) when the time or data limit is exceeded. You cannot set budget new-connection to allow and budget current-connection to drop at the same time. If you set budget new-connection to disallow and budget current-connection to keep, the ISG50 allows you to transmit data using the current connection, but you cannot build a new connection if the existing connection is disconnected.
budget percentage {ptime|pdata} <0..99>	Sets a percentage (0~99) of time budget (ptime) or data (pdata) limit. When the specified limit is exceeded, the ISG50 takes the action configured using the budget {log-percentage|log-percentage-alert} command.
budget {log-percentage|log-percentage-alert} [recursive <1..65535>]	Sets to have the ISG50 create a log (log-percentage) or an alart log (log-percentage-alert) when the set percentage of time budget or data limit is exceeded. You can configure the percentage using the budget percentage command. You can also set how often (from 1 to 65535 minutes) to send the log or alert.

Table 26 Cellular Interface Commands (continued)

COMMAND	DESCRIPTION
`no budget log-percentage [recursive]`	Sets the ISG50 to not create a log when the set percentage of time budget or data limit is exceeded. You can configure the percentage using the `budget percentage` command. You can also specify `recursive` to have the ISG50 only create a log one time when the set percentage of time budget or data limit is exceeded.
`connectivity {nail-up | dial-on-demand}`	Sets the connection to be always on or only when there is traffic.
`[no] device <device_model_name>`	Sets (or clears) the model name of the cellular device that the cellular interface uses. Use 0-30 alphanumeric characters, underscores(_), or dashes (-).
`[no] local-address <ip>`	Sets (or clears) the cellular interface's local (own) IP address.
`mtu <576..1492>`	Sets the Maximum Transmission Unit in bytes.
`[no] pin <pin code>`	Sets (or clears) the PIN code for the cellular device's 3G card. Use 1-4 alphanumeric characters, underscores(_), or dashes (-).
`[no] remote-address <ip>`	Sets (or clears) the IP address of the cellular interface's peer (like a gateway or PPPoE server).
`interface cellular budget-auto-save <5..1440>`	Sets how often (in minutes) the ISG50 saves time and data usage records for a connection using the 3G card.
`show interface cellular [corresponding-slot|device-status|support-device]`	Shows the status of the specified cellular interface.
`show interface cellular corresponding-slot`	Shows which cellular interface is on which slot and whether which cellular interface has been configured.
`show interface cellular device-status`	Displays the installed SIM card and 3G card status.
`show interface cellular support-device`	Displays all 3G card models the ISG50 can support.
`show interface cellular budget-auto-save`	Displays how often (in minutes) the ISG50 records time and data usage of your 3G budgets.
`show interface cellular status`	Displays the traffic statistics and connection status for your cellular interfaces. See Section 6.6.1 on page 72 for all possible cellular status descriptions.
`show interface interface_name [budget]`	Displays the budget control settings for the specified cellular interface.
`show interface interface_name device status`	Displays the 3G card and SIM card information for the specified cellular interface.
`show interface interface_name device profile`	Displays the 3G connection profile settings of the specified cellular interface.

6.6.1 Cellular Status

The following table describes the different kinds of cellular connection status on the ISG50.

Table 27 Cellular Status

STATUS	DESCRIPTION
No device	no 3G device is connected to the ISG50.
No service	no 3G network is available in the area; you cannot connect to the Internet.

Table 27 Cellular Status

STATUS	DESCRIPTION
Limited service	returned by the service provider in cases where the SIM card is expired, the user failed to pay for the service and so on; you cannot connect to the Internet.
Device detected	displays when you connect a 3G device.
Device error	a 3G device is connected but there is an error.
Probe device fail	the ISG50's test of the 3G device failed.
Probe device ok	the ISG50's test of the 3G device failed.
Init device fail	the ISG50 was not able to initialize the 3G device.
Init device ok	the ISG50 initialized the 3G card.
Check lock fail	the ISG50's check of whether or not the 3G device is locked failed.
Device locked	the 3G device is locked.
SIM error	there is a SIM card error on the 3G device.
SIM locked-PUK	the PUK is locked on the 3G device's SIM card.
SIM locked-PIN	the PIN is locked on the 3G device's SIM card.
Unlock PUK fail	Your attempt to unlock a WCDMA 3G device's PUK failed because you entered an incorrect PUK.
Unlock PIN fail	Your attempt to unlock a WCDMA 3G device's PIN failed because you entered an incorrect PIN.
Unlock device fail	Your attempt to unlock a CDMA2000 3G device failed because you entered an incorrect device code.
Device unlocked	You entered the correct device code and unlocked a CDMA2000 3G device.
Get dev-info fail	The ISG50 cannot get cellular device information.
Get dev-info ok	The ISG50 succeeded in retrieving 3G device information.
Searching network	The 3G device is searching for a network.
Get signal fail	The 3G device cannot get a signal from a network.
Network found	The 3G device found a network.
Apply config	The ISG50 is applying your configuration to the 3G device.
Inactive	The 3G interface is disabled.
Active	The 3G interface is enabled.
Incorrect device	The connected 3G device is not compatible with the ISG50.
Correct device	The ISG50 detected a compatible 3G device.
Set band fail	Applying your band selection was not successful.
Set band ok	The ISG50 successfully applied your band selection.
Set profile fail	Applying your ISP settings was not successful.
Set profile ok	The ISG50 successfully applied your ISP settings.
PPP fail	The ISG50 failed to create a PPP connection for the cellular interface.
Need auth-password	You need to enter the password for the 3G card in the cellular edit screen.
Device ready	The ISG50 successfully applied all of your configuration and you can use the 3G connection.

6.6.2 Cellular Interface Command Examples

This example shows the configuration of a cellular interface named cellular2 for use with a Sierra Wireless AC850 3G card. It uses only a 3G (or 3.5G) connection, PIN code 1234, an MTU of 1200 bytes, a description of "This is cellular2" and sets the connection to be nailed-up.

```
Router(config)# interface cellular2
Router(config-if-cellular)# device AC850
Router(config-if-cellular)# band wcdma
Router(config-if-cellular)# pin 1234
Router(config-if-cellular)# connectivity nail-up
Router(config-if-cellular)# description This is cellular2
Router(config-if-cellular)# mtu 1200
Router(config-if-cellular)# exit
```

This second example shows specifying a new PIN code of 4567.

```
Router(config)# interface cellular2
Router(config-if-cellular)# pin 4567
Router(config-if-cellular)# exit
```

This example shows the 3G and SIM card information for interface cellular2 on the ISG50.

```
Router(config)# show interface cellular2 device status
interface name: cellular2
extension slot: USB 1
service provider: Chunghwa Telecom
cellular system: WCDMA
signal strength: -95 dBm
signal quality: Poor
device type: WCDMA
device manufacturer: Huawei
device model: E220/E270/E800A
device firmware: 076.11.07.106
device IMEI/ESN: 351827019784694
SIM card IMSI: 466923100565274
```

This example shows the 3G connection profile settings for interface cellular2 on the ISG50. You have to dial *99***1# to use profile 1, but authentication is not required. Dail *99***2# to use profile 2 and authentication is required.

```
Router(config)# show interface cellular2 device profile
profile: 1
apn: internet
dial-string: *99***1#
authentication: none
user: n/a
password: n/a
profile: 2
apn: internet
dial-string: *99***2#
authentication: chap
user:
password: ***
----------------------SNIP!-----------------------------------------------
```

6.7 USB Storage Specific Commands

Use these commands to configure settings that apply to the USB storage device connected to the ISG50.

Note: For the ISG50 which supports more than one USB ports, these commands only apply to the USB storage device that is first attached to the ISG50.

Table 28 USB Storage General Commands

COMMAND	DESCRIPTION
show usb-storage	Displays the status of the connected USB storage device.
[no] usb-storage activate	Enables or disables the connected USB storage service.
usb-storage warn *number* <*percentage*|megabyte>	Sets a number and the unit (percentage or megabyte) to send a warning message when the remaining USB storage space is less than the set value.
usb-storage mount	Mounts the connected USB storage device.
usb-storage umount	Unmounts the connected USB storage device.
[no] logging usb-storage	Sets to have the ISG50 log or not log any information about the connected USB storage device(s) for the system log.
show logging status usb-storage	Displays the logging settings for the connected USB storage device.
logging usb-storage category *category* level <all|normal>	Configures the logging settings for the specified category for the connected USB storage device.
logging usb-storage category *category* disable	Stops logging for the specified category to the connected USB storage device.
logging usb-storage flushThreshold <1..100>	Configures the maximum storage space (in percentage) for storing syetem logs on the connected USB storage device.

Table 28 USB Storage General Commands (continued)

COMMAND	DESCRIPTION
`[no] diag-info copy usb-storage`	Sets to have the ISG50 save or stop saving the current system diagnostics information to the connected USB storage device. You may need to send this file to customer support for troubleshooting.
`show diag-info copy usb-storage`	Displays whether (enable or disable) the ISG50 saves the current system diagnostics information to the connected USB storage device.
`[no] corefile copy usb-storage`	Sets to have the ISG50 save or not save a process's core dump to the connected USB storage device if the process terminates abnormally (crashes). You may need to send this file to customer support for troubleshooting.
`show corefile copy usb-storage`	Displays whether (enable or disable) the ISG50 saves core dump files to the connected USB storage device.

6.7.1 USB Storage General Commands Example

This example shows how to display the status of the connected USB storage device.

```
Router> show usb-storage
USBStorage Configuration:
Activation: enable
Criterion Number: 100
Criterion Unit: megabyte
USB Storage Status:
Device description: N/A
Usage: N/A
Filesystem: N/A
Speed: N/A
Status: none
Detail: none
```

6.8 VLAN Interface Specific Commands

This section covers commands that are specific to VLAN interfaces. VLAN interfaces also use many of the general interface commands discussed at the beginning of Section 6.2 on page 54.

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 29 Input Values for VLAN Interface Commands

LABEL	DESCRIPTION
interface_name	VLAN interface: vlan*x*, *x* = 0 - 4094 Ethernet interface: Use ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your ISG50 model.

This table lists the VLAN interface commands.

Table 30 interface Commands: VLAN Interfaces

COMMAND	DESCRIPTION
`interface` *`interface_name`*	Creates the specified interface if necessary and enters sub-command mode.
`[no] port` *`interface_name`*	Specifies the Ethernet interface on which the VLAN interface runs. The `no` command clears the port.
`[no] vlan-id <1..4094>`	Specifies the VLAN ID used to identify the VLAN. The `no` command clears the VLAN ID.
`show port vlanid`	Displays the Ethernet interface VLAN settings.

6.8.1 VLAN Interface Command Examples

The following commands show you how to set up VLAN vlan100 with the following parameters: VLAN ID 100, interface ge1, IP 1.2.3.4, subnet 255.255.255.0, MTU 598, gateway 2.2.2.2, description "I am vlan100", upstream bandwidth 345, and downstream bandwidth 123.

```
Router# configure terminal
Router(config)# interface vlan100
Router(config-if-vlan)# vlan-id 100
Router(config-if-vlan)# port ge1
Router(config-if-vlan)# ip address 1.2.3.4 255.255.255.0
Router(config-if-vlan)# ip gateway 2.2.2.2
Router(config-if-vlan)# mtu 598
Router(config-if-vlan)# upstream 345
Router(config-if-vlan)# downstream 123
Router(config-if-vlan)# description I am vlan100
Router(config-if-vlan)# exit
```

6.9 Bridge Specific Commands

This section covers commands that are specific to bridge interfaces. Bridge interfaces also use many of the general interface commands discussed at the beginning of Section 6.2 on page 54.

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 31 Input Values for Bridge Interface Commands

LABEL	DESCRIPTION
`interface_name`	The name of the interface. Ethernet interface: Use ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your ISG50 model. VLAN interface: vlan*x*, *x* = 0 - 4094 bridge interface: br*x*, *x* = 0 - N, where N depends on the number of bridge interfaces your ISG50 model supports.

This table lists the bridge interface commands.

Table 32 interface Commands: Bridge Interfaces

COMMAND	DESCRIPTION
`interface` *`interface_name`*	Creates the specified interface if necessary and enters sub-command mode.
`[no] join` *`interface_name`*	Adds the specified Ethernet interface or VLAN interface to the specified bridge. The `no` command removes the specified interface from the specified bridge.
`show bridge available member`	Displays the available interfaces that could be added to a bridge.

6.9.1 Bridge Interface Command Examples

The following commands show you how to set up a bridge interface named br0 with the following parameters: member ge1, IP 1.2.3.4, subnet 255.255.255.0, MTU 598, gateway 2.2.2.2, upstream bandwidth 345, downstream bandwidth 123, and description “I am br0”.

```
Router# configure terminal
Router(config)# interface br0
Router(config-if-brg)# join ge1
Router(config-if-brg)# ip address 1.2.3.4 255.255.255.0
Router(config-if-brg)# ip gateway 2.2.2.2
Router(config-if-brg)# mtu 598
Router(config-if-brg)# upstream 345
Router(config-if-brg)# downstream 123
Router(config-if-brg)# description I am br0
Router(config-if-brg)# exit
```

7

Trunks

This chapter shows you how to configure trunks on your ISG50.

7.1 Trunks Overview

You can group multiple interfaces together into trunks to have multiple connections share the traffic load to increase overall network throughput and enhance network reliability. If one interface's connection goes down, the ISG50 sends traffic through another member of the trunk. For example, you can use two interfaces for WAN connections. You can connect one interface to one ISP (or network) and connect the another to a second ISP (or network). The ISG50 can balance the load between multiple connections. If one interface's connection goes down, the ISG50 can automatically send its traffic through another interface.

You can use policy routing to specify through which interface to send specific traffic types. You can use trunks in combination with policy routing. You can also define multiple trunks for the same physical interfaces. This allows you to send specific traffic types through the interface that works best for that type of traffic, and if that interface's connection goes down, the ISG50 can still send its traffic through another interface.

7.2 Trunk Scenario Examples

Suppose one of the ISG50's interfaces is connected to an ISP that is also your Voice over IP (VoIP) service provider. You may want to set that interface as active and set another interface (connected to another ISP) to passive. This way VoIP traffic goes through the interface connected to the VoIP service provider whenever the interface's connection is up.

Another example would be if you use multiple ISPs that provide different levels of service to different places. Suppose ISP A has better connections to Europe while ISP B has better connections to Australia. You could use policy routing and trunks to send traffic for your European branch offices primarily through ISP A and traffic for your Australian branch offices primarily through ISP B.

7.3 Trunk Commands Input Values

The following table explains the values you can input with the `interface-group` commands.

Table 33 interface-group Command Input Values

LABEL	DESCRIPTION
group-name	A descriptive name for the trunk. Use up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive.
interface-name	The name of an interface, it could be an Ethernet, PPP, VLAN or bridge interface. The possible number of each interface type and the abbreviation to use are as follows. Ethernet interface: Use ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your ISG50 model. PPPoE/PPTP interface: ppp*x*, *x* = 0 - N, where N depends on the number of PPPoE/PPTP interfaces your ISG50 model supports. VLAN interface: vlan*x*, *x* = 0 - 4094 bridge interface: br*x*, *x* = 0 - N, where N depends on the number of bridge interfaces your ISG50 model supports.
num	The interface's position in the trunk's list of members <1..8>.
<CR>	Carriage Return (the "enter" key).

7.4 Trunk Commands Summary

The following table lists the `interface-group` commands. You must use the `configure terminal` command to enter the configuration mode before you can use these commands. See Table 33 on page 80 for details about the values you can input with these commands.

Table 34 interface-group Commands Summary

COMMAND	DESCRIPTION
`show interface-group {system-default|user-define|`*`group-name`*`}`	Displays pre-configured system default trunks, your own user configuration trunks or a specified trunk's settings.
`[no] interface-group` *`group-name`*	Creates a trunk name and enters the trunk sub-command mode where you can configure the trunk. The `no` command removes the trunk.
`algorithm {wrr|llf|spill-over}`	Sets the trunk's load balancing algorithm.
`exit`	Leaves the trunk sub-command mode.
`flush`	Deletes a trunk's interface settings.
`interface {`*`num`*`|append|insert` *`num`*`}` *`interface-name`* `[weight <1..10>|limit <1..2097152>|passive]`	This subcommand adds an interface to a trunk. Sets the interface's number. It also sets the interface's weight and spillover limit or sets it to be passive.

Table 34 interface-group Commands Summary (continued)

COMMAND	DESCRIPTION
loadbalancing-index <outbound|inbound|total>	Use this command only if you use least load first or spill-over as the trunk's load balancing algorithm. Set either outbound, inbound or outbound and inbound traffic (total) to which the ISG50 will apply the specified algorithm. Outbound traffic means the traffic travelling from an internal interface (ex. LAN) to an external interface (ex. WAN). Inbound traffic means the opposite.
mode {normal|trunk}	Sets the mode for a trunk. Do this first in the trunk's sub-command mode.
move <1..8> to <1..8>	Changes a the interface order in a trunk.
[no] interface {*num*|*interface-name*}	Removes an interface from the trunk.
system default-interface-group *group-name*	Sets the ISG50 to first attempt to use the specified WAN trunk for routing traffic going through the ISG50.
system default-interface-group system-service *group-name*	Sets the ISG50 to first attempt to use the specified WAN trunk for routing traffic originating from the ISG50 itself. This includes the PBX traffic. The trunk can only have one member interface set to active mode.
[no] system default-snat	Enables or disables Source NAT (SNAT). When SNAT is enabled, the ISG50 uses the IP address of the outgoing interface as the source IP address of the packets it sends out through the WAN interfaces.
show system default-snat	Displays whether the ISG50 enable SNAT or not. The ISG50 performs SNAT by default for traffic going to or from the WAN interfaces.
show system default-interface-group	Displays the WAN trunk the ISG50 first attempts to use for routing traffic going through the ISG50.
show system default-interface-group system-service	Displays the WAN trunk the ISG50 first attempts to use for routing traffic originating from the ISG50 itself. This includes the PBX traffic.

7.5 Trunk Command Examples

The following example creates a weighted round robin trunk for Ethernet interfaces ge1 and ge2. The ISG50 sends twice as much traffic through ge1.

```
Router# configure terminal
Router(config)# interface-group wrr-example
Router(if-group)# mode trunk
Router(if-group)# algorithm wrr
Router(if-group)# interface 1 ge1 weight 2
Router(if-group)# interface 2 ge2 weight 1
Router(if-group)# exit
Router(config)#
```

The following example creates a least load first trunk for Ethernet interface ge3 and VLAN 5, which will only apply to outgoing traffic through the trunk. The ISG50 sends new session traffic through the least utilized of these interfaces.

```
Router# configure terminal
Router(config)# interface-group llf-example
Router(if-group)# mode trunk
Router(if-group)# algorithm llf
Router(if-group)# interface 1 ge3
Router(if-group)# interface 2 vlan5
Router(if-group)# loadbalancing-index outbound
Router(if-group)# exit
Router(config)#
```

The following example creates a spill-over trunk for Ethernet interfaces ge1 and ge3, which will apply to both incoming and outgoing traffic through the trunk.. The ISG50 sends traffic through ge1 until it hits the limit of 1000 kbps. The ISG50 sends anything over 1000 kbps through ge3.

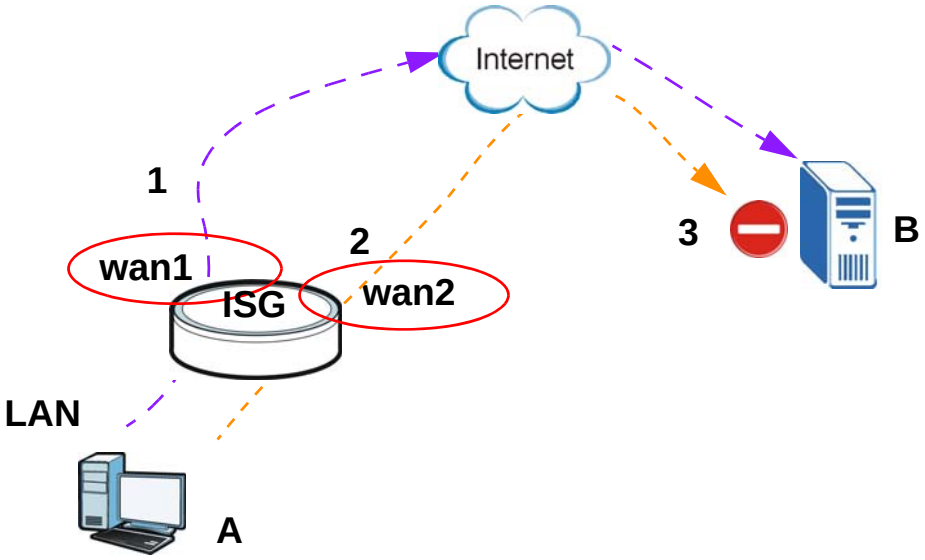
```
Router# configure terminal
Router(config)# interface-group spill-example
Router(if-group)# mode trunk
Router(if-group)# algorithm spill-over
Router(if-group)# interface 1 ge1 limit 1000
Router(if-group)# interface 2 ge3 limit 1000
Router(if-group)# loadbalancing-index total
Router(if-group)# exit
Router(config)#
```

Link Sticking

You can have the ISG50 send each local computer's traffic that is going to the same destination through a single WAN interface for a specified period of time. This is useful when a server requires authentication. For example, the ISG50 sends a user's traffic through one WAN IP address when he

logs into a server B. If the user's subsequent sessions came from a different WAN IP address, the server would deny them. Here is an example.

Figure 14 Link Sticking



1 LAN user **A** logs into server **B** on the Internet. The ISG50 uses wan1 to send the request to server **B**.

2 The ISG50 is using active/active load balancing. So when LAN user **A** tries to access something on the server, the request goes out through wan2.

3 The server finds that the request comes from wan2's IP address instead of wan1's IP address and rejects the request.

If link sticking had been configured, the ISG50 would have still used wan1 to send LAN user **A**'s request to the server and server would have given the user **A** access.

7.6 Link Sticking Commands Summary

The following table lists the `ip load-balancing link-sticking` commands for link sticking. (The link sticking commands have the prefix `ip load-balancing` because they affect the ISG50's load balancing behavior.) You must use the `configure terminal` command to enter the configuration mode before you can use these commands. See Table 33 on page 80 for details about the values you can input with these commands.

Table 35 ip load-balancing link-sticking Commands Summary

COMMAND	DESCRIPTION
`[no] ip load-balancing link-sticking activate`	Turns link sticking on or off.

Table 35 ip load-balancing link-sticking Commands Summary (continued)

COMMAND	DESCRIPTION
`[no] ip load-balancing link-sticking timeout` *`timeout`*	Sets for how many seconds (30-3600) the ISG50 sends all of each local computer's traffic through one WAN interface.
`show ip load-balancing link-sticking status`	Displays the current link sticking settings.

7.7 Link Sticking Command Example

This example shows how to activate link sticking and set the timeout to 600 seconds (ten minutes).

```
Router(config)# ip load-balancing link-sticking activate
Router(config)# ip load-balancing link-sticking timeout 600
Router(config)# show ip load-balancing link-sticking status
active    : yes
timeout   : 300
```

8

Route

This chapter shows you how to configure policies for IP routing and static routes on your ISG50.

8.1 Policy Route

Traditionally, routing is based on the destination address only and the ISG50 takes the shortest path to forward a packet. IP Policy Routing (IPPR) provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to incoming packets on a per interface basis, prior to the normal routing.

8.2 Policy Route Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 36 Input Values for General Policy Route Commands

LABEL	DESCRIPTION
address_object	The name of the IP address (group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
interface_name	The name of the interface. Ethernet interface: Use ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your ISG50 model. virtual interface on top of Ethernet interface: add a colon (:) and the number of the virtual interface. For example: ge*x*:*y*, *x* = 1 - N, *y* = 1 - 4 VLAN interface: vlan*x*, *x* = 0 - 4094 virtual interface on top of VLAN interface: vlan*x*:*y*, *x* = 0 - 4094, *y* = 1 - 12 bridge interface: br*x*, *x* = 0 - N, where N depends on the number of bridge interfaces your ISG50 model supports. virtual interface on top of bridge interface: br*x*:*y*, *x* = the number of the bridge interface, *y* = 1 - 4 PPPoE/PPTP interface: ppp*x*, *x* = 0 - N, where N depends on the number of PPPoE/PPTP interfaces your ISG50 model supports.
policy_number	The number of a policy route. 1 - *X* where *X* is the highest number of policy routes the ISG50 model supports. See the ISG50's User's Guide for details.
schedule_object	The name of the schedule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

Table 36 Input Values for General Policy Route Commands (continued)

LABEL	DESCRIPTION
service_name	The name of the service (group). You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
user_name	The name of a user (group). You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

The following table describes the commands available for policy route. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 37 Command Summary: Policy Route

COMMAND	DESCRIPTION
`[no] bwm activate`	Globally enables bandwidth management. You must globally activate bandwidth management to have individual policy routes apply bandwidth management. The `no` command globally disables bandwidth management.
`policy {`*`policy_number`* `| append | insert` *`policy_number`*`}`	Enters the policy-route sub-command mode to configure, add or insert a policy.
`[no] auto-destination`	When you set `tunnel` as the next-hop type (using the `next-hop tunnel` command) for this route, you can use this command to have the ISG50 use the local network of the peer router that initiated an incoming dynamic IPSec tunnel as the destination address of the policy instead of what you configure by using the `destination` command. The `no` command disables the setting.
`[no] auto-disable`	When you set `interface` or `trunk` as the next-hop type (using the `next-hop interface` or `next-hop trunk` command) for this route, you can use this command to have the ISG50 automatically disable this policy route when the next-hop's connection is down. The `no` command disables the setting.
`[no] bandwidth <1..1048576> priority <1..1024> [maximize-bandwidth-usage]`	Sets the maximum bandwidth and priority for the policy. The `no` command removes bandwidth settings from the rule. You can also turn maximize bandwidth usage on or off.
`[no] deactivate`	Disables the specified policy. The `no` command enables the specified policy.
`[no] description` *`description`*	Sets a descriptive name for the policy. The `no` command removes the name for the policy.
`[no] destination {`*`address_object`*`|any}`	Sets the destination IP address the matched packets must have. The `no` command resets the destination IP address to the default (any). any means all IP addresses.
`[no] dscp {any | <0..63>}`	Sets a custom DSCP code point (0~63). This is the DSCP value of incoming packets to which this policy route applies. any means all DSCP value or no DSCP marker.

Table 37 Command Summary: Policy Route (continued)

COMMAND	DESCRIPTION
[no] dscp class {default | *dscp_class*}	Sets a DSCP class. Use default to apply this policy route to incoming packets that are marked with DSCP value 0. Use one of the pre-defined AF classes (including af11~af13, af21~af23, af31~af33, and af41~af43) to apply this policy route to incoming packets that are marked with the DSCP AF class. The "af" entries stand for Assured Forwarding. The number following the "af" identifies one of four classes and one of three drop preferences. See Assured Forwarding (AF) PHB for DiffServ on page 88 for more details.
dscp-marking <0..63>	Sets a DSCP value to have the ISG50 apply that DSCP value to the route's outgoing packets.
dscp-marking class {default | *dscp_class*}	Sets how the ISG50 handles the DSCP value of the outgoing packets that match this route. Set this to default to have the ISG50 set the DSCP value of the packets to 0. Set this to an "af" class (including af11~af13, af21~af23, af31~af33, and af41~af43) which stands for Assured Forwarding. The number following the "af" identifies one of four classes and one of three drop preferences. See Assured Forwarding (AF) PHB for DiffServ on page 88 for more details.
no dscp-marking	Use this command to have the ISG50 not modify the DSCP value of the route's outgoing packets.
[no] interface *interface_name*	Sets the interface on which the incoming packets are received. The no command resets the incoming interface to the default (any). any means all interfaces.
[no] next-hop {auto|gateway *address object* |interface *interface_name* |trunk *trunk_name*|tunnel *tunnel_name*}	Sets the next-hop to which the matched packets are routed. The no command resets next-hop settings to the default (auto).
[no] schedule *schedule_object*	Sets the schedule. The no command removes the schedule setting to the default (none). none means any time.
[no] service {*service_name*|any}	Sets the IP protocol. The no command resets service settings to the default (any). any means all services.
[no] snat {outgoing-interface|pool {*address_object*}}	Sets the source IP address of the matched packets that use SNAT. The no command removes source NAT settings from the rule.
[no] source {*address_object*|any}	Sets the source IP address that the matched packets must have. The no command resets the source IP address to the default (any). any means all IP addresses.
[no] trigger <1..8> incoming *service_name* trigger *service_name*	Sets a port triggering rule. The no command removes port trigger settings from the rule.
trigger append incoming *service_name* trigger *service_name*	Adds a new port triggering rule to the end of the list.
trigger delete <1..8>	Removes a port triggering rule.
trigger insert <1..8> incoming *service_name* trigger *service_name*	Adds a new port triggering rule before the specified number.
trigger move <1..8> to <1..8>	Moves a port triggering rule to the number that you specified.

Table 37 Command Summary: Policy Route (continued)

COMMAND	DESCRIPTION
[no] tunnel *tunnel_name*	Sets the incoming interface to an IPSec VPN tunnel. The no command removes the IPSec VPN tunnel through which the incoming packets are received.
[no] user *user_name*	Sets the user name. The no command resets the user name to the default (any). any means all users.
[no] policy controll-ipsec-dynamic-rules activate	Enables the ISG50 to use policy routes to manually specify the destination addresses of dynamic IPSec rules. You must manually create these policy routes. The ISG50 automatically obtains source and destination addresses for dynamic IPSec rules that do not match any of the policy routes. The no command has the ISG50 automatically obtain source and destination addresses for all dynamic IPSec rules.
policy default-route	Enters the policy-route sub-command mode to set a route with the name “default-route”.
policy delete *policy_number*	Removes a routing policy.
policy flush	Clears the policy routing table.
policy list table	Displays all policy route settings.
policy move *policy_number* to *policy_number*	Moves a routing policy to the number that you specified.
[no] policy override-direct-route activate	Use this command to have the ISG50 forward packets that match a policy route according to the policy route instead of sending the packets to a directly connected network. Use the no command to disable it.
show bwm activation	Displays whether or not the global setting for bandwidth management on the ISG50 is enabled.
show bwm-usage < [policy-route *policy_number*] | [interface *interface_name*]	Displays the specified policy route or interface’s bandwidth allotment, current bandwidth usage, and bandwidth usage statistics.
show policy-route [*policy_number*]	Displays all or specified policy route settings.
show policy-route begin <1..200> end <1..200>	Displays the specified range of policy route settings.
show policy-route controll-ipsec-dynamic-rules	Displays whether the ISG50 checks policy routes first before IPSec dynamic rules.
show policy-route override-direct-route	Displays whether or not the ISG50 forwards packets that match a policy route according to the policy route instead of sending the packets to a directly connected network.
show policy-route rule_count	Displays the number of policy routes that have been configured on the ISG50.
show policy-route underlayer-rules	Displays all policy route rule details for advanced debugging.

8.2.1 Assured Forwarding (AF) PHB for DiffServ

Assured Forwarding (AF) behavior is defined in RFC 2597. The AF behavior group defines four AF classes. Inside each class, packets are given a high, medium or low drop precedence. The drop precedence determines the probability that routers in the network will drop packets when congestion occurs. If congestion occurs between classes, the traffic in the higher class (smaller numbered class) is generally given priority. Combining the classes and drop precedence produces

the following twelve DSCP encodings from AF11 through AF43. The decimal equivalent is listed in brackets.

Table 38 Assured Forwarding (AF) Behavior Group

	CLASS 1	CLASS 2	CLASS 3	CLASS 4
Low Drop Precedence	AF11 (10)	AF21 (18)	AF31 (26)	AF41 (34)
Medium Drop Precedence	AF12 (12)	AF22 (20)	AF32 (28)	AF42 (36)
High Drop Precedence	AF13 (14)	AF23 (22)	AF33 (30)	AF43 (38)

8.2.2 Policy Route Command Example

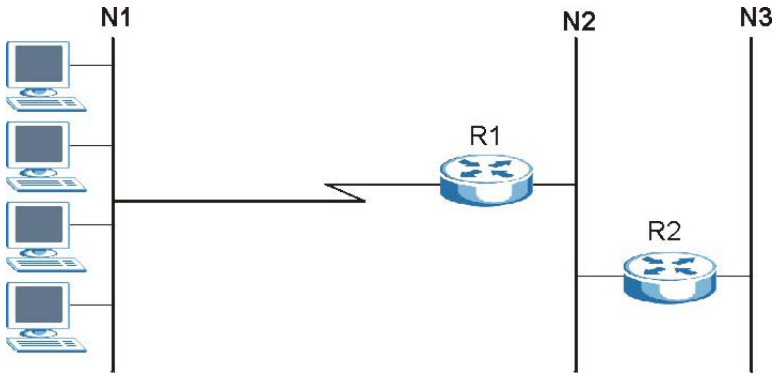
The following commands create two address objects (TW_SUBNET and GW_1) and insert a policy that routes the packets (with the source IP address TW_SUBNET and any destination IP address) through the interface ge1 to the next-hop router GW_1. This route uses the IP address of the outgoing interface as the matched packets' source IP address.

```
Router(config)# address-object TW_SUBNET 192.168.2.0 255.255.255.0
Router(config)# address-object GW_1 192.168.2.250
Router(config)# policy insert 1
Router(policy-route)# description example
Router(policy-route)# destination any
Router(policy-route)# interface ge1
Router(policy-route)# next-hop gateway GW_1
Router(policy-route)# snat outgoing-interface
Router(policy-route)# source TW_SUBNET
Router(policy-route)# exit
Router(config)# show policy-route 1
index: 1
  active: yes
  description: example
  user: any
  schedule: none
  interface: ge1
  tunnel: none
  sslvpn: none
  source: TW_SUBNET
  destination: any
  DSCP code: any
  service: any
  nexthop type: Gateway
  nexthop: GW_1
  nexthop state: Not support
  auto destination: no
  bandwidth: 0
  bandwidth priority: 0
  maximize bandwidth usage: no
  SNAT: outgoing-interface
  DSCP marking: preserve
  amount of port trigger: 0
Router(config)#
```

8.3 IP Static Route

The ISG50 has no knowledge of the networks beyond the network that is directly connected to the ISG50. For instance, the ISG50 knows about network **N2** in the following figure through gateway **R1**. However, the ISG50 is unable to route a packet to network **N3** because it doesn't know that there is a route through the same gateway **R1** (via gateway **R2**). The static routes are for you to tell the ISG50 about the networks beyond the network connected to the ISG50 directly.

Figure 15 Example of Static Routing Topology



8.4 Static Route Commands

The following table describes the commands available for static route. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 39 Command Summary: Static Route

COMMAND	DESCRIPTION
`[no] ip route {w.x.y.z} {w.x.y.z} {interface|w.x.y.z} <0..127>`	Sets a static route. The `no` command disables a static route.
`ip route replace {w.x.y.z} {w.x.y.z} {interface|w.x.y.z} <0..127> with {w.x.y.z} {w.x.y.z} {interface|w.x.y.z} <0..127>`	Changes an existing route's settings.
`show ip route-settings`	Displays static route information. Use `show ip route` to see learned route information. See Section 9.2.5 on page 96.

8.4.1 Static Route Commands Example

The following command sets a static route with IP address 10.10.10.0 and subnet mask 255.255.255.0 and with the next-hop interface ge1. Then use the show command to display the setting.

```
Router(config)# ip route 10.10.10.0 255.255.255.0 ge1
Router(config)#
Router(config)# show ip route-settings
Route           Netmask         Nexthop         Metric
================================================================================
10.10.10.0      255.255.255.0   ge1             0
```

9

Routing Protocol

This chapter describes how to set up RIP and OSPF routing protocols for the ISG50.

9.1 Routing Protocol Overview

Routing protocols give the ISG50 routing information about the network from other routers. The ISG50 then stores this routing information in the routing table, which it uses when it makes routing decisions. In turn, the ISG50 can also provide routing information via routing protocols to other routers.

The ISG50 supports two standards, RIP and OSPF, for routing protocols. RIP and OSPF are compared in Table 40 on page 93, and they are discussed further in the next two sections.

Table 40 OSPF vs. RIP

	OSPF	RIP
Network Size	Large	Small (with up to 15 routers)
Metric	Bandwidth, hop count, throughput, round trip time and reliability.	Hop count
Convergence	Fast	Slow

9.2 Routing Protocol Commands Summary

The following table describes the values required for many routing protocol commands. Other values are discussed with the corresponding commands.

Table 41 Input Values for Routing Protocol Commands

LABEL	DESCRIPTION
ip	The 32-bit name of the area or virtual link in IP address format.
authkey	The password for text or MD5 authentication. You may use alphanumeric characters or underscores(_). text password: 1-8 characters long MD5 password: 1-16 characters long

The following sections list the routing protocol commands.

9.2.1 RIP Commands

This table lists the commands for RIP.

Table 42 router Commands: RIP

COMMAND	DESCRIPTION
`router rip`	Enters sub-command mode.
`[no] network` *interface_name*	Enables RIP on the specified Ethernet interface. The no command disables RIP on the specified interface.
`[no] redistribute {static | ospf}`	Enables redistribution of routing information learned from the specified source. The no command disables redistribution from the specified source.
`redistribute {static | ospf} metric <0..16>`	Sets the metric when redistributing routing information learned from the specified source.
`[no] version <1..2>`	Sets the default RIP version for all interfaces with RIP enabled. If the interface RIP version is blank, the interface uses the default version. This is not available in the GUI. The no command sets the default RIP version to 2.
`[no] passive-interface` *interface_name*	Sets the direction to “In-Only” for the specified interface. The no command sets the direction to bi-directional.
`[no] authentication mode {md5 | text}`	Sets the authentication mode for RIP. The no command sets the authentication mode to “none”.
`[no] authentication string` *authkey*	Sets the password for text authentication. The no command clears the password.
`authentication key <1..255> key-string` *authkey*	Sets the MD5 ID and password for MD5 authentication.
`no authentication key`	Clears the MD5 ID and password.
`[no] outonly-interface` *interface_name*	Sets the direction to “Out-Only” for the specified interface. The no command sets the direction to “BiDir”.

9.2.2 General OSPF Commands

This table lists the commands for general OSPF configuration.

Table 43 router Commands: General OSPF Configuration

COMMAND	DESCRIPTION
`router ospf`	Enters sub-command mode.
`[no] redistribute {static | rip}`	Enables redistribution of routing information learned from the specified non-OSPF source. The no command disables redistribution from the specified non-OSPF source.
`[no] redistribute {static | rip} metric-type <1..2> metric <0..16777214>`	Sets the metric for routing information learned from the specified non-OSPF source. The no command clears the metric.

Table 43 router Commands: General OSPF Configuration (continued)

COMMAND	DESCRIPTION
[no] passive-interface *interface_name*	Sets the direction to “In-Only” for the specified interface. The no command sets the direction to “BiDir”.
[no] router-id IP	Sets the 32-bit ID (in IP address format) of the ISG50. The no command resets it to “default”, or the highest available IP address.

9.2.3 OSPF Area Commands

This table lists the commands for OSPF areas.

Table 44 router Commands: OSPF Areas

COMMAND	DESCRIPTION
router ospf	Enters sub-command mode.
[no] network *interface* area IP	Adds the specified interface to the specified area. The no command removes the specified interface from the specified area.
[no] area IP [{stub | nssa}]	Creates the specified area and sets it to the indicated type. The no command removes the area.
[no] area IP authentication	Enables text authentication in the specified area. The no command disables authentication in the specified area.
[no] area IP authentication message-digest	Enables MD5 authentication in the specified area. The no command disables authentication in the specified area.
[no] area IP authentication authentication-key *authkey*	Sets the password for text authentication in the specified area. The no command clears the password.
[no] area IP authentication message-digest-key <1..255> md5 *authkey*	Sets the MD5 ID and password for MD5 authentication in the specified area. The no command clears the MD5 ID and password.

9.2.4 Virtual Link Commands

This table lists the commands for virtual links in OSPF areas.

Table 45 router Commands: Virtual Links in OSPF Areas

COMMAND	DESCRIPTION
show ospf area IP virtual-link	Displays information about virtual links for the specified area.
router ospf	
[no] area IP virtual-link IP	Creates the specified virtual link in the specified area. The no command removes the specified virtual link.
[no] area IP virtual-link IP authentication	Enables text authentication in the specified virtual link. The no command disables authentication in the specified virtual link.

Table 45 router Commands: Virtual Links in OSPF Areas (continued)

COMMAND	DESCRIPTION
[no] area IP virtual-link IP authentication message-digest	Enables MD5 authentication in the specified virtual link. The no command disables authentication in the specified virtual link.
[no] area IP virtual-link IP authentication authentication-key *authkey*	Sets the password for text authentication in the specified virtual link. The no command clears the password in the specified virtual link.
[no] area IP virtual-link IP authentication message-digest-key <1..255> md5 *authkey*	Sets the MD5 ID and password for MD5 authentication in the specified virtual link. The no command clears the MD5 ID and password in the specified virtual link.
[no] area IP virtual-link IP authentication same-as-area	Sets the virtual link's authentication method to the area's default authentication.
[no] area IP virtual-link IP authentication-key *authkey*	Sets the password for text authentication in the specified virtual link. The no command clears the password.
area IP virtual-link IP message-digest-key <1..255> md5 *authkey*	Sets the MD5 ID and password for MD5 authentication in the specified virtual link.
no area IP virtual-link IP message-digest-key <1..255>	Clears the MD5 ID in the specified virtual link.

9.2.5 Learned Routing Information Commands

This table lists the commands to look at learned routing information.

Table 46 ip route Commands: Learned Routing Information

COMMAND	DESCRIPTION
show ip route [kernel | connected | static | ospf | rip | bgp]	Displays learned routing and other routing information.

9.2.6 show ip route Command Example

The following example shows learned routing information on the ISG50.

```
Router> show ip route
Flags: A - Activated route, S - Static route, C - directly Connected
       O - OSPF derived, R - RIP derived, G - selected Gateway
       ! - reject, B - Black hole, L - Loop

IP Address/Netmask    Gateway          IFace           Metric    Flags    Persist
================================================================================
0.0.0.0/0             172.23.26.254    wan1            0         ASG      -
127.0.0.0/8           0.0.0.0          lo              0         ACG      -
172.23.26.0/24        0.0.0.0          wan1            0         ACG      -
192.168.1.0/24        0.0.0.0          lan1            0         ACG      -
192.168.2.0/24        0.0.0.0          lan2            0         ACG      -
192.168.3.0/24        0.0.0.0          dmz             0         ACG      -
```

10

Zones

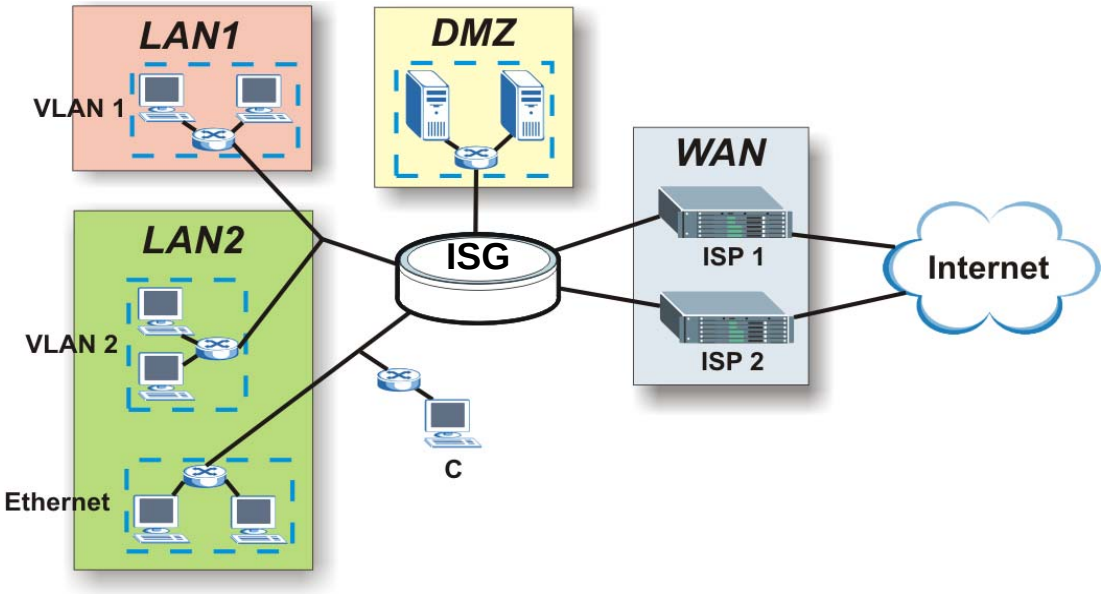
Set up zones to configure network security and network policies in the ISG50.

10.1 Zones Overview

A zone is a group of interfaces and VPN tunnels. The ISG50 uses zones, not interfaces, in many security and policy settings, such as firewall rules and remote management.

Zones cannot overlap. Each Ethernet interface, VLAN interface, bridge interface, PPPoE/PPTP interface, and VPN tunnel can be assigned to at most one zone. Virtual interfaces are automatically assigned to the same zone as the interface on which they run.

Figure 16 Example: Zones



10.2 Zone Commands Summary

The following table describes the values required for many zone commands. Other values are discussed with the corresponding commands.s

Table 47 Input Values for Zone Commands

LABEL	DESCRIPTION
profile_name	The name of a zone, or the name of a VPN tunnel. Use up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive.

This table lists the zone commands.

Table 48 zone Commands

COMMAND	DESCRIPTION
show zone [*profile_name*]	Displays information about the specified zone or about all zones.
show zone binding-iface	Displays each interface and zone mappings.
show zone default-binding	Displays the pre-configured interface and zone mappings that come with the ISG50.
show zone none-binding	Displays the interfaces and tunnels that are not associated with a zone yet.
show zone system-default	Displays the pre-configured default zones that you cannot delete from the ISG50.
show zone user-define	Displays all customized zones.
[no] zone *profile_name*	Creates the zone if necessary and enters sub-command mode. The no command deletes the zone.
zone *profile_name*	Enter the sub-command mode.
[no] block	Blocks intra-zone traffic. The no command allows intra-zone traffic.
[no] interface *interface_name*	Adds the specified interface to the specified zone. The no command removes the specified interface from the specified zone. See Section 6.2 on page 54 for information about interface names.
[no] crypto *profile_name*	Adds the specified IPSec VPN tunnel to the specified zone. The no command removes the specified IPSec VPN tunnel from the specified zone.

10.2.1 Zone Command Examples

The following commands add Ethernet interfaces ge1 and ge2 to zone A and block intra-zone traffic.

```
Router# configure terminal
Router(config)# zone A
Router(zone)# interface ge1
Router(zone)# interface ge2
Router(zone)# block
Router(zone)# exit
Router(config)# show zone
No. Name                            Block  Member
=============================================================================
1   A                                 yes    ge1,ge2
Router(config)# show zone A
blocking intra-zone traffic: yes
No. Type                            Member
=============================================================================
1   interface                       ge1
2   interface                       ge2
```

11

DDNS

This chapter describes how to configure dynamic DNS (DDNS) services for the ISG50.

11.1 DDNS Overview

DNS maps a domain name to a corresponding IP address and vice versa. Similarly, dynamic DNS maps a domain name to a dynamic IP address. As a result, anyone can use the domain name to contact you (in NetMeeting, CU-SeeMe, etc.) or to access your FTP server or Web site, regardless of the current IP address.

Note: You must have a public WAN IP address to use Dynamic DNS.

Set up a dynamic DNS account with a supported DNS service provider to be able to use Dynamic DNS services with the ISG50. When registration is complete, the DNS service provider gives you a password or key. At the time of writing, the ISG50 supports the following DNS service providers. See the listed websites for details about the DNS services offered by each.

Table 49 Network > DDNS

DDNS SERVICE PROVIDER	SERVICE TYPES SUPPORTED	WEBSITE	NOTES
DynDNS	Dynamic DNS, Static DNS, and Custom DNS	www.dyndns.com)	
Dynu	Basic, Premium	www.dynu.com	
No-IP	No-IP	www.no-ip.com	
Peanut Hull	Peanut Hull	www.oray.cn	Chinese website

Note: Record your DDNS account's user name, password, and domain name to use to configure the ISG50.

After, you configure the ISG50, it automatically sends updated IP addresses to the DDNS service provider, which helps redirect traffic accordingly.

11.2 DDNS Commands Summary

The following table describes the values required for many DDNS commands. Other values are discussed with the corresponding commands.

Table 50 Input Values for DDNS Commands

LABEL	DESCRIPTION
profile_name	The name of the DDNS profile. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

The following table lists the DDNS commands.

Table 51 ip ddns Commands

COMMAND	DESCRIPTION
`show ddns [`*profile_name*`]`	Displays information about the specified DDNS profile or about all DDNS profiles.
`[no] ip ddns profile` *profile_name*	Creates the specified DDNS profile if necessary and enters sub-command mode. The no command deletes it.
`[no] service-type {dyndns | dyndns_static | dyndns_custom | dynu-basic | dynu-premium | no-ip | peanut-hull | 3322-dyn | 3322-static}`	Sets the service type in the specified DDNS profile. The no command clears it.
`[no] username` *username* `password` *password*	Sets the username and password in the specified DDNS profile. The no command clears these fields. *username*: You can use up to 31 alphanumeric characters and the underscore (_). *password*: You can use up to 64 alphanumeric characters and the underscore (_).
`[no] host` *hostname*	Sets the domain name in the specified DDNS profile. The no command clears the domain name. *hostname*: You may up to 254 alphanumeric characters, dashes (-), or periods (.), but the first character must be alphanumeric.
`[no] ip-select {iface | auto | custom}`	Sets the IP address update policy in the specified DDNS profile. The no command clears the policy.
`[no] ip-select-backup {iface | auto | custom}`	Sets the alternate IP address update policy in the specified DDNS profile. The no command clears the policy.
`[no] custom` *ip*	Sets the static IP address in the specified DDNS profile. The no command clears it.
`[no] backup-custom` *ip*	Sets the static IP address for the backup interface in the specified DDNS profile. The no command clears it.

Table 51 ip ddns Commands (continued)

COMMAND	DESCRIPTION
[no] mx {*ip* | *domain_name*}	Enables the mail exchanger and sets the fully-qualified domain name of the mail server to which mail from this domain name is forwarded. The no command disables the mail exchanger. *domain_name*: You may up to 254 alphanumeric characters, dashes (-), or periods (.), but the first character must be alphanumeric.
[no] wan-iface *interface_name*	Sets the WAN interface in the specified DDNS profile. The no command clears it.
[no] backup-iface *interface_name*	Sets the backup WAN interface in the specified DDNS profile. The no command clears it.
[no] ha-iface *interface_name*	Sets the HA interface in the specified DDNS profile. The no command clears it.
[no] backmx	Enables the backup mail exchanger. The no command disables it.
[no] wildcard	Enables the wildcard feature. The no command disables it.

12

Virtual Servers

This chapter describes how to set up, manage, and remove virtual servers. Virtual server commands configure NAT.

12.1 Virtual Server Overview

Virtual server is also known as port forwarding or port translation.

Virtual servers are computers on a private network behind the ISG50 that you want to make available outside the private network. If the ISG50 has only one public IP address, you can make the computers in the private network available by using ports to forward packets to the appropriate private IP address.

12.1.1 1:1 NAT and Many 1:1 NAT

1:1 NAT - If the private network server will initiate sessions to the outside clients, use 1:1 NAT to have the ISG50 translate the source IP address of the server's outgoing traffic to the same public IP address that the outside clients use to access the server.

Many 1:1 NAT - If you have a range of private network servers that will initiate sessions to the outside clients and a range of public IP addresses, use many 1:1 NAT to have the ISG50 translate the source IP address of each server's outgoing traffic to the same one of the public IP addresses that the outside clients use to access the server. The private and public ranges must have the same number of IP addresses.

One many 1:1 NAT rule works like multiple 1:1 NAT rules, but it eases the configuration effort since you only create one rule.

12.2 Virtual Server Commands Summary

The following table describes the values required for many virtual server commands. Other values are discussed with the corresponding commands.

Table 52 Input Values for Virtual Server Commands

LABEL	DESCRIPTION
service_object	The name of a service. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
profile_name	The name of the virtual server. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

The following table lists the virtual server commands.

Table 53 ip virtual-server Commands

COMMAND	DESCRIPTION
`show ip virtual-server [profile_name]`	Displays information about the specified virtual server or about all the virtual servers.
`no ip virtual-server profile_name`	Deletes the specified virtual server.
`ip virtual-server profile_name interface interface_name original-ip {any | ip | address_object} map-to {address_object | ip} map-type any [nat-loopback [nat-1-1-map] [deactivate] | nat-1-1-map [deactivate] | deactivate]`	Creates or modifies the specified virtual server and maps the specified destination IP address (for all destination ports) to the specified destination address object or IP address. The original destination IP is defined by the specified interface (any), the specified IP address (IP), or the specified address object (*address-object*). NAT loopback allows local users to use a domain name to access this virtual server. Select what kind of NAT this rule is to perform. `nat-1-1-map`: means the NAT type is either 1:1 NAT or many 1:1 NAT. See Section 12.1.1 on page 105 for more information. Using this command without `nat-1-1-map` means the NAT type is Virtual Server. This makes computers on a private network behind the ISG50 available to a public network outside the ISG50 (like the Internet). The `deactivate` command disables the virtual server rule.
`ip virtual-server profile_name interface interface_name original-ip {any | IP | address_object} map-to {address_object | ip} map-type port protocol {any | tcp | udp} original-port <1..65535> mapped-port <1..65535> [nat-loopback [nat-1-1-map] [deactivate] | nat-1-1-map [deactivate] | deactivate]`	Creates or modifies the specified virtual server and maps the specified (destination IP address, protocol, and destination port) to the specified (destination IP address and destination port). The original destination IP is defined by the specified interface (any), the specified IP address (IP), or the specified address object (*address-object*). NAT loopback allows local users to use a domain name to access this virtual server. `nat-1-1-map`: means the NAT type is either 1:1 NAT or many 1:1 NAT. See Section 12.1.1 on page 105 for more information. Using this command without `nat-1-1-map` means the NAT type is Virtual Server. This makes computers on a private network behind the ISG50 available to a public network outside the ISG50 (like the Internet). The `deactivate` command disables the virtual server rule.

Table 53 ip virtual-server Commands (continued)

COMMAND	DESCRIPTION
ip virtual-server *profile_name* interface *interface_name* original-ip {any | IP | *address_object*} map-to {*address_object* | *ip*} map-type ports protocol {any | tcp | udp} original-port-begin <1..65535> original-port-end <1..65535> mapped-port-begin <1..65535> [nat-loopback [nat-1-1-map] [deactivate] | nat-1-1-map [deactivate] | deactivate]	Creates or modifies the specified virtual server and maps the specified (destination IP address, protocol, and range of destination ports) to the specified (destination IP address and range of destination ports). The original destination IP is defined by the specified interface (any), the specified IP address (IP), or the specified address object (*address-object*). NAT loopback allows local users to use a domain name to access this virtual server. nat-1-1-map: means the NAT type is either 1:1 NAT or many 1:1 NAT. See Section 12.1.1 on page 105 for more information. Using this command without nat-1-1-map means the NAT type is Virtual Server. This makes computers on a private network behind the ISG50 available to a public network outside the ISG50 (like the Internet). The deactivate command disables the virtual server rule.
ip virtual-server *profile_name* interface *interface_name* original-ip {any | IP | *address_object*} map-to {*address_object* | *ip*} map-type original-service *service_object* mapped-service *service_object* [nat-loopback [nat-1-1-map] [deactivate] | nat-1-1-map [deactivate] | deactivate]	Creates or modifies the specified virtual server and maps the specified (destination IP address, protocol, and service object) to the specified (destination IP address and service object). The original destination IP is defined by the specified interface (any), the specified IP address (IP), or the specified address object (*address-object*). NAT loopback allows local users to use a domain name to access this virtual server. nat-1-1-map: means the NAT type is either 1:1 NAT or many 1:1 NAT. See Section 12.1.1 on page 105 for more information. Using this command without nat-1-1-map means the NAT type is Virtual Server. This makes computers on a private network behind the ISG50 available to a public network outside the ISG50 (like the Internet). The deactivate command disables the virtual server rule.
ip virtual-server {activate | deactivate} *profile_name*	Activates or deactivates the specified virtual server.
ip virtual-server delete *profile_name*	Deletes the specified virtual server.
ip virtual-server flush	Deletes all virtual servers.
ip virtual-server rename *profile_name* *profile_name*	Renames the specified virtual server from the first *profile_name* to the second *profile_name*.

12.2.1 Virtual Server Command Examples

The following command creates virtual server WAN-LAN_H323 on the wan1 interface that maps IP addresses 10.0.0.8 to 192.168.1.56. for TCP protocol traffic on port 1720. It also adds a NAT loopback entry.

```
Router# configure terminal
Router(config)# ip virtual-server WAN-LAN_H323 interface wan1 original-ip
10.0.0.8 map-to 192.168.1.56 map-type port protocol tcp original-port 1720
mapped-port 1720 nat-loopback
Router(config)#
```

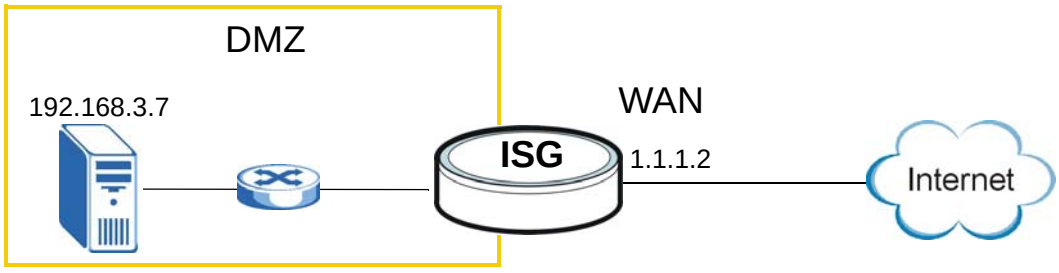
The following command shows information about all the virtual servers in the ISG50.

```
Router(config)# show ip virtual-server
virtual server: WAN-LAN_H323
  active: yes
  interface: wan1
  NAT-loopback active: yes
  NAT 1-1: no
  original IP: 10.0.0.8
  mapped IP: 192.168.1.56
  mapping type: port
  protocol type: tcp
  original service:
  mapped service:
  original start port: 1720
  original end port:
  mapped start port: 1720
  mapped end port:
Router(config)#
```

12.2.2 Tutorial - How to Allow Public Access to a Server

This is an example of making an HTTP (web) server in the DMZ zone accessible from the Internet (the WAN zone). You will use a public IP address of 1.1.1.2 on the ge2 interface and map it to the HTTP server's private IP address of 192.168.3.7.

Figure 17 Public Server Example Network Topology



Follow the following steps for the setting.

1 Configure Address object

Create two address objects. One is named DMZ_HTTP for the HTTP server's private IP address of 192.168.3.7. The other one is named ge2_HTTP for the ge2 (wan1) public IP address of 1.1.1.2.

```
Router# configure terminal
Router(config)# address-object DMZ_HTTP 192.168.3.7
Router(config)# address-object ge2_HTTP 1.1.1.2
Router(config)#
```

2 Configure NAT

You need a NAT rule to send HTTP traffic coming to IP address 1.1.1.2 on ge2 (wan1) to the HTTP server's private IP address of 192.168.3.7. Use the following settings:

- This NAT rule is for any HTTP traffic coming in on ge2 (wan1) to IP address 1.1.1.2.
- The NAT rule sends this traffic to the HTTP server's private IP address of 192.168.3.7 (defined in the DMZ_HTTP object).
- HTTP traffic and the HTTP server in this example both use TCP port 80. So you set the port mapping type to "port", the protocol type to "TCP", and the original and mapped ports to "80".

```
Router(config)# ip virtual-server To-VirtualServer-WWW interface ge2
original-ip ge2_HTTP map-to DMZ_HTTP map-type port protocol tcp original-
port 80 mapped-port 80
Router(config)#
```

3 Configure firewall

Create a firewall rule to allow HTTP traffic from the WAN zone to the DMZ web server.

```
Router(config)# firewall insert 1
Router(firewall)# description To-VirtualServer-WWW
Router(firewall)# from WAN
Router(firewall)# to DMZ
Router(firewall)# destinationip DMZ_HTTP
Router(firewall)# service HTTP
Router(firewall)# exit
Router(config)# write
Router(config)#
```

Now the public can go to IP address 1.1.1.2 to access the HTTP server.

13

HTTP Redirect

This chapter shows you how to configure HTTP redirection on your ISG50.

13.1 HTTP Redirect Overview

HTTP redirect forwards the client's HTTP request (except HTTP traffic destined for the ISG50) to a web proxy server.

13.1.1 Web Proxy Server

A proxy server helps client devices make indirect requests to access the Internet or outside network resources/services. A proxy server can act as a firewall or an ALG (application layer gateway) between the private network and the Internet or other networks. It also keeps hackers from knowing internal IP addresses.

13.2 HTTP Redirect Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 54 Input Values for HTTP Redirect Commands

LABEL	DESCRIPTION
description	The name to identify the rule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
interface_name	The name of the interface. Ethernet interface: Use ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your ISG50 model. virtual interface on top of Ethernet interface: add a colon (:) and the number of the virtual interface. For example: ge*x*:*y*, *x* = 1 - N, *y* = 1 - 4 VLAN interface: vlan*x*, *x* = 0 - 4094 virtual interface on top of VLAN interface: vlan*x*:*y*, *x* = 0 - 4094, *y* = 1 - 4 bridge interface: br*x*, *x* = 0 - N, where N depends on the number of bridge interfaces your ISG50 model supports. virtual interface on top of bridge interface: br*x*:*y*, *x* = the number of the bridge interface, *y* = 1 - 4 PPPoE/PPTP interface: ppp*x*, *x* = 0 - N, where N depends on the number of PPPoE/PPTP interfaces your ISG50 model supports.

The following table describes the commands available for HTTP redirection. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 55 Command Summary: HTTP Redirect

COMMAND	DESCRIPTION
`ip http-redirect` *`description`* `interface` *`interface_name`* `redirect-to` *`w.x.y.z`* `<1..65535>`	Sets a HTTP redirect rule.
`ip http-redirect` *`description`* `interface` *`interface_name`* `redirect-to` *`w.x.y.z`* `<1..65535> deactivate`	Disables a HTTP redirect rule.
`ip http-redirect activate` *`description`*	Enables a rule with the specified rule name.
`ip http-redirect deactivate` *`description`*	Disables a rule with the specified rule name.
`no ip http-redirect` *`description`*	Removes a rule with the specified rule name.
`ip http-redirect flush`	Clears all HTTP redirect rules.
`show ip http-redirect [`*`description`*`]`	Displays HTTP redirect settings.

13.2.1 HTTP Redirect Command Examples

The following commands create a HTTP redirect rule, disable it and display the settings.

```
Router# configure terminal
Router(config)# ip http-redirect example1 interface ge1 redirect-to
10.10.2.3 80
Router(config)# ip http-redirect example1 interface ge1 redirect-to
10.10.2.3 80 deactivate
Router(config)# show ip http-redirect
Name                            Interface    Proxy Server    Port    Active
================================================================================
example1                         ge1          10.10.2.3       80      no
```

14

ALG

This chapter covers how to use the ISG50's ALG feature to allow certain applications to pass through the ISG50.

14.1 ALG Introduction

The ISG50 can function as an Application Layer Gateway (ALG) to allow certain NAT un-friendly applications (such as SIP) to operate properly through the ISG50's NAT.

Some applications cannot operate through NAT (are NAT un-friendly) because they embed IP addresses and port numbers in their packets' data payload. The ISG50 examines and uses IP address and port number information embedded in the VoIP traffic's data stream. When a device behind the ISG50 uses an application for which the ISG50 has VoIP pass through enabled, the ISG50 translates the device's private IP address inside the data stream to a public IP address. It also records session port numbers and allows the related sessions to go through the firewall so the application's traffic can come in from the WAN to the LAN.

The ISG50 only needs to use the ALG feature for traffic that goes through the ISG50's NAT. The firewall allows related sessions for VoIP applications that register with a server. The firewall allows or blocks peer to peer VoIP traffic based on the firewall rules.

You do not need to use a TURN (Traversal Using Relay NAT) server for VoIP devices behind the ISG50 when you enable the SIP ALG.

14.2 ALG Commands

The following table lists the `alg` commands. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 56 alg Commands

COMMAND	DESCRIPTION
`[no] alg <h323 | ftp> [signal-port <1025..65535> | signal-extra-port <1025..65535> | transformation]`	Turns on or configures the H.323 or FTP ALG. Use `signal-port` with a listening port number (1025 to 65535) if you are using H.323 on a TCP port other than 1720 or FTP on a TCP port other than 21. Use `signal-extra-port` with a listening port number (1025 to 65535) if you are also using H.323 or FTP on an additional TCP port number, enter it here. Use `transformation` to have the ISG50 modify IP addresses and port numbers embedded in the H.323 or FTP data payload. You do not need to use this if you have an H.323 or FTP device or server that will modify IP addresses and port numbers embedded in the H.323 or FTP data payload. The `no` command turns off the H.323 or FTP ALG or removes the settings that you specify.
`show alg <h323 | ftp>`	Displays the specified ALG's configuration.

14.3 ALG Commands Example

The following example turns on pass through for FTP and turns it off for H.323.

```
Router# configure terminal
Router(config)# alg ftp
Router(config)# no alg h323
```

15

IP/MAC Binding

15.1 IP/MAC Binding Overview

IP address to MAC address binding helps ensure that only the intended devices get to use privileged IP addresses. The ISG50 uses DHCP to assign IP addresses and records to MAC address it assigned each IP address. The ISG50 then checks incoming connection attempts against this list. A user cannot manually assign another IP to his computer and use it to connect to the ISG50.

Suppose you configure access privileges for IP address 192.168.1.27 and use static DHCP to assign it to Tim's computer's MAC address of 12:34:56:78:90:AB. IP/MAC binding drops traffic from any computer with another MAC address that tries to use IP address 192.168.1.27.

15.2 IP/MAC Binding Commands

The following table lists the `ip-mac-binding` commands. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 57 ip-mac-binding Commands

COMMAND	DESCRIPTION
`[no] ip ip-mac-binding` *interface_name* `activate`	Turns on IP/MAC binding for the specified interface. The `no` command turns IP/MAC binding off for the specified interface.
`[no] ip ip-mac-binding` *interface_name* `log`	Turns on the IP/MAC binding logs for the specified interface. The `no` command turns IP/MAC binding logs off for the specified interface.
`ip ip-mac-binding exempt` *name start-ip end-ip*	Adds a named IP range as being exempt from IP/MAC binding.
`no ip ip-mac-binding exempt` *name*	Deletes the named IP range from the list of addresses that are exempt from IP/MAC binding.
`show ip ip-mac-binding` *interface_name*	Shows whether IP/MAC binding is enabled or disabled for the specified interface.
`show ip ip-mac-binding all`	Shows whether IP/MAC binding is enabled or disabled for all interfaces.
`show ip ip-mac-binding status` *interface_name*	Displays the current IP/MAC bindings for the specified interface.
`show ip ip-mac-binding status all`	Displays the current IP/MAC bindings for all interfaces.
`show ip ip-mac-binding exempt`	Shows the current IP/MAC binding exempt list.
`ip ip-mac-binding clear-drop-count` *interface_name*	Resets the packet drop counter for the specified interface.
`debug ip ip-mac-binding activate`	Turns on the IP/MAC binding debug logs.
`no debug ip ip-mac-binding activate`	Turns off the IP/MAC binding debug logs.

15.3 IP/MAC Binding Commands Example

The following example enables IP/MAC binding on the LAN1 interface and displays the interface's IP/MAC binding status..

```
Router# configure terminal
Router(config)# ip ip-mac-binding lan1 activate
Router(config)# show ip ip-mac-binding lan1
Name: lan1
Status: Enable
Log: No
Binding Count: 0
Drop Count: 0
Router(config)#
```

16

Firewall

This chapter introduces the ISG50's firewall and shows you how to configure your ISG50's firewall.

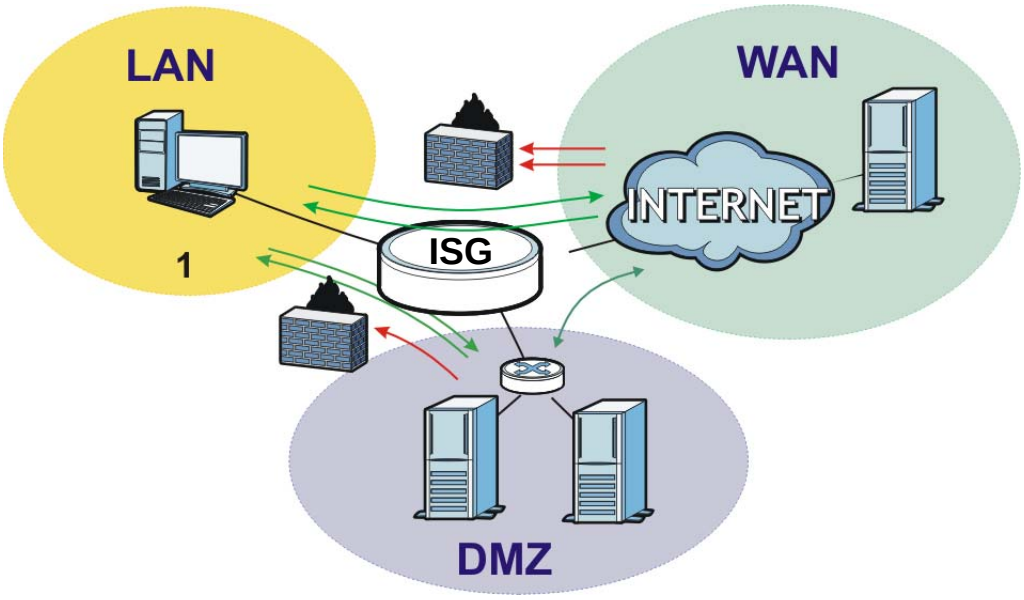
16.1 Firewall Overview

The ISG50's firewall is a stateful inspection firewall. The ISG50 restricts access by screening data packets against defined access rules. It can also inspect sessions. For example, traffic from one zone is not allowed unless it is initiated by a computer in another zone first.

A zone is a group of interfaces or VPN tunnels. Group the ISG50's interfaces into different zones based on your needs. You can configure firewall rules for data passing between zones or even between interfaces and/or VPN tunnels in a zone.

The following figure shows the ISG50's default firewall rules in action as well as demonstrates how stateful inspection works. User **1** can initiate a Telnet session from within the LAN zone and responses to this request are allowed. However, other Telnet traffic initiated from the WAN or DMZ zone and destined for the LAN zone is blocked. Communications between the WAN and the DMZ zones are allowed. The firewall allows VPN traffic between any of the networks.

Figure 18 Default Firewall Action



Your customized rules take precedence and override the ISG50's default settings. The ISG50 checks the schedule, user name (user's login name on the ISG50), source IP address, destination IP address and IP protocol type of network traffic against the firewall rules (in the order you list them). When the traffic matches a rule, the ISG50 takes the action specified in the rule.

For example, if you want to allow a specific user from any computer to access one zone by logging in to the ISG50, you can set up a rule based on the user name only. If you also apply a schedule to the firewall rule, the user can only access the network at the scheduled time. A user-aware firewall rule is activated whenever the user logs in to the ISG50 and will be disabled after the user logs out of the ISG50.

16.2 Firewall Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 58 Input Values for General Firewall Commands

LABEL	DESCRIPTION
address_object	The name of the IP address (group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
user_name	The name of a user (group). You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
zone_object	The name of the zone. Use up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive.
rule_number	The priority number of a firewall rule. 1 - *X* where *X* is the highest number of rules the ISG50 model supports. See the ISG50's datasheet for details.
schedule_object	The name of the schedule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
service_name	The name of the service (group). You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

The following table describes the commands available for the firewall. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 59 Command Summary: Firewall

COMMAND	DESCRIPTION
`[no] connlimit max-per-host <1..8192>`	Sets he highest number of sessions that the ISG50 will permit a host to have at one time. The `no` command removes the settings.
`firewall` *`rule_number`*	Enters the firewall sub-command mode to set a firewall rule. See Table 60 on page 120 for the sub-commands.
`firewall` *`zone_object`* `{`*`zone_object`*`|Device}` *`rule_number`*	Enters the firewall sub-command mode to set a direction specific through-Device rule or to-Device rule. See Table 60 on page 120 for the sub-commands.
`firewall` *`zone_object`* `{`*`zone_object`*`|Device} append`	Enters the firewDeviceall sub-command mode to add a direction specific through-Device rule or to-Device rule to the end of the global rule list. See Table 60 on page 120 for the sub-commands.

Table 59 Command Summary: Firewall (continued)

COMMAND	DESCRIPTION
`firewall *zone_object* {*zone_object*|Device} delete <1..5000>`	Removes a direction specific through-Device rule or to-Device rule. <1..5000>: the index number in a direction specific firewall rule list.
`firewall *zone_object* {*zone_object*|Device} flush`	Removes all direction specific through-Device rule or to-Device rules.
`firewall *zone_object* {*zone_object*|Device} insert *rule_number*`	Enters the firewall sub-command mode to add a direction specific through-Device rule or to-Device rule before the specified rule number. See Table 60 on page 120 for the sub-commands.
`firewall *zone_object* {*zone_object*|Device} move *rule_number* to *rule_number*`	Moves a direction specific through-Device rule or to-Device rule to the number that you specified.
`[no] firewall activate`	Enables the firewall on the ISG50. The no command disables the firewall.
`firewall append`	Enters the firewall sub-command mode to add a global firewall rule to the end of the global rule list. See Table 60 on page 120 for the sub-commands.
`firewall default-rule action {allow | deny | reject} { no log | log [alert] }`	Sets how the firewall handles packets that do not match any other firewall rule.
`firewall delete *rule_number*`	Removes a firewall rule.
`firewall flush`	Removes all firewall rules.
`firewall insert *rule_number*`	Enters the firewall sub-command mode to add a firewall rule before the specified rule number. See Table 60 on page 120 for the sub-commands.
`firewall move *rule_number* to *rule_number*`	Moves a firewall rule to the number that you specified.
`show connlimit max-per-host`	Displays the highest number of sessions that the ISG50 will permit a host to have at one time.
`show firewall`	Displays all firewall settings.
`show firewall *rule_number*`	Displays a firewall rule's settings.
`show firewall *zone_object* {*zone_object*|Device}`	Displays all firewall rules settings for the specified packet direction.
`show firewall *zone_object* {*zone_object*|Device} *rule_number*`	Displays a specified firewall rule's settings for the specified packet direction.
`show firewall status`	Displays whether the firewall is active or not.

16.2.1 Firewall Sub-Commands

The following table describes the sub-commands for several firewall commands.

Table 60 firewall Sub-commands

COMMAND	DESCRIPTION
`action {allow|deny|reject}`	Sets the action the ISG50 takes when packets match this rule.
`[no] activate`	Enables a firewall rule. The no command disables the firewall rule.
`[no] ctmatch {dnat | snat}`	Use dnat to block packets sent from a computer on the ISG50's WAN network from being forwarded to an internal network according to a virtual server rule. Use snat to block packets sent from a computer on the ISG50's internal network from being forwarded to the WAN network according to a 1:1 NAT or Many 1:1 NAT rule. The no command forwards the matched packets.
`[no] description` *description*	Sets a descriptive name (up to 60 printable ASCII characters) for a firewall rule. The no command removes the descriptive name from the rule.
`[no] destinationip` *address_object*	Sets the destination IP address. The no command resets the destination IP address(es) to the default (any). any means all IP addresses.
`[no] from` *zone_object*	Sets the zone on which the packets are received. The no command removes the zone on which the packets are received and resets it to the default (any). any means all interfaces or VPN tunnels.
`[no] log [alert]`	Sets the ISG50 to create a log (and optionally an alert) when packets match this rule. The no command sets the ISG50 not to create a log or alert when packets match this rule.
`[no] schedule` *schedule_object*	Sets the schedule that the rule uses. The no command removes the schedule settings from the rule.
`[no] service` *service_name*	Sets the service to which the rule applies. The no command resets the service settings to the default (any). any means all services.
`[no] sourceip` *address_object*	Sets the source IP address(es). The no command resets the source IP address(es) to the default (any). any means all IP addresses.
`[no] sourceport {tcp|udp} {eq <1..65535>|range <1..65535> <1..65535>}`	Sets the source port for a firewall rule. The no command removes the source port from the rule.
`[no] to {`*zone_object*`|Device}`	Sets the zone to which the packets are sent. The no command removes the zone to which the packets are sent and resets it to the default (any). any means all interfaces or VPN tunnels.
`[no] user` *user_name*	Sets a user-aware firewall rule. The rule is activated only when the specified user logs into the system. The no command resets the user name to the default (any). any means all users.

16.2.2 Firewall Command Examples

The following example shows you how to add a firewall rule to allow a MyService connection from the WAN zone to the IP addresses Dest_1 in the LAN zone.

- Enter configuration command mode.
- Create an IP address object.
- Create a service object.
- Enter the firewall sub-command mode to add a firewall rule.
- Set the direction of travel of packets to which the rule applies.
- Set the destination IP address(es).
- Set the service to which this rule applies.
- Set the action the ISG50 is to take on packets which match this rule.

```
Router# configure terminal
Router(config)# service-object MyService tcp eq 1234
Router(config)# address-object Dest_1 10.0.0.10-10.0.0.15
Router(config)# firewall insert 3
Router(firewall)# from WAN
Router(firewall)# to LAN
Router(firewall)# destinationip Dest_1
Router(firewall)# service MyService
Router(firewall)# action allow
```

The following command displays the firewall rule(s) (including the default firewall rule) that applies to the packet direction from WAN to LAN. The firewall rule numbers in the menu are the firewall rules' priority numbers in the global rule list.

```
Router# configure terminal
Router(config)# show firewall WAN LAN
firewall rule: 3
  description:
  user: any, schedule: none
  from: WAN, to: LAN
  source IP: any, source port: any
  destination IP: Dest_1, service: MyService
  log: no, action: allow, status: yes
firewall rule: 4
  description:
  user: any, schedule: none
  from: WAN, to: LAN
  source IP: any, source port: any
  destination IP: any, service: any
  log: log, action: deny, status: yes

Router(config)# show firewall WAN LAN 2
firewall rule: 4
  description:
  user: any, schedule: none
  from: WAN, to: LAN
  source IP: any, source port: any
  destination IP: any, service: any
  log: no, action: deny, status: yes
Router(config)#
```

16.3 Session Limit Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 61 Input Values for General Session Limit Commands

LABEL	DESCRIPTION
rule_number	The priority number of a session limit rule, 1 - 1000.
address_object	The name of the IP address (group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
user_name	The name of a user (group). You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

The following table describes the session-limit commands. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 62 Command Summary: Session Limit

COMMAND	DESCRIPTION
`[no] session-limit activate`	Turns the session-limit feature on or off.
`session-limit limit <0..8192>`	Sets the default number of concurrent NAT/ firewall sessions per host.
`session-limit` *`rule_number`*	Enters the session-limit sub-command mode to set a session-limit rule.
`[no] activate`	Enables the session-limit rule. The `no` command disables the session limit rule.
`[no] address` *`address_object`*	Sets the source IP address. The `no` command sets this to `any`, which means all IP addresses.
`[no] description` *`description`*	Sets a descriptive name (up to 64 printable ASCII characters) for a session-limit rule. The `no` command removes the descriptive name from the rule.
`exit`	Quits the firewall sub-command mode.
`[no] limit <0..8192>`	Sets the limit for the number of concurrent NAT/firewall sessions this rule's users or addresses can have. 0 means any.
`[no] user` *`user_name`*	Sets a session-limit rule for the specified user. The `no` command resets the user name to the default (`any`). `any` means all users.
`session-limit append`	Enters the session-limit sub-command mode to add a session-limit rule to the end of the session-limit rule list.
`session-limit delete` *`rule_number`*	Removes a session-limit rule.
`session-limit flush`	Removes all session-limit rules.
`session-limit insert` *`rule_number`*	Enters the session-limit sub-command mode to add a session-limit rule before the specified rule number.
`session-limit move` *`rule_number`* `to` *`rule_number`*	Moves a session-limit to the number that you specified.
`show session-limit`	Shows the session-limit configuration.
`show session-limit begin` *`rule_number`* `end` *`rule_number`*	Shows the settings for a range of session-limit rules.
`show session-limit` *`rule_number`*	Shows the session-limit rule's settings.
`show session-limit status`	Shows the general session-limit settings.

17

IPSec VPN

This chapter explains how to set up and maintain IPSec VPNs in the ISG50.

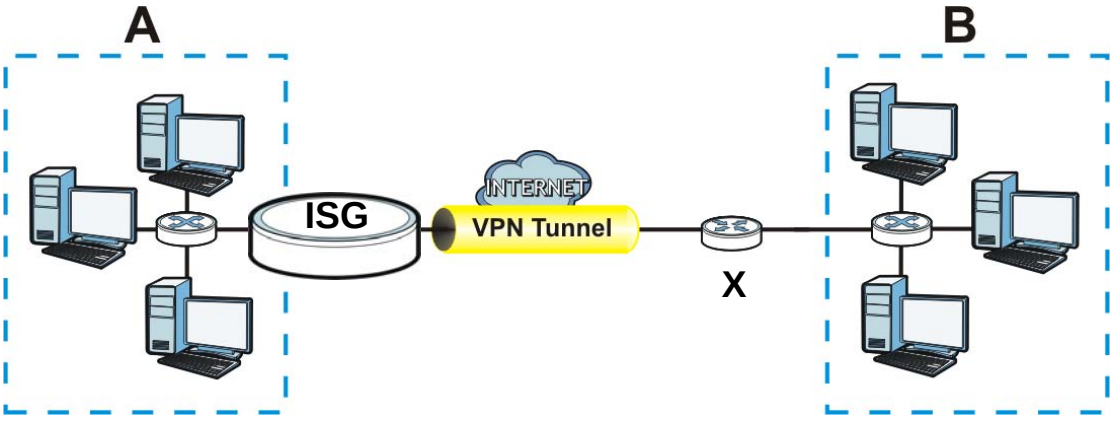
17.1 IPSec VPN Overview

A virtual private network (VPN) provides secure communications between sites without the expense of leased site-to-site lines. A secure VPN is a combination of tunneling, encryption, authentication, access control and auditing. It is used to transport traffic over the Internet or any insecure network that uses TCP/IP for communication.

Internet Protocol Security (IPSec) is a standards-based VPN that offers flexible solutions for secure data communications across a public network like the Internet. IPSec is built around a number of standardized cryptographic techniques to provide confidentiality, data integrity and authentication at the IP layer.

The following figure is one example of a VPN tunnel.

Figure 19 IPSec VPN Example

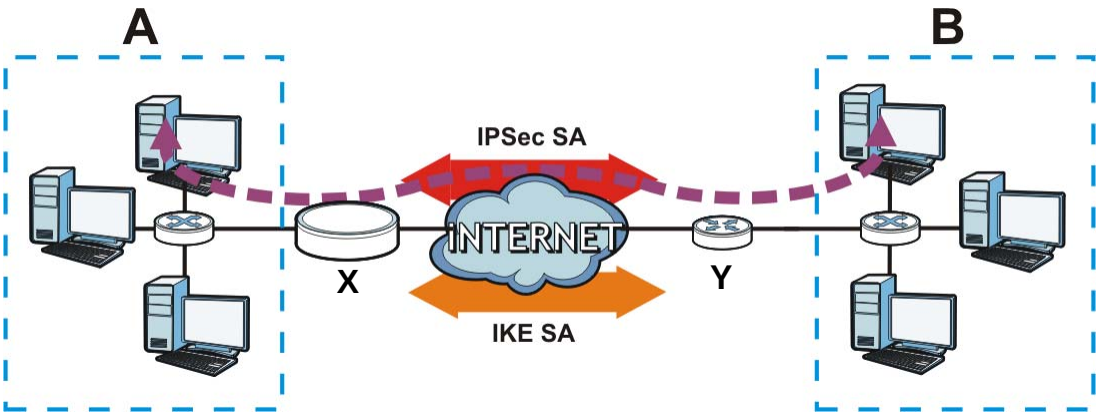


The VPN tunnel connects the ISG50 and the remote (peer) IPSec router (**X**). These routers then connect the local network (**A**) and remote network (**B**).

A VPN tunnel is usually established in two phases. Each phase establishes a security association (SA), a contract indicating what security parameters the ISG50 and the remote IPSec router will use. The first phase establishes an Internet Key Exchange (IKE) SA between the ISG50 and remote IPSec router. The second phase uses the IKE SA to securely establish an IPSec SA through which

the ISG50 and remote IPSec router can send data between computers on the local network and remote network. This is illustrated in the following figure.

Figure 20 VPN: IKE SA and IPSec SA



In this example, a computer in network **A** is exchanging data with a computer in network **B**. Inside networks **A** and **B**, the data is transmitted the same way data is normally transmitted in the networks. Between routers **X** and **Y**, the data is protected by tunneling, encryption, authentication, and other security features of the IPSec SA. The IPSec SA is secure because routers **X** and **Y** established the IKE SA first.

17.2 IPSec VPN Commands Summary

The following table describes the values required for many IPSec VPN commands. Other values are discussed with the corresponding commands.

Table 63 Input Values for IPSec VPN Commands

LABEL	DESCRIPTION
profile_name	The name of a VPN concentrator. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
policy_name	The name of an IKE SA. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
map_name	The name of an IPSec SA. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
domain_name	Fully-qualified domain name. You may use up to 254 alphanumeric characters, dashes (-), or periods (.), but the first character cannot be a period.
e_mail	An e-mail address. You can use up to 63 alphanumeric characters, underscores (_), dashes (-), or @ characters.

Table 63 Input Values for IPSec VPN Commands (continued)

LABEL	DESCRIPTION
distinguished_name	A domain name. You can use up to 511 alphanumeric, characters, spaces, or .@=,_- characters.
sort_order	Sort the list of currently connected SAs by one of the following classifications. algorithm encapsulation inbound name outbound policy timeout uptime

The following sections list the IPSec VPN commands.

17.2.1 IKE SA Commands

This table lists the commands for IKE SAs (VPN gateways).

Table 64 isakmp Commands: IKE SAs

COMMAND	DESCRIPTION
show isakmp keepalive	Displays the Dead Peer Detection period.
show isakmp policy [*policy_name*]	Shows the specified IKE SA or all IKE SAs.
isakmp keepalive <2..60>	Sets the Dead Peer Detection period.
[no] isakmp policy *policy_name*	Creates the specified IKE SA if necessary and enters sub-command mode. The no command deletes the specified IKE SA.
activate deactivate	Activates or deactivates the specified IKE SA.
authentication {pre-share | rsa-sig}	Specifies whether to use a pre-shared key or a certificate for authentication.
certificate *certificate-name*	Sets the certificate that can be used for authentication.
[no] dpd	Enables Dead Peer Detection (DPD). The no command disables DPD.
[no] fall-back	Set this to have the ISG50 reconnect to the primary address when it becomes available again and stop using the secondary connection, if the connection to the primary address goes down and the ISG50 changes to using the secondary connection. Users will lose their VPN connection briefly while the ISG50 changes back to the primary connection. To use this, the peer device at the secondary address cannot be set to use a nailed-up VPN connection.
fall-back-check-interval <60..86400>	Sets how often (in seconds) the ISG50 checks if the primary address is available.
mode {main | aggressive}	Sets the negotiating mode.

Table 64 isakmp Commands: IKE SAs (continued)

COMMAND	DESCRIPTION
transform-set isakmp-algo [isakmp_algo [isakmp_algo]]	Sets the encryption and authentication algorithms for each proposal. ISAKMP_ALGO: {des-md5 | des-sha | 3des-md5 | 3des-sha | aes128-md5 | aes128-sha | aes192-md5 | aes192-sha | aes256-md5 | aes256-sha}
lifetime <180..3000000>	Sets the IKE SA life time to the specified value.
group1 group2 group5	Sets the DH*x* group to the specified group.
[no] natt	Enables NAT traversal. The no command disables NAT traversal.
local-ip {ip {*ip* | *domain_name*} | interface *interface_name*}	Sets the local gateway address to the specified IP address, domain name, or interface.
peer-ip {*ip* | *domain_name*} [*ip* | *domain_name*]	Sets the remote gateway address(es) to the specified IP address(es) or domain name(s).
keystring *pre_shared_key*	Sets the pre-shared key that can be used for authentication. The PRE_SHARED_KEY can be: • 8 - 32 alphanumeric characters or ,;|`~!@#$%^&*()_+\{}':./<>=-". • 16 - 64 hexadecimal (0-9, A-F) characters, preceded by "0x". The pre-shared key is case-sensitive.
local-id type {ip *ip* | fqdn *domain_name* | mail *e_mail* | dn *distinguished_name*}	Sets the local ID type and content to the specified IP address, domain name, or e-mail address.
peer-id type {any | ip *ip* | fqdn *domain_name* | mail *e_mail* | dn *distinguished_name*}	Sets the peer ID type and content to any value, the specified IP address, domain name, or e-mail address.
[no] xauth type {server *xauth_method* | client name *username* password *password*}	Enables extended authentication and specifies whether the ISG50 is the server or client. If the ISG50 is the server, it also specifies the extended authentication method (aaa authentication *profile_name*); if the ISG50 is the client, it also specifies the username and password to provide to the remote IPSec router. The no command disables extended authentication. *username*: You can use alphanumeric characters, underscores (_), and dashes (-), and it can be up to 31 characters long. *password*: You can use most printable ASCII characters. You cannot use square brackets [ ], double quotation marks ("), question marks (?), tabs or spaces. It can be up to 31 characters long.
isakmp policy rename *policy_name policy_name*	Renames the specified IKE SA (first *policy_name*) to the specified name (second *policy_name*).

17.2.2 IPSec SA Commands (except Manual Keys)

This table lists the commands for IPSec SAs, excluding manual keys (VPN connections using VPN gateways).

Table 65 crypto Commands: IPSec SAs

COMMAND	DESCRIPTION
[no] crypto ignore-df-bit	Fragment packets larger than the MTU (Maximum Transmission Unit) that have the "don't" fragment" bit in the header turned on. The no command has the ISG50 drop packets larger than the MTU that have the "don't" fragment" bit in the header turned on.
show crypto map [*map_name*]	Shows the specified IPSec SA or all IPSec SAs.
crypto map dial *map_name*	Dials the specified IPSec SA manually. This command does not work for IPSec SAs using manual keys or for IPSec SAs where the remote gateway address is 0.0.0.0.
[no] crypto map *map_name*	Creates the specified IPSec SA if necessary and enters sub-command mode. The no command deletes the specified IPSec SA.
crypto map rename *map_name map_name*	Renames the specified IPSec SA (first *map_name*) to the specified name (second *map_name*).
crypto map *map_name*	
activate deactivate	Activates or deactivates the specified IPSec SA.
ipsec-isakmp *policy_name*	Specifies the IKE SA for this IPSec SA and disables manual key.
encapsulation {tunnel | transport}	Sets the encapsulation mode.
transform-set *esp_crypto_algo* [*esp_crypto_algo* [*esp_crypto_algo*]]	Sets the active protocol to ESP and sets the encryption and authentication algorithms for each proposal. *esp_crypto_algo*: {esp-3des-md5 | esp-3des-sha | esp-aes128-md5 | esp-aes128-sha | esp-aes192-md5 | esp-aes192-sha | esp-aes256-md5 | esp-aes256-sha | esp-des-md5 | esp-des-sha | esp-null-md5 | esp-null-sha}
transform-set {ah-md5 | ah-sha} [{ah-md5 | ah-sha} [{ah-md5 | ah-sha}]]	Sets the active protocol to AH and sets the encryption and authentication algorithms for each proposal.
scenario {site-to-site-static|site-to-site-dynamic|remote-access-server|remote-access-client}	Select the scenario that best describes your intended VPN connection. Site-to-site: The remote IPSec router has a static IP address or a domain name. This ISG50 can initiate the VPN tunnel. site-to-site-dynamic: The remote IPSec router has a dynamic IP address. Only the remote IPSec router can initiate the VPN tunnel. remote-access-server: Allow incoming connections from IPSec VPN clients. The clients have dynamic IP addresses and are also known as dial-in users. Only the clients can initiate the VPN tunnel. remote-access-client: Choose this to connect to an IPSec server. This ISG50 is the client (dial-in user) and can initiate the VPN tunnel.

Table 65 crypto Commands: IPSec SAs (continued)

COMMAND	DESCRIPTION
set security-association lifetime seconds <180..3000000>	Sets the IPSec SA life time.
set pfs {group1 | group2 | group5 | none}	Enables Perfect Forward Secrecy group.
local-policy *address_name*	Sets the address object for the local policy (local network).
remote-policy *address_name*	Sets the address object for the remote policy (remote network).
[no] policy-enforcement	Drops traffic whose source and destination IP addresses do not match the local and remote policy. This makes the IPSec SA more secure. The no command allows traffic whose source and destination IP addresses do not match the local and remote policy. Note: You must allow traffic whose source and destination IP addresses do not match the local and remote policy, if you want to use the IPSec SA in a VPN concentrator.
[no] nail-up	Automatically re-negotiates the SA as needed. The no command does not.
[no] replay-detection	Enables replay detection. The no command disables it.
[no] netbios-broadcast	Enables NetBIOS broadcasts through the IPSec SA. The no command disables NetBIOS broadcasts through the IPSec SA.
[no] out-snat activate	Enables out-bound traffic SNAT over IPSec. The no command disables out-bound traffic SNAT over IPSec.
out-snat source *address_name* destination *address_name* snat *address_name*	Configures out-bound traffic SNAT in the IPSec SA.
[no] in-snat activate	Enables in-bound traffic SNAT in the IPSec SA. The no command disables in-bound traffic SNAT in the IPSec SA.
in-snat source *address_name* destination *address_name* snat *address_name*	Configures in-bound traffic SNAT in the IPSec SA.
[no] in-dnat activate	Enables in-bound traffic DNAT in the IPSec SA. The no command disables in-bound traffic DNAT in the IPSec SA.
in-dnat delete <1..10>	Deletes the specified rule for in-bound traffic DNAT in the specified IPSec SA.
in-dnat move <1..10> to <1..10>	Moves the specified rule (first rule number) to the specified location (second rule number) for in-bound traffic DNAT.
in-dnat append protocol {all | tcp | udp} original-ip *address_name* <0..65535> <0..65535> mapped-ip *address_name* <0..65535> <0..65535>	Maps the specified IP address and port range (original-ip) to the specified IP address and port range (mapped-ip) and appends this rule to the end of the rule list for in-bound traffic DNAT.
in-dnat insert <1..10> protocol {all | tcp | udp} original-ip *address_name* <0..65535> <0..65535> mapped-ip *address_name* <0..65535> <0..65535>	Maps the specified IP address and port range (original-ip) to the specified IP address and port range (mapped-ip) and inserts this rule before the specified rule.
in-dnat <1..10> protocol {all | tcp | udp} original-ip *address_name* <0..65535> <0..65535> *mapped-ip address_name* <0..65535> <0..65535>	Creates or revises the specified rule and maps the specified IP address and port range (original-ip) to the specified IP address and port range (mapped-ip).

17.2.3 IPSec SA Commands (for Manual Keys)

This table lists the additional commands for IPSec SAs using manual keys (VPN connections using manual keys).

Table 66 crypto map Commands: IPSec SAs (Manual Keys)

COMMAND	DESCRIPTION
`crypto map map_name`	
`set session-key {ah <256..4095> auth_key | esp <256..4095> [cipher enc_key] authenticator auth_key}`	Sets the active protocol, SPI (<256..4095>), authentication key and encryption key (if any). *auth_key*: You can use any alphanumeric characters or ,;|`~!@#$%^&*()_+\{}':./<>=-". The length of the key depends on the algorithm. md5 - 16-20 characters sha - 20 characters *enc_key*: You can use any alphanumeric characters or ,;\|`~!@#$%^&*()_+\{}':./<>=-". The length of the key depends on the algorithm. des - 8-32 characters 3des - 24-32 characters aes128 - 16-32 characters aes192 - 24-32 characters aes256 - 32 characters If you want to enter the key in hexadecimal, type “0x” at the beginning of the key. For example, "0x0123456789ABCDEF" is in hexadecimal format; in “0123456789ABCDEF” is in ASCII format. If you use hexadecimal, you must enter twice as many characters. The ISG50 automatically ignores any characters above the minimum number of characters required by the algorithm. For example, if you enter 1234567890XYZ for a DES encryption key, the ISG50 only uses 12345678. The ISG50 still stores the longer key.
`local-ip ip`	Sets the local gateway address to the specified IP address.
`peer-ip ip`	Sets the remote gateway address to the specified IP address.

17.2.4 VPN Concentrator Commands

This table lists the commands for the VPN concentrator.

Table 67 vpn-concentrator Commands: VPN Concentrator

COMMAND	DESCRIPTION
`show vpn-concentrator [profile_name]`	Shows the specified VPN concentrator or all VPN concentrators.
`[no] vpn-concentrator profile_name`	Creates the specified VPN concentrator if necessary and enters sub-command mode. The no command deletes the specified VPN concentrator.

Table 67 vpn-concentrator Commands: VPN Concentrator (continued)

COMMAND	DESCRIPTION
[no] crypto *map_name*	Adds the specified IPSec SA to the specified VPN concentrator. The no command removes the specified IPSec SA from the specified VPN concentrator.
vpn-concentrator rename *profile_name profile_name*	Renames the specified VPN concentrator (first *profile_name*) to the specified name (second *profile_name*).

17.2.5 SA Monitor Commands

This table lists the commands for the SA monitor.

Table 68 sa Commands: SA Monitor

COMMAND	DESCRIPTION
show sa monitor [{begin <1..1000>} | {end <1..1000>} | {crypto-map *regexp*} | {policy *regexp*} |{rsort *sort_order*} | {sort *sort_order*}]	Displays the current IPSec SAs and the status of each one. You can specify a range of SA entries to display. You can also control the sort order of the display and search by VPN connection or (local or remote) policy. *regexp*: A keyword or regular expression. Use up to 30 alphanumeric and _+-.()!$*^:?|{}[]<>/ characters. A question mark (?) lets a single character in the VPN connection or policy name vary. For example, use "a?c" (without the quotation marks) to specify abc, acc and so on. Wildcards (*) let multiple VPN connection or policy names match the pattern. For example, use "*abc" (without the quotation marks) to specify any VPN connection or policy name that ends with "abc". A VPN connection named "testabc" would match. There could be any number (of any type) of characters in front of the "abc" at the end and the VPN connection or policy name would still match. A VPN connection or policy name named "testacc" for example would not match. A * in the middle of a VPN connection or policy name has the ISG50 check the beginning and end and ignore the middle. For example, with "abc*123", any VPN connection or policy name starting with "abc" and ending in "123" matches, no matter how many characters are in between. The whole VPN connection or policy name has to match if you do not use a question mark or asterisk. See Table 63 on page 126 for other parameter description.
show isakmp sa	Displays current IKE SA and the status of each one.
no sa spi *spi*	Deletes the SA specified by the SPI. *spi*: 2-8 hexadecimal (0-9, A-F) characters
no sa tunnel-name *map_name*	Deletes the specified IPSec SA.
show vpn-counters	Displays VPN traffic statistics.

18

PBX

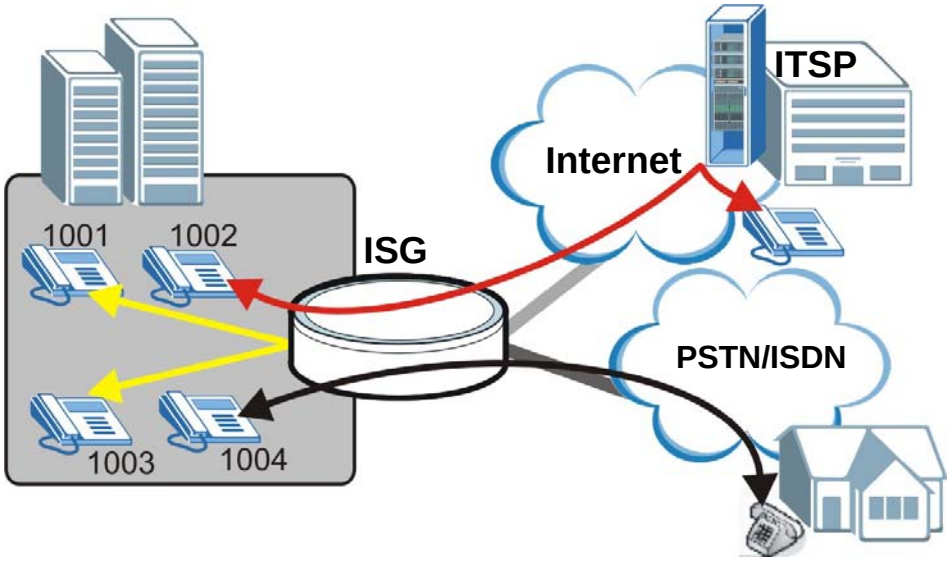
18.1 PBX Overview

An IP PBX is a telephone exchange device located at a company site which allows an organization to set up and control calls. IP stands for Internet Protocol, and PBX stands for Private Branch Exchange. A regular company telephone switchboard is an example of a PBX. The company's telephones are connected to the IP PBX. The IP PBX is then connected to the outside world via connections to any combination of the following networks:

- A traditional Public Switched Telephone Network (PSTN)
- A broadband Internet connection to an Internet Telephony Service Provider (ITSP)
- An Integrated Services Digital Network/Basic Rate Interface Network (ISDN BRI)

Each telephone connected to an IP PBX has an extension assigned to it. An extension is a unique telephone number within an organization typically consisting of only a few digits. People inside the company can call each other by dialing extensions. Calls to the outside world go through the IP PBX to the PSTN, ITSP, or ISDN.

Figure 21 IP PBX Example



The ISG50 can function as a stand alone telephone switchboard for a small organization. It can also supplement a legacy PBX within an organization by providing VoIP telephony features.

18.2 PBX Brute Force Attack Prevention Commands

Use these commands to protect PBX extension passwords from password guessing attacks. The ISG50 can protect extensions' web-portal logins and SIP logins (the sending of SIP register/invite packets from a SIP client). The following table describes the PBX brute force attack prevention commands. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 69 PBX Brute Force Attack Prevention Commands Summary

COMMAND	DESCRIPTION
`pbx attack-prevent {web-login|sip} block-time <1..1440>`	Set for how many minutes to block an extension's web-portal login or SIP access after the allowed number of failed access attempts is reached.
`pbx attack-prevent {web-login|sip} fail-access <1..10>`	Set how many consecutive failed web-portal login or SIP access attempts are allowed for an extension before the ISG50 blocks access to the extension.
`pbx attack-prevent {web-login|sip} unlock {all|`*`pbx_exten_num`*`}`	Unlock web-portal login or SIP access for extensions locked by brute force attack prevention. You can unlock all locked extensions or the specified locked extension. *`pbx_exten_num`*: The 3-10 digit extension number.
`[no] pbx attack-prevent {web-login|sip} activate`	Turns brute force attack prevention on or off for web-portal login or SIP access. Note: Turning off brute force attack prevention automatically unlocks all locked extensions.
`show pbx attack-prevent {web-login|sip}`	Displays the brute force attack prevention configuration for web-portal login or SIP access.
`show pbx attack-prevent {web-login|sip} lock-list`	Displays the list of extensions for which brute force attack prevention has locked web-portal login or SIP access.

18.2.1 PBX Brute Force Attack Prevention Command Examples

Here are some examples of using PBX brute force attack prevention commands.

18.2.1.1 PBX Brute Force Attack Prevention Configuration Example

The following example sets the PBX brute force attack prevention web-portal login blocking time to 100 minutes, sets the PBX brute force attack prevention web-portal login fail count to 4, turns on PBX brute force attack prevention, and displays the configuration.

After four consecutive failed attempts to log into an extension's web-portal, the ISG50 blocks access to the extension's web-portal for 100 minutes.

```
Router> configure terminal
Router(config)# pbx attack-prevent web-login block-time 100
Router(config)# pbx attack-prevent web-login fail-count 4
Router(config)# pbx attack-prevent web-login activate
Router(config)# show pbx attack-prevent web-login
block-time         fail-count                    activate
================================================================
100                        4                                  yes
```

18.2.1.2 PBX Brute Force Attack Prevention Locked Extensions Example

The following example displays the list of extensions with web-login access blocked by PBX brute force attack prevention and then unlocks extension 1002.

```
Router# configure terminal
Router(config)# show pbx attack-prevent web-login lock-list
extension         lock-time                    unlock-time
================================================================
1001           2011/05/31 19:05:55     2011/05/31 20:05:55
1002           2011/05/31 18:55:55     2011/05/31 19:55:55
Router(config)# pbx attack-prevent web-login unlock 1002
```

18.3 PBX Monitor Commands

The following table describes the PBX monitor commands. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 70 PBX Monitor Commands Summary

COMMAND	DESCRIPTION
`show pbx monit-status {bri-trunk|cti-peer|fxo-trunk|fxs-peer|sip-peer|sip-trunk} all`	Displays the selected PBX status details.
`no pbx monit-status channel <channel_id>`	Hangs up the call for the specified channel in an FXO trunk or SIP peer. Use the `show pbx monit-status` command to display the channel IDs.

18.3.1 PBX Monitor Command Examples

Here are some examples of using PBX monitor commands.

18.3.1.1 Show PBX Monitor Status Command Example

The following example displays FXO trunk details for all of the ISG50's FXO trunks.

```
Router# configure terminal
Router(config)# show pbx monit-status fxo-trunk all
Slot                        Port                        Group Name                    Call
Status                    Channel

================================================================================
A                       1                       N/A                       Idle
N/A

A                       2                       N/A                       Idle
N/A

A                       3                       N/A                       Idle
N/A

A                       4                       N/A                       Idle
N/A
```

18.3.1.2 PBX Hang Up Command Example

The following example hangs up the SIP/1001-001 channel.

```
Router# configure terminal
Router(config)#no pbx monit-status channel SIP/1001-001
```

18.4 PBX CDR Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 71 Input Values for PBX CDR Commands

LABEL	DESCRIPTION
port	The database connect port. <1..65535>
cdr_row_limit	When the CDR database has more rows than this many rows, the ISG50 backs up the CDR database to a backup file. <1..100000>
cdr_row_offset	The index number of a row in the CDR database. <1..100000>
cdr_flag	The CDR action flag (on|off).
cdr_aged_act	Sets how to handle aged backup files (drop|mail).
cdr_backup_type	CDR backup file type (sql|csv).
cdr_db_field	Name of a database field. [0-9a-zA-Z_]+
cdr_db_order	Sets the CDR database order to ascending or descending. (asc|desc|ASC|DESC)
cdr_db_user	Username for the CDR database. [0-9a-zA-Z_]+
cdr_db_password	Password for the CDR database. [0-9a-zA-Z_ ,#@\"'/\\]+

Table 71 Input Values for PBX CDR Commands (continued)

LABEL	DESCRIPTION
cdr_backup_index	backup file index. [1-9]+
cdr_query_condition	CDR query condition. [0-9a-zA-Z_ @#%=():<,>\-\"'\/\\]+
cdr_db_name	CDR database name. [0-9a-zA-Z_]+
cdr_db_table	Table name of the CDR database. [0-9a-zA-Z_]+
cdr_conn_timeout	CDR connection timeout. [0-9]+

The following table describes the CDR (Call Detail Record) commands You must use the `configure terminal` command to enter the configuration mode before you can use these commands. s

Table 72 PBX CDR Commands Summary

COMMAND	DESCRIPTION
`show log cdr config`	Displays the CDR configuration.
`show log cdr database`	Displays the CDR database configuration.
`show log cdr database usage`	Displays the percentage of CDR database usage.
`show log cdr backup`	Displays the backups of CDR files.
`show log cdr report offset` *cdr_row_offset* `limit` *cdr_row_limit* `order` *cdr_db_field* `in` *cdr_db_order* `condition` *cdr_query_condition*	Generates a CDR report for the specified query condition and field sorting.
`log cdr config email` *e-mail*	Sets the email address to which the ISG50 sends CDR usage warning and aged file mails.
`log cdr config internal-call` *cdr_flag*	Sets whether or not to log internal calls in the CDR database.
`log cdr config alert` *cdr_flag*	Sets whether or not to send an alert to the administrator's email address when the CDR database usage reaches 80%.
`log cdr config aged-action` *cdr_aged_act*	Sets whether to drop or mail an aged backup file.
`log cdr config backup-type` *cdr_backup_type*	Sets whether backup files are "sql" or "csv".
`log cdr database remote` *cdr_flag*	Sets whether or not to use the remote PostgreSQL database server as the CDR log server.
`log cdr database hostname` *fqdn*	Sets the connection address of the remote database server.
`log cdr database port` *port*	Sets the connection port for the remote database server.
`log cdr database user` *cdr_db_user*	Sets the username for connecting to the remote database server.
`log cdr database password` *cdr_db_password*	Sets the password for connecting to the remote database server.
`log cdr database dbname` *cdr_db_name*	Sets the database name for the remote database server.
`log cdr database table` *cdr_db_table*	Sets the table name for the remote database server.
`log cdr database connect_timeout` *cdr_conn_timeout*	Sets the connection timeout for the remote database server.
`log cdr backup forward` *cdr_backup_index*	Mails a database backup file to the administrator.
`log cdr backup now`	Backs up the CDR database to a backup file right now.

Table 72 PBX CDR Commands Summary (continued)

COMMAND	DESCRIPTION
`no log cdr config all`	Removes all CDR configuration and has the ISG50 use the default CDR behavior.
`no log cdr config email`	Removes the CDR administrator email setting.
`no log cdr config internal-call`	Resets to the default internal-call setting, which is “off”.
`no log cdr config alert`	Resets to the default alert setting, which is “off”.
`no log cdr config aged-action`	Resets to the default action for aged backup files, which is “drop”.
`no log cdr config backup-type`	Resets to the default backup-type setting, which is “sql”.
`no log cdr database remote`	Resets to the default remote setting, which is “off”.
`no log cdr backup` *`cdr_backup_index`*	Deletes the CDR backup file with the specified backup file index.

18.4.1 PBX CDR Command Examples

Here are some examples of using PBX commands.

18.4.1.1 Qeury CDR Report Example

The following example queries the CDR report.

```
Router# configure terminal
Router(config)# show show log cdr report offset 0 limit 5000 order calldate in asc condition
WHERE calldate between now()-interval '7 day' and now()
row: 0
  calldate: 2011/04/20 15:06:20
  clid: 1002
  src: 1002
  dst: 1001
  dcontext: paa_voicemail
  channel: SIP/1002
  dstchannel:
  duration: 22
  billsec: 22
  disposition: ANSWERED
  record:
  rtcp:
row: 1
  calldate: 2011/04/20 15:07:03
  clid: 1002
  src: 1002
  dst: 1001
  dcontext: paa_voicemail
  channel: SIP/1002
  dstchannel:
  duration: 40
  billsec: 40
  disposition: ANSWERED
  record:
  rtcp:
```

18.4.1.2 Display CDR Backup Files Example

The following example displays all CDR backup files.

```
Router# configure terminal
Router(config)# show log cdr backup
index            filename
================================================================ 1
cdr.20110314113626.sql.tgz
2                cdr.20110331190421.sql.tgz
```

18.4.1.3 Remove CDR Backup Files Example

The following example deletes the first CDR backup file.

```
Router# configure terminal
Router(config)# no log cdr backup 1
```

18.5 Global PBX Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 73 Input Values for Global PBX Commands

LABEL	DESCRIPTION
sipconf_realmname	The SIP server realm name. You may use 1-63 of the following characters [a-zA-Z0-9\._-].

The following table describes the commands for showing and configuring global PBX settings. Use the `enable` or `configure terminal` command to be able to use the show commands. You must use the `configure terminal` command to enter the configuration mode before you can use the configuration commands.

Table 74 PBX Global Commands Summary

COMMAND	DESCRIPTION
`show pbx monit-status {all|fakeip-info|p2p-info|p2p-localnet}`	Displays the selected PBX global setting details.
`pbx global`	Enters the sub-command mode for configuring PBX global settings.
`realm` *sipconf_realmname*	Sets the SIP server realm name.
`port <1..65535>`	Sets the ISG50's listening port number. This is the port number your SIP clients need to use to register with the ISG50.
`register-timer-nonat <60..86400>`	Sets the number of seconds SIP clients that use the UDP or TCP protocol but do not use NAT are registered with the ISG50 (that acts as a SIP registrar) before their registration record is deleted.
`register-timer-nat <60..86400>`	Sets the number of seconds SIP clients that use NAT and the UDP protocol are registered with the ISG50 (that acts as a SIP registrar) before their registration record is deleted.
`register-timer-nat-tcp <60..86400>`	Sets the number of seconds SIP clients that use NAT and the TCP protocol are registered with the ISG50 (that acts as a SIP registrar) before their registration record is deleted.
`rtp-port-start <1..65535>`	Sets the port number at the beginning of the range of listening port numbers for RTP traffic.
`rtp-port-end <1..65535>`	Sets the port number at the end of the range of listening port numbers for RTP traffic.
`dns-srv {disable|enable}`	Sets whether or not to query your ISP's DNS server for a list of any available SIP servers that it maintains.
`rtcp-status {disable|enable}`	Sets whether or not to use RTCP (RTP Control Protocol) as an optional signalling protocol for SIP traffic.
`session-timer-mode {originate|refuse}`	Sets the session timer mode.
`session-timer-expires <60..86400>`	Sets the duration in seconds before an idle SIP connection expires.
`session-timer-minse <90..1800>`	Sets the minimum time in seconds before an idle SIP connection expires.
`register-timeout <2..32>`	Sets the number of seconds the ISG50 waits for a response from a SIP registrar before considering the SIP registration timed out and re-registering.

Table 74 PBX Global Commands Summary (continued)

COMMAND	DESCRIPTION
ring-timer <1..300>	Sets for how many seconds to send a ringing tone to client devices for incoming calls.
internal-aa {disable|enable}	Sets whether or not to enable the ISG50's auto-attendant feature for calls received from outside the PBX-managed telephone system.
external-aa {disable|enable}	Sets whether or not to enable the ISG50's auto-attendant feature for calls received from within the PBX-managed telephone system.
p2p-status {disable|enable}	Sets whether or not to set up direct connections between two IP phones on the same subnet. If you enable it, set up the local net for peer to peer.
(no) p2p-localnet *ipv4_cidr*	Defines a subnet for which the ISG50 can set up peer-to-peer networking. Enter an IPv4-compatible IP address in this field then select the length of the subnet mask from the list.
fakeip-status {disable|enable}	Enables to replace the IP address inside all outgoing SIP packets with the IP address of the upstream NAT router on your network. If you enable it, configure the fake IP address.
fakeip-address {*ipv4*|*hostname*}	Specifies the public IP address that the upstream NAT router uses to send out the ISG50's SIP traffic. This is the IP address that will be inserted into all outgoing SIP traffic.
exit	Leaves the sub-command mode.

18.5.1 Global PBX Command Examples

Here are some examples of using PBX global commands.

18.5.1.1 Show Global PBX Command Example

The following example displays the global PBX settings.

```
Router> show pbx global all
Realm: default
port: 5060
Register expiration with NAT: 60
Register expiration NonNAT: 3600
RTP start port: 10000
RTP end port: 20000
Ring time: 20
RTCP flag: enable
Personal AA status: disable
Extern personal AA status: enable
DNS SRV status: disable
Session timer mode: refuse
Session timer expires: 1800
Session timer minse: 90
Register limit: 30,22,14,6,1
Invite limit: 15,11,7,3,1
```

18.5.1.2 Show Global PBX Peer-to-peer Status Command Example

The following example displays the global PBX peer-to-peer status.

```
Router> show pbx global p2p-info
P2p status: disable
```

18.5.1.3 Global Ring Timer and DNS SRV Command Example

The following example configures the PBX global ring timer and enables DNS SRV.

```
Router> configure terminal
Router(config)#pbx global
Router(config-pbx-sipconfig)#ring-timer 30
Router(config-pbx-sipconfig)#dns-srv enable
Router(config-pbx-sipconfig)# exit
Router(config)# exit
Router#
```

18.6 Feature Code PBX Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 75 Input Values for Feature Code PBX Commands

LABEL	DESCRIPTION
exten_num	An extension number already configured in the ISG50.
feature_code	The code a user dials to enable or diable a feature for the user's extension. [0-9*]{1,3} Here are the default feature code values: Group-pickup: *94 Call Transfer: *96 Direct Pickup: *95 Follow Me On: *22 Follow Me Off: *23 Voice Mail: ** Mobile Extension On: *97 Mobile Extension Off: *98 Mobile Extension Auto: *99 Call Recording On Demand: *88

The following table describes the commands for showing and configuring PBX feature code PBX settings. A user can dial these codes to enable or disable features for their extension by entering these codes on his phone's keypad. Use the `enable` or `configure terminal` command to be able to

use the show commands. You must use the `configure terminal` command to enter the configuration mode before you can use the configuration commands.

Table 76 Feature Code PBX Commands Summary

COMMAND	DESCRIPTION
`show pbx feature-code all`	Displays all of the feature code settings.
`pbx feature-code`	Enters the sub-command mode for configuring feature code settings.
`[no] second-dial <0-9>`	Sets or disables the code to get a second dial tone (for the outside telephone network).
`internal-operator {0|9} extension` *`exten_num`*	Sets which number (0 or 9) internal users dial to reach the internal operator and specifies the operator's extension number.
`no internal-operator`	Turns off the internal operator feature.
`group-pickup` *`feature_code`*	Sets the code that allows you to pick up calls for your extension from a different extension in the same authority group.
`direct-pickup` *`feature_code`*	Sets the code for picking up calls for your extension from a different extension.
`call-transfer` *`feature_code`*	Sets the code for transferring calls.
`voicemail` *`feature_code`*	Sets the code for accessing voice mail.
`followme-on` *`feature_code`*	Sets the code for turning on the Follow Me feature for this extension.
`followme-off` *`feature_code`*	Sets the code for turning off the Follow Me feature for this extension.
`mobile-extension-on` *`feature_code`*	Sets the code for sending calls to both your extension and the phone designated as the user's mobile extension.
`mobile-extension-off` *`feature_code`*	Sets the code for turning off the mobile extension feature from your regular telephone extension.
`mobile-extension-auto` *`feature_code`*	Sets the code for changing the mobile extension feature's setting from off to on or from on to off.
`call-recording-on-demand` *`feature_code`*	Sets the code to start recording the current call.
`exit`	Leaves the sub-command mode.

18.6.1 Feature Code PBX Command Examples

Here are some examples of using PBX feature code commands.

18.6.1.1 Show Feature Code Settings Command Example

The following example displays the feature code settings.

```
Router> configure terminal
Router(config)# show pbx feature-code all
group pickup: *11
direct pickup: *95
call transfer: *10
voice mail: **
followme on: *22
followme off: *23
second dial:
mobile extension on: *97
mobile extension off: *98
mobile extension auto: *99
internal operator:
internal operator ext:
call record on demand: *88
Router(config)#
```

18.6.1.2 Configuring Feature Codes Command Example

The following example configures the codes for the group pickup, and call transfer features.

```
Router> configure terminal
Router(config)# pbx feature-code
Router(Feature Code)# group-pickup *11
Router(Feature Code)# call-transfer *10
Router(Feature Code)# exit
Router(config)#
```

18.7 E-mail PBX Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 77 Input Values for E-mail PBX Commands

LABEL	DESCRIPTION
e_mail	An e-mail address. You can use up to 80 alphanumeric characters, underscores (_), periods (.), or dashes (-), and you must use the @ character.

The following table describes the commands for showing and configuring PBX e-mail settings for sending voice mails and Call Detail Records (CDRs). Use the `enable` or `configure terminal`

command to be able to use the show commands. You must use the `configure terminal` command to enter the configuration mode before you can use the configuration commands.

Table 78 E-mail PBX Commands Summary

COMMAND	DESCRIPTION
`pbx mail`	Enters the sub-command mode for configuring PBX e-mail settings.
`smtp-address {`*`ip`*` | `*`hostname`*`}`	Sets the SMTP mail server IP address or domain name.
`[no] smtp-auth activate`	Enables or disables SMTP authentication.
`no smtp-address`	Resets the SMTP mail server configuration.
`mail-from `*`e_mail`*	Sets the sender value of the PBX e-mails.
`no mail-from`	Clears the configured sender value of the PBX e-mails.
`smtp-auth username `*`username`*` password `*`password`*	Sets the username and password for SMTP authentication.
`no smtp-auth username`	Resets the authentication configuration.
`exit`	Leaves the sub-command mode.
`show pbx mail`	Displays the PBX e-mail server settings.

18.7.1 E-mail PBX Command Examples

Here are some examples of using PBX e-mail commands.

18.7.1.1 PBX E-mail Settings Command Example

The following example configures the settings for sending PBX e-mails.

```
To configure E-Mail server setting
Router> configure terminal
Router(config)#pbx mail
Router(config)# smtp-address 192.168.125.214
Router(config)# smtp-auth activate
Router(config)# mail-from xxx@example.com
Router(config)# smtp-auth username xxx password 1234
Router(config)# exit
Router#
```

18.7.1.2 Show PBX E-mail Settings Command Example

The following example displays the PBX e-mail settings.

```
Router> show pbx mail
smtp-address: 192.168.125.214
mail-from: xxx@example.com
smtp-auth: yes
username: xxx
password: 1234
```

18.8 QoS PBX Commands

The following table describes the commands for showing and configuring PBX QoS (DSCP) settings for sending SIP and RTP packets and auto provisioning the DSCP value to phones. Use the `enable` or `configure terminal` command to be able to use the show commands. You must use the `configure terminal` command to enter the configuration mode before you can use the configuration commands.

Table 79 QoS PBX Commands Summary

COMMAND	DESCRIPTION
`pbx dscp`	Enters the sub-command mode for configuring PBX QoS settings.
`{sip|audio} class {default|af11|af12|af13|af21|af22|af23|af31|af32|af33|af41|af42|af43}`	Sets the DSCP setting for SIP control packets or SIP audio payload packets (RTP) to one of the Assured Forwarding (AF) values. See Section 8.2.1 on page 88 for more on Assured Forwarding.
`{sip|audio} <0..63>`	Sets the DSCP setting for SIP control packets or SIP audio payload packets (RTP) to the specified value.
`exit`	Leaves the sub-command mode.
`show pbx dscp`	Displays the PBX QoS settings.

18.8.1 QoS PBX Command Examples

Here are some examples of using PBX QoS commands.

18.8.1.1 PBX QoS Settings Command Example

The following example configures the SIP and audio DSCP settings.

```
Router> configure terminal
Router(config)#pbx dscp
Router(config)# sip class af11
Router(config)# audio 40
Router(config)# exit
Router#
```

18.8.1.2 Show PBX QoS Settings Command Example

The following example displays the SIP and audio DSCP settings.

```
Router# show pbx dscp
type       value
================================================================================
sip        af11
audio      40
```

18.9 Voice Interface Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 80 Input Values for Voice Interface Commands

LABEL	DESCRIPTION
voiceport	The location of the PSTN port. <1-5>
gain_level	The level of volume gain for telephone signals sent from or received by the port. <-6-6> -6 is the quietest, and 6 is the loudest.
country_code	The lower-case, three-letter country code for the port.
busytone_frequency1 /2	The frequency (in Hz) of a busy tone. <0-999>
busytone_ontime	The cadence On time (in ms) of a busy tone. <0-999>
busytone_offtime	The cadence Off time (in ms) of a busy tone. <0-999>

18.9.1 PSTN Voice Interface Commands

The following table describes the commands for showing and configuring PSTN port settings. Use the `enable` or `configure terminal` command to be able to use the show commands. You must use the `configure terminal` command to enter the configuration mode before you can use the configuration commands.

Table 81 PSTN Voice Interface Commands Summary

COMMAND	DESCRIPTION
[no] voice-port <*voiceport*> {fxo|fxs}	Enters the sub-command mode for configuring the specified PSTN port.
[no] cptone *country_code*	Sets the country code which controls the telephone signals to use for the port. The no command restores the default setting.
no custom-busytone	Removes the tone frequency and cadence settings that you specify.
custom-busytone frequency *busytone_frequency1* [*busytone_frequency2*] cadence *busytone_ontime busytone_offtime*	Sets the frequency(ies) and cadence of the busy tone, a signal that indicates the line is busy.
[no] tx-volume *gain_level*	Sets the volume level for telephone signals transmitted from the port. The no command restores the default setting.
[no] rx-volume *gain_level*	Sets the volume level for telephone signals recieved through the port. The no command restores the default setting.
[no] dial-interval <1-10>	Sets the number of seconds to wait after the user stops dialing numbers before making the phone call. The no command restores the default setting.
[no] busy-detect <1-10>	Sets the number of busy tones that have to be detected before the port plays a busy tone for an incoming call. The no command restores the default setting.

Table 81 PSTN Voice Interface Commands Summary (continued)

COMMAND	DESCRIPTION
[no] fax-protocol <pass-through|t38>	Sets how the FXS port handles fax messages. Use pass-through to use UDP packets with G.711 format or t38 to use T.38 format. T.38 provides better quality, but the peer devices must also use T.38. The no command restores the default setting.
exit	Leaves the sub-command mode.
show voice-port <*voiceport* | all>	Displays the voice port's settings.

18.9.2 PSTN Voice Interface Command Examples

Here are some examples of configuring PSTN port settings.

18.9.2.1 PSTN Voice Interface Settings Command Example

The following example configures the FXO PSTN port 1 to use the USA country code, -1 for the TX volume, -2 for the RX volutme, and 5 seconds for the dial interval.

```
Router(config)# voice-port 1 fxo
Router(config-voiceport 1)# cptone usa
Router(config-voiceport 1)# tx-volume -1
Router(config-voiceport 1)# rx-volume 1
Router(config-voiceport 1)# dial-interval 5
Router(config-voiceport 1/1)# exit
Router(config)#
```

18.9.2.2 PSTN Show Voice Interface Settings Command Example

The following example displays the settings for one PSTN voice interface or all of them.

```
Router(config)# show voice-port 1
cptone: usa
dial interval: 5
rx volume: -1
tx volume: -1
fax-protocol:
Router(config)# show voice-port all
Position        Type            State
=====================================================================
1               FXO             Connected
2               FXO             Connected
3               FXO             Connected
4               FXO             Not connected or malfunction
5               FXS             On-hook, not connected or malfunction
```

18.9.3 ISDN Voice Interface Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 82 Input Values for ISDN Voice Interface Commands

LABEL	DESCRIPTION
isdn	The location of the ISDN port. <1-4>
number_prefix	The prefix number 1-20 digits in length.
gain_level	The level of volume gain for telephone signals sent from or received by the port. <-6-6> -6 is the quietest, and 6 is the loudest.

The following table describes the commands for showing and configuring ISDN port settings. Use the `enable` or `configure terminal` command to be able to use the show commands. You must use the `configure terminal` command to enter the configuration mode before you can use the configuration commands.

Table 83 ISDN Voice Interface Commands Summary

COMMAND	DESCRIPTION
`[no] isdn <`*isdn*`>` {bri|fxs}	Enters the sub-command mode for configuring the specified ISDN port.
`[no] force-active`	Enables the port. The `no` version of the command disables it.
`[no] incoming-cgpn-abbreviated-prefix` *number_prefix*	Sets the prefix to add to the calling party numbers of incoming abbreviated calls. The `no` command restores the default setting.
`[no] incoming-cgpn-national-prefix` *number_prefix*	Sets the prefix to add to the calling party numbers of incoming national calls. The `no` command restores the default setting.
`[no] incoming-cgpn-subscriber-prefix` *number_prefix*	Sets the prefix to add to the calling party numbers of incoming subscriber calls. The `no` command restores the default setting.
`[no] incoming-cgpn-international-prefix` *number_prefix*	Sets the prefix to add to the calling party numbers of incoming international calls. The `no` command restores the default setting.
`[no] incoming-cgpn-networkspecific-prefix` *number_prefix*	Sets the prefix to add to the calling party numbers of incoming network-specific calls. The `no` command restores the default setting.
`[no] incoming-cgpn-unknown-prefix` *number_prefix*	Sets the prefix to add to the calling party numbers of incoming calls of unknown type. The `no` command restores the default setting.
`[no] isup <overlap-receiving | enbloc>`	Sets the signalling method for receiving a callee's number through the BRI port. `overlap-receiving`: Receive digits of a callee's number one-by-one. `enbloc`: Receive a complete callee's number at one time. The `no` command restores the default setting.
`[no] outgoing-cgpn-ton < unknown | national | international | network-specific | subscriber | abbreviated >`	Sets the type for the prefix number which might be required by your telephone company to make outgoing calls. The `no` command restores the default setting.

Table 83 ISDN Voice Interface Commands Summary (continued)

COMMAND	DESCRIPTION
[no] outgoing-cgpn-ton-prefix *number_prefix*	Sets the number to add to the beginning of the outgoing caller's numbers when using this trunk line. The no command restores the default setting.
[no] tx-volume *gain_level*	Sets the volume level for telephone signals transmitted from the port. The no command restores the default setting.
[no] rx-volume *gain_level*	Sets the volume level for telephone signals recieved through the port. The no command restores the default setting.
[no] tei-number *number_tei*	Sets the Terminal Endpoint Identifier for this TE device. Specify the 0-63 digit number provided by the telephone company or use dynamic to automatically request an ID when the ISG50 is connected to the network. Note: Use the same TEI setting on the port and its connected BRI device.
exit	Leaves the sub-command mode.
show isdn <*isdn* | all>	Displays the ISDN voice port's settings.

18.9.4 ISDN Voice Interface Command Examples

Here are some examples of configuring ISDN port settings.

18.9.4.1 ISDN Voice Interface Settings Command Example

The following example configures the BRI ISDN port 1 to use -1 for the TX volume, 2 for the RX volutme, and the enbloc signalling method for receiving a callee's number.

```
Router(config)# isdn 1 bri
Router(config-isdn 1/1)# tx-volume -1
Router(config-isdn 1/1)# rx-volume 2
Router(config-isdn 1/1)# isup enbloc
Router(config-isdn 1/1)# exit
Router(config)#
```

18.9.4.2 ISDN Show Voice Interface Settings Command Example

The following example displays the settings for all of the ISDN voice interfaces.

```
Router(config)# show isdn all
Position        Type            State
=====================================================================
1               BRI             Power off, layer 1 deactivated or malfunction
2               BRI             Power off, layer 1 deactivated or malfunction
3               BRI             Power off, layer 1 deactivated or malfunction
4               BRI             Power off, layer 1 deactivated or malfunction
```

18.10 Extension Management Commands

These sections cover how to configure settings for managing groups of extensions.

18.10.1 Authority Group Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 84 Input Values for Authority Group Commands

LABEL	DESCRIPTION
pbx_grp_name	The name of the authority group. Use 0-29 alphanumeric characters.
pbx_grp_id	The number of the authority group (1-5 digits).
pbx_description	A description using 0-62 alphanumeric characters (A-Z, a-z, 0-9) and spaces.

The following table describes the commands for creating, editing and removing autority groups. Use the `enable` or `configure terminal` command to be able to use the show commands. You must use the `configure terminal` command to enter the configuration mode before you can use the configuration commands.

Table 85 Authority Group Commands Summary

COMMAND	DESCRIPTION
`no pbx authority-group` *pbx_grp_name*	Deletes the specified authority group.
`pbx authority-group` *pbx_grp_name*	Creates the specified authority group and enters the sub-command mode for configuring it.
`group-id` *pbx_grp_id*	Configures the authority group's ID number.
`description` *pbx_description*	Configures the authority group's description.
`no description`	Removes the authority group's description.
`cac` *cac_code*	Configures the authority group's Call Access Code. Use 5-20 digits.
`no cac`	Removes the authority group's Call Access Code. Use 5-20 digits.
`[no] office-hour dow {sun|mon|tue|wed|thu|fri|sat}`	Enables or disables the authority group's office hour configuration on the specified day of the week.
`[no] office-hour dow {sun|mon|tue|wed|thu|fri|sat} time <0..23>: <0..59>-<0..23>:<0..59>`	Sets the authority group's office hours for the specified day of the week to the specified time period.
`no office-hour dow {sun|mon|tue|wed|thu|fri|sat} time all`	Removes all of the authority group's office hours for the specified day of the week.
`[no] office-hour holiday <01-12>/<01-31>`	Sets the specified month and day as a holiday for the authority group.
`no office-hour holiday all`	Removes all of the authority group's holidays.
`office-hour holiday <01-12>/<01-31> description` *pbx_description*	Adds a descriptive name for the holiday on the specified month and day.
`no office-hour holiday <01-12>/<01-31> description`	Removes the descriptive name for the holiday on the specified month and day.

Table 85 Authority Group Commands Summary (continued)

COMMAND	DESCRIPTION
office-hour apply {default|from-system|to-extension}	Applies the authority group's office hour policy.
exit	Leaves the sub-command mode.
show pbx authority-group-list	Lists the configured authority groups.
show pbx authority-group	Shows all of the authority groups and group IDs and descriptions.
show pbx authority-group *pbx_grp_name*	Shows the specified authority group's configuration.
show pbx authority-group-extension	Shows which extensions belong to each authority group.
show pbx authority-group-extension *pbx_grp_name*	Lists the specified authority group's extensions.
show pbx authority-group *pbx_grp_name* office-hour [|dow|dow-time|holiday]	Displays the specified authority group's office hours configuration. Specify dow to show by the days of the week, dow-time to show by the days of the week and times, or holiday to see the holidays.

18.10.2 Authority Group Command Examples

Here are some examples of configuring authority group settings.

18.10.2.1 Configuring an Authority Group by Commands Example

The following example creates an authority group named AG1 and configures it with the following settings:

- Group ID: 1
- Description: "this is my 1st authority group"
- Call access code:12345
- Office hours for 9:00-17:00 on Mondays
- Holiday on 01/01
- Applies the system office hour configuration to the authority group

```
Router# configure terminal
Router(config)# pbx authority-group AG1
Router(auth-grp)# group-id 1
Router(auth-grp)# description this is my 1st authority group
Router(auth-grp)# cac 12345
Router(auth-grp)# no office-hour dow mon
Router(auth-grp)# office-hour dow mon time 09:00-17:00
Router(auth-grp)# office-hour holiday 01/01
Router(auth-grp)# office-hour apply from-system
Router(auth-grp)# exit
Router(config)# exit
Router#
```

18.10.2.2 Show Authority Group Settings Command Example

The following example displays the settings for the AG1 authority group.

```
Router# configure terminal
Router(config)# show pbx authority-group AG1
Authority Group Name: AG1
Group ID: 1
Description: this is my 1st authority group
CAC Code:12345
```

18.10.3 Authority TAPI Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 86 Input Values for Authority TAPI Commands

LABEL	DESCRIPTION
exten_num	The extension number (3-10 digits).
tapi_user_name	The user name of the TAPI server account. You must use one to 30 alphanumeric and -_@. characters. Spaces are not allowed.
tapi_password	The password of the TAPI server account. You must use one to 63 printable ASCII characters. Spaces are not allowed.

The following table describes the commands for configuring the TAPI settings on the ISG50. You must use the `configure terminal` command to enter the configuration mode before you can use the configuration commands.

Table 87 Authority TAPI Commands Summary

COMMAND	DESCRIPTION
`no pbx authority-tapi`	Disables TAPI on the ISG50.
`no pbx authority-tapi server1 username` *tapi_user_name*	Removes the first TAPI server account settings.
`no pbx authority-tapi server2 username` *tapi_user_name*	Removes the second TAPI server account settings.
`pbx authority-tapi`	Enables TAPI on the ISG50. You should register the ISG50 and activate the TAPI service first.
`pbx authority-tapi {client|server}`	Sets the extension number(s) that can be managed by a TAPI server or TAPI client and enters the sub-command mode for configuring it.
`no tapi-line` *exten_num*	Sets the extension number to not be managed by a TAPI server or client.
`tapi-line` *exten_num*	Allows the extension number to be managed by a TAPI server or client.
`exit`	Leaves the sub-command mode.
`pbx authority-tapi server1 username` *tapi_user_name* `password` *tapi_password*	Sets the user name and password for the first TAPI server account.

Table 87 Authority TAPI Commands Summary (continued)

COMMAND	DESCRIPTION
pbx authority-tapi server2 username *tapi_user_name* password *tapi_password*	Sets the user name and password for the second TAPI server account.
show pbx authority-tapi {server|client} tapi-line	Lists all the TAPI lines that can be managed and monitored by a TAPI server or TAPI client.
show pbx authority-tapi status	Shows whether TAPI is enabled on the ISG50 and the TAPI server account information.

18.10.4 Authority TAPI Command Examples

Here are some examples of configuring authority TAPI settings.

18.10.4.1 Configuring a TAPI Server Account by Commands Example

The following example creates a TAPI server account with the following settings:

- User name: tapiserver1
- Password: qwerty12345

```
Router# configure terminal
Router(config)# pbx authority-tapi server1 username tapiserver1 password
qwerty12345
Router(config)# exit
Router#
```

18.10.4.2 Configuring TAPI lines for TAPI Server Example

The following example allows a TAPI server to manage extensions 2001, 2002 and 2003 via a TAPPI connection to the ISG50.

```
Router# configure terminal
Router(config)# pbx authority-tapi server
Router(server tapi-line)# tapi-line 2001
Router(server tapi-line)# tapi-line 2002
Router(server tapi-line)# tapi-line 2003
Router(server tapi-line)# exit
Router(config)# show pbx authority-tapi server tapi-line
Index    Extension
================================================================================
1        2001
2        2002
3        2003
Router(config)# exit
Router#
```

18.10.5 PBX Extension Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 88 Input Values for PBX Extension Commands

LABEL	DESCRIPTION
pbx_exten_num	The extension number (3-10 digits).
pbx_grp_name	The name of the authority group. Use 0-29 alphanumeric characters.
description	A description using 0-62 alphanumeric characters (A-Z, a-z, 0-9) and spaces.
phone_num	A phone number.
pbx_codec	One of the following codecs: {ulaw|alaw|g723|g729|g726|h263|h261|g722|h264|mpeg4}

The following table describes the commands for creating, editing and removing SIP or FXS extensions. Use the `enable` or `configure terminal` command to be able to use the show commands. You must use the `configure terminal` command to enter the configuration mode before you can use the configuration commands.

Table 89 PBX Extension Commands Summary

COMMAND	DESCRIPTION
`no pbx extension` *pbx_exten_num*	Deletes the specified SIP or FXS extension.
`pbx extension` *pbx_exten_num*	Creates the specified SIP or FXS extension and enters the sub-command mode for configuring it.
`group` *pbx_grp_name*	Assigns the extension to the specified authority group.
`pin-code` *pbx_exten_num*	Configures the extension's PIN-code.
`auth-name` *auth-name*	Configures the extension's authentication user name.
`auth-password` *auth-password*	Configures the extension's authentication password.
`department department`	Configures the department the extension's user belongs to.
`first-name` *name*	Configures the first name of the extension's user.
`no first-name`	Removes the extension's first name configuration.
`last-name` *name*	Configures the last name of the extension's user.
`no last-name`	Removes the extension's last name configuration.
`description` *description*	Configures a description for the extension.
`no description`	Removes the extension's description.
`dtmf {rfc2833|inband|info}`	Sets how to handle the tones made by pressing the buttons on this extension's phone. Use the same mode as your VoIP service provider. • `rfc2833` - Follow the RFC 2833 standard and send the DTMF tones in RTP packets. • `inband` - Send the DTMF tones in the voice data stream. • `info` - Send the DTMF tones in SIP messages.
`[no] mwi`	Turns the Message Waiting Indicator on or off for the extension.
`[no] group-pickup`	Turns group pickup on or off for the extension.

Table 89 PBX Extension Commands Summary (continued)

COMMAND	DESCRIPTION
[no] call-waiting	Turns call-waiting on or off for the extension.
[no] call-forward blind	Turns blind forwarding on or off for the extension.
call-forward blind voice-mail	Configures blind forwarding to voice mail.
call-forward blind extension *pbx_exten_num*	Configures blind forwarding to the specified extension.
no call-forward blind extension	Removes the configuration for blind forwarding to an extension.
[no] call-forward busy	Turns busy forwarding on or off for the extension.
call-forward busy voice-mail	Configures busy forwarding to voice mail.
call-forward busy extension *pbx_exten_num*	Configures busy forwarding to the specified extension.
no call-forward busy extension	Removes the configuration for busy forwarding to an extension.
[no] call-forward noanswer	Turns no-answer forwarding on or off for the extension.
call-forward noanswer voice-mail	Configures no-answer forwarding to voice mail.
call-forward noanswer extension *pbx_exten_num*	Configures no-answer forwarding to the specified extension.
no call-forward noanswer extension *pbx_exten_num*	Removes the configuration for no-answer forwarding to the specified extension.
no call-forward noanswer extension all	Removes all of the extension's no-answer forwarding configuration.
call-forward noanswer extension move *pbx_exten_num* to *pbx_exten_num*	Changes the sequence of the extension in the extension's find-me list. The number you enter first moves to the position of the number you list second, which gets pushed down one.
[no] call-forward night-service	Turns night-service call forwarding on or off for the extension.
call-forward night-service voice-mail	Configures night-service call forwarding to voice mail.
call-forward night-service extension *pbx_exten_num*	Configures night-service call forwarding to the specified extension.
no call-forward night-service extension	Removes the configuration for night-service forwarding to an extension.
call-forward follow-me extension *pbx_exten_num*	Configures follow-me forwarding for the specified extension.
[no] office-hour dow {sun|mon|tue|wed|thu|fri|sat}	Enables or disables office hour configuration for the extension on the specified day of the week.
[no] office-hour dow {sun|mon|tue|wed|thu|fri|sat} time <0..23>:<0..59>-<0..23>:<0..59>	Sets the extension's office hours for the specified day of the week to the specified time period.
no office-hour dow {sun|mon|tue|wed|thu|fri|sat} time all	Removes all of the authority group's office hours for the specified day of the week.
[no] office-hour holiday <01-12>/<01-31>	Sets the specified month and day as a holiday for the authority group.
no office-hour holiday all	Removes all of the authority group's holidays.
office-hour holiday <01-12>/<01-31> description *pbx_description*	Adds a descriptive name for the holiday on the specified month and day.

Table 89 PBX Extension Commands Summary (continued)

COMMAND	DESCRIPTION
no office-hour holiday <01-12>/<01-31> description	Removes the descriptive name for the holiday on the specified month and day.
[no] office-hour user-defined	Sets whether to apply user-defined office hour configuration or the authority group's office hour configuration.
show office-hour	Displays the extension's office-hour configuration.
[no] dnd	Enables or disables the Do Not Disturb (DND) feature for the extension.
dnd voice-mail	Forwards calls to voice mail when the user activates DND.
[no] dnd white-list extension *phone_num*	Adds or removes a DND white list number that can still call this extension when it has Do Not Disturb activated.
no dnd white-list extension all	Removes all DND white list entries.
show dnd	Displays the extension's DND configuration.
[no] black-list	Enables or disables the black-list feature.
[no] black-list extension *phone_num*	Adds or removes a black list number that cannot call this extension when the black-list feature is activated.
no black-list extension all	Removes all black list entries.
show black-list	Displays the extension's black list configuration.
[no] block no-caller-id	Enables or disables the blocking of incoming calls without caller ID.
voice-mail address *e-mail*	Sets the e-mail address for sending the extension's voice messages.
no voice-mail address	Removes the e-mail address configured for sending the extension's voice messages.
[no] voice-mail attached-voice-msg	Enables or disables the emailing of voice messages.
[no] voice-mail delete-voice-msg	Enables or disables the deleting of voice mail messages stored on the ISG50 after they have been emailed.
show voice-mail	Shows the extension's voice mail configuration.
[no] codec *pbx_codec*	Add a codec to (or remove a codec from) the list of codecs the extension can use.
codec default	Set the extension to only use the default codecs.
codec move *pbx_codec* to *pbx_codec*	Changes the sequence of the codec in the extension's list. The number you enter first moves to the position of the number you list second, which gets pushed down one.
show codec	Shows the extension's codec list.
mobile-extension option {manually|force-enable}	Sets whether to allow authority group members to turn this feature on and off using feature codes (manually) or override the authority group member settings and require all calls to use this feature (force-enable).
mobile-extension status [0|1]	Turns the mobile extension feature on (1) or off (0) for this extension.
mobile-extension extension *pbx_exten_num*	Sets the number to which to forward any incoming calls to this extension.

Table 89 PBX Extension Commands Summary (continued)

COMMAND	DESCRIPTION
`no mobile-extension extension`	Removes the configuration for the number to which to forward any incoming calls to this extension.
`mobile-extension dial-rule` *`dial_rule`*	Specifies the dial rule to apply to the mobile extension. Dial rules correspond to the Least Cost Routing rules. *`dial_rule`*: (0-29) alphanumeric or _
`no mobile-extension dial-rule`	Removes the configured mobile extension dial rule.
`show mobile-extension`	Displays the extension's mobile extension settings.
`exit`	Leaves the sub-command mode.
`show pbx extension available-fxs`	Displays the FXS interfaces available for configuration.
`show pbx extension` *`pbx_exten_num`*	Displays the configuration for the specified extension.
`show pbx extension` *`pbx_exten_num`* `basic`	Displays the specified extension's basic information.
`show pbx extension` *`pbx_exten_num`* `black-list`	Displays the specified extension's black list configuration.
`show pbx extension` *`pbx_exten_num`* `dnd`	Displays the specified extension's Do Not Disturb configuration.
`show pbx extension` *`pbx_exten_num`* `codec`	Displays the specified extension's codec configuration.
`show pbx extension` *`pbx_exten_num`* `office-hour dow`	Displays the specified extension's office hour configuration for each day of the week.
`show pbx extension` *`pbx_exten_num`* `office-hour holiday`	Displays the specified extension's holiday configuration.
`show pbx extension` *`pbx_exten_num`* `call-forward noanswer`	Displays the specified extension's no-answer call forwarding configuration.

18.10.6 PBX Extension Command Examples

Here are some examples of configuring PBX extension settings.

18.10.6.1 Creating a SIP Extension Example

The following example creates SIP extension 1000.

```
Router# configure terminal
Router(config)# pbx extension 1000
Router(extension)# exit
Router(config)# exit
Router#
```

18.10.6.2 Configuring an FXS Extension Example

The following example creates FXS extension 1111.

```
Router# configure terminal
Router(config)# pbx fxs extension 1111
Router(extension)# exit
Router(config)# exit
Router#
```

18.10.6.3 Removing a SIP Extension Example

The following example removes SIP extension 1000.

```
Router# configure terminal
Router(config)# no pbx extension 1000
Router(config)# exit
Router#
```

18.10.6.4 Assigning an Extension to an Authority Group Example

The following example adds SIP extension 1000 to authority group AG1.

```
Router# configure terminal
Router(config)# pbx extension 1000
Router(extension)# group AG1
Router(extension)# exit
Router(config)# exit
Router#
```

18.10.6.5 PIN Code for an Extension Example

The following example sets PIN code 12345 for SIP extension 1000.

```
Router# configure terminal
Router(config)# pbx extension 1000
Router(extension)# pin-code 12345
Router(extension)# exit
Router(config)# exit
Router#
```

18.10.6.6 Authentication Name and Password for an Extension Example

The following example sets authentication name “Name1000” and authentication password “Passwd1000” for SIP extension 1000.

```
Router# configure terminal
Router(config)# configure terminal
Router(config)# pbx extension 1000
Router(extension)# auth-name Name1000
Router(extension)# auth-password Passwd1000
Router(extension)# exit
Router(config)# exit
Router#
```

18.10.6.7 Configuring Information for an Extension Example

The following example sets the department, first name, last name, and description for SIP extension 1000.

```
Router# configure terminal
Router(config)# pbx extension 1000
Router(extension)# department SDD2
Router(extension)# first-name Dean
Router(extension)# last-name Hsiao
Router(extension)# description Happy
Router(extension)# exit
Router(config)# exit
Router#
```

18.10.6.8 DTMF Setting for an Extension Example

The following example sets the DTMF mode to rfc2833 for SIP extension 1000.

```
Router# configure terminal
Router(config)# pbx extension 1000
Router(extension)# dtmf rfc2833
Router(extension)# exit
Router(config)# exit
Router#
```

18.10.6.9 MWI, Group Pickup and Call Waiting Settings for an Extension Examples

The following example enables MWI, Group Pickup, and Call Waiting for SIP extension 1000.

```
Router# configure terminal
Router(config)# pbx extension 1000
Router(extension)# mwi
Router(extension)# group-pickup
Router(extension)# call-waiting
Router(extension)# exit
Router(config)# exit
Router#
```

The following example disables MWI, Group Pickup, and Call Waiting for SIP extension 1000.

```
Router# configure terminal
Router(config)# pbx extension 1000
Router(extension)# no mwi
Router(extension)# no group-pickup
Router(extension)# no call-waiting
Router(extension)# exit
Router(config)# exit
Router#
```

18.10.6.10 Blind Call Forwarding Setting for an Extension Example

The following example activates blind call forwarding to extension 1001 for SIP extension 1000.

```
Router# configure terminal
Router(config)# pbx extension 1000
Router(extension)# call-forward blind
Router(extension)# call-forward blind extension 1001
Router(extension)# exit
Router(config)# exit
Router#
```

18.10.6.11 Blind Call Forwarding to Voice Mail Setting for an Extension Example

The following example configures blind call forwarding to forward to voice mail for SIP extension 1000.

```
Router# configure terminal
Router(config)# pbx extension 1000
Router(extension)# call-forward blind voice-mail
Router(extension)# exit
Router(config)# exit
Router#
```

18.10.6.12 No Blind Call Forwarding for an Extension Example

The following example disables blind call forwarding for SIP extension 1000 and removes the forwarding extension number.

```
Router# configure terminal
Router(config)# pbx extension 1000
Router(extension)# no call-forward blind
Router(extension)# no call-forward blind extension
Router(extension)# exit
Router(config)# exit
Router#
```

18.10.6.13 Busy Forwarding Setting for an Extension Example

The following example activates busy call forwarding to extension 1001 for SIP extension 1000.

```
Router# configure terminal
Router(config)# pbx extension 1000
Router(extension)# call-forward busy
Router(extension)# call-forward busy extension 1001
Router(extension)# exit
Router(config)# exit
Router#
```

18.10.6.14 Busy Call Forwarding to Voice Mail Setting for an Extension Example

The following example configures busy call forwarding to forward to voice mail for SIP extension 1000.

```
Router# configure terminal
Router(config)# pbx extension 1000
Router(extension)# call-forward busy voice-mail
Router(extension)# exit
Router(config)# exit
Router#
```

18.10.6.15 Removing Busy Call Forwarding for an Extension Example

The following example disables busy call forwarding for SIP extension 1000 and removes the forwarding extension number.

```
Router# configure terminal
Router(config)# pbx extension 1000
Router(extension)# no call-forward busy
Router(extension)# no call-forward busy extension
Router(extension)# exit
Router(config)# exit
Router#
```

18.10.6.16 No-answer Forwarding Setting for an Extension Example

The following example activates no answer call forwarding for SIP extension 1000 and adds extensions 1001 and 1002 in the extension's find-me list.

```
Router# configure terminal
Router(config)# pbx extension 1000
Router(extension)# call-forward noanswer
Router(extension)# call-forward noanswer extension 1001
Router(extension)# call-forward noanswer extension 1002
Router(extension)# exit
Router(config)# exit
Router#
```

18.10.6.17 No-answer Forwarding to Voice Mail Setting for an Extension Example

The following example configures no answer call forwarding to forward to voice mail for SIP extension 1000.

```
Router# configure terminal
Router(config)# pbx extension 1000
Router(extension)# call-forward noanswer voice-mail
Router(extension)# exit
Router(config)# exit
Router#
```

18.10.6.18 Disable No-answer Call Forwarding for an Extension Example

The following example disables no answer call forwarding for SIP extension 1000 and removes the forwarding extension number 1001 from the find-me list.

```
Router# configure terminal
Router(config)# pbx extension 1000
Router(extension)# no call-forward noanswer
Router(extension)# no call-forward noanswer extension 1001
Router(extension)# exit
Router(config)# exit
Router#
```

18.10.6.19 Remove Find-me List From an Extension Example

The following example removes all no-answer call forwarding extension numbers from SIP extension 1000's find-me list.

```
Router# configure terminal
Router(config)# pbx extension 1000
Router(extension)# no call-forward noanswer extension all
Router(extension)# exit
Router(config)# exit
Router#
```

18.10.6.20 No-answer Forwarding Find-me List Sequence for an Extension Example

The following example changes the sequence of SIP extension 1000's find-me list.

```
Router(config)# pbx extension 1000
Router(extension)# call-forward noanswer extension 1001
Router(extension)# call-forward noanswer extension 1002
Router(extension)# show call-forward noanswer
No Answer: 1000
  Forward: disable
Sequence Number
================================================================================
1        1001
2        1002
Router(extension)# call-forward noanswer extension move 1002 to 1001
Router(extension)# show call-forward noanswer
No Answer: 1000
  Forward: disable
Sequence Number
================================================================================
1        1002
2        1001
Router(extension)# exit
Router(config)# exit
Router#
```

18.10.6.21 After Office Hour Call Forwarding to an Extension Example

The following example enables after office hour call forwarding from SIP extension 1000 to extension 1001.

```
Router# configure terminal
Router(config)# pbx extension 1000
Router(extension)# call-forward night-service
Router(extension)# call-forward night-service extension 1001
Router(extension)# exit
Router(config)# exit
Router#
```

18.10.6.22 After Office Hour Forwarding to Voice Mail Setting for an Extension Example

The following example configures after office hour call forwarding to forward to voice mail for SIP extension 1000.

```
Router# configure terminal
Router(config)# pbx extension 1000
Router(extension)# call-forward night-service voice-mail
Router(extension)# exit
Router(config)# exit
Router#
```

18.10.6.23 Removing After Office Hour Forwarding for an Extension Example

The following example disables after office hour call forwarding for SIP extension 1000 and removes the forwarding extension number.

```
Router# configure terminal
Router(config)# pbx extension 1000
Router(extension)# no call-forward night-service
Router(extension)# no call-forward night-service extension
Router(extension)# exit
Router(config)# exit
Router#
```

18.10.6.24 Assign a Follow-me Forwarding Extension

The following example assigns extension number 1001 as a follow-me call forwarding extension for extension 1000 (which also activates follow-me call forwarding for extension 1000).

```
Router# configure terminal
Router(config)# pbx extension 1000
Router(extension)# call-forward follow-me extension 1001
Router(extension)# exit
Router(config)# exit
Router#
```

18.10.6.25 Remove a Follow-me Forwarding Extension

The following example removes extension 1000's follow-me call forwarding extension configuration (which also disables follow-me call forwarding for extension 1000).

```
Router# configure terminal
Router(config)# pbx extension 1000
Router(extension)# no call-forward follow-me extension
Router(extension)# exit
Router(config)# exit
Router#
```

18.10.6.26 Enable Office Hours for an Extension on a Day of the Week

The following example enables office hours for extension 1000 on Mondays.

```
Router# configure terminal
Router(config)# pbx extension 1000
Router(extension)# office-hour dow mon
Router(extension)# exit
Router(config)# exit
Router#
```

18.10.6.27 Disable Office Hours for an Extension on a Day of the Week

The following example disables office hours for extension 1000 on Mondays.

```
Router# configure terminal
Router(config)# pbx extension 1000
Router(extension)# no office-hour dow mon
Router(extension)# exit
Router(config)# exit
Router#
```

18.10.6.28 Configure the Office Hours Time Range for an Extension on a Day of the Week

The following example sets office hours to be from 8 A.M. to 5:30 P.M. for extension 1000 on Mondays.

```
Router# configure terminal
Router(config)# pbx extension 1000
Router(extension)# office-hour dow mon time 08:00-17:30
Router(extension)# exit
Router(config)# exit
Router#
```

18.10.6.29 Remove an Office Hours Time Range for an Extension on a Day of the Week

The following example removes the 8 A.M. to 5 P.M. office hours configured for extension 1000 on Mondays.

```
Router# configure terminal
Router(config)# pbx extension 1000
Router(extension)# no office-hour dow mon time 08:00-17:30
Router(extension)# exit
Router(config)# exit
Router#
```

18.10.6.30 Remove the Office Hours Time Range Configuration for an Extension on a Day of the Week

The following example removes office hours configured for extension 1000 on Mondays.

```
Router# configure terminal
Router(config)# pbx extension 1000
Router(extension)# no office-hour dow mon time all
Router(extension)# exit
Router(config)# exit
Router#
```

18.10.6.31 Set a Holiday on an Extension

The following example sets January 1 to be a holiday for extension 1000.

```
Router# configure terminal
Router(config)# pbx extension 1000
Router(extension)# office-hour holiday 01/01
Router(extension)# exit
Router(config)# exit
Router#
```

18.10.6.32 Remove a Holiday on an Extension

The following example removes January 1 from extension 1000's holiday list.

```
Router# configure terminal
Router(config)# pbx extension 1000
Router(extension)# no office-hour holiday 01/01
Router(extension)# exit
Router(config)# exit
Router#
```

18.10.6.33 Remove All of an Extension's Holidays

The following example removes all holidays from extension 1000's holiday list.

```
Router# configure terminal
Router(config)# pbx extension 1000
Router(extension)# no office-hour holiday all
Router(extension)# exit
Router(config)# exit
Router#
```

18.10.6.34 Set a Holiday With a Description on an Extension

The following example sets January 1 to be a holiday with the description “1st holiday” for extension 1000.

```
Router# configure terminal
Router(config)# pbx extension 1000
Router(extension)# office-hour holiday 01/01 description 1st holiday
Router(extension)# exit
Router(config)# exit
Router#
```

18.10.6.35 Remove a Holiday Description on an Extension

The following example removes the description for the January 1st holiday on extension 1000.

```
Router# configure terminal
Router(config)# pbx extension 1000
Router(extension)# no office-hour holiday 01/01 description
Router(extension)# exit
Router(config)# exit
Router#
```

18.10.6.36 Apply User-defined Office Hour Configuration on an Extension

The following example enables user-defined office hour configuration for extension 1000.

```
Router# configure terminal
Router(config)# pbx extension 1000
Router(extension)# office-hour user-defined
Router(extension)# exit
Router(config)# exit
Router#
```

18.10.6.37 Apply Authority Group Office Hour Configuration on an Extension

The following example disables user-defined office hour configuration for extension 1000 which means the ISG50 applies the office hours configured for the authority group to which the extension belongs.

```
Router# configure terminal
Router(config)# pbx extension 1000
Router(extension)# no office-hour user-defined
Router(extension)# exit
Router(config)# exit
Router#
```

18.10.6.38 Show an Extension's Office Hour Configuration

The following example displays the office hour configuration for extension 1000.

```
Router# configure terminal
Router(config)# pbx extension 1000
Router(extension)# show office-hour
Office Hour: User defined
Sun: enable
Mon: enable
Tue: enable
Wed: enable
Thu: enable
Fri: enable
Sat: enable
Sequence Sun Time
================================================================================
Sequence mon Time
================================================================================
1        08:00-17:30
Sequence Tue Time
================================================================================
Sequence Wed Time
================================================================================
Sequence Thu Time
================================================================================
Sequence Fri Time
================================================================================
Sequence Sat Time
================================================================================
Date  Description
================================================================================
Router(extension)# exit
Router(config)#
```

18.10.6.39 Configure DND for an Extension

The following example turns on the DND (Do Not Disturb) feature on extension 1000 and adds the number patterns 2XXX (which covers extensions 2000-2999) and 33XX (which covers extensions 3300-3399) to the extension's DND white list.

```
Router# configure terminal
Router(config)# pbx extension 1000
Router(extension)# dnd
Router(extension)# dnd white-list extension 2XXX
Router(extension)# dnd white-list extension 33XX
Router(extension)# show dnd
DND: 1000
  DND: enable
Sequence DND Number
================================================================================
1        2XXX
2        33XX
Router(extension)# exit
Router(config)# exit
Router#
```

18.10.6.40 Disable DND for an Extension and Remove a White List Entry

The following example turns off the DND (Do Not Disturb) feature on extension 1000 and removes the 2XXX number pattern from the extension's DND white list.

```
Router# configure terminal
Router(config)# pbx extension 1000
Router(extension)# no dnd
Router(extension)# no dnd white-list extension 2XXX
Router(extension)# exit
Router(config)# exit
Router#
```

18.10.6.41 Remove All of an Extension's White List Entries

The following example removes all of the number patterns from extension 1000's DND white list.

```
Router# configure terminal
Router(config)# pbx extension 1000
Router(extension)# no dnd white-list extension all
Router(extension)# exit
Router(config)# exit
Router#
```

18.10.6.42 Configure Black List for an Extension

The following example turns on the black-list feature on extension 1000 and adds the number patterns 2XXX (which covers extensions 2000-2999) and 33XX (which covers extensions 3300-3399) to the extension's black list.

```
Router# configure terminal
Router(config)# pbx extension 1000
Router(extension)# black-list
Router(extension)# black-list extension 2XXX
Router(extension)# black-list extension 33XX
Router(extension)# show black-list
Black List: 1000
  Black list: enable
Sequence Number
================================================================================
1        2XXX
2        33XX
Router(extension)# exit
Router(config)# exit
Router#
```

18.10.6.43 Disable Black List for an Extension and Remove a Black List Entry

The following example turns off the black-list feature on extension 1000 and removes the 2XXX number pattern from the extension's black list.

```
Router# configure terminal
Router(config)# pbx extension 1000
Router(extension)# no black-list
Router(extension)# no black-list extension 2XXX
Router(extension)# exit
Router(config)# exit
Router#
```

18.10.6.44 Remove All of an Extension's Black List Entries

The following example removes all of the number patterns from extension 1000's black list.

```
Router# configure terminal
Router(config)# pbx extension 1000
Router(extension)# no black-list extension all
Router(extension)# exit
Router(config)# exit
Router#
```

18.10.6.45 Enable Blocking of Unidentified Calls for an Extension

The following example blocks calls without caller ID from going to extension 1000.

```
Router# configure terminal
Router(config)# pbx extension 1000
Router(extension)# block no-caller-id
Router(extension)# exit
Router(config)# exit
Router#
```

18.10.6.46 Disable Blocking of Unidentified Calls for an Extension

The following example allows calls without caller ID to go to extension 1000.

```
Router# configure terminal
Router(config)# pbx extension 1000
Router(extension)# no block no-caller-id
Router(extension)# exit
Router(config)# exit
Router#
```

18.10.6.47 Voice Mail Settings for an Extension

The following example sets the e-mail address to which to send extension 1000's voice mail, enables attaching of voice messages to the e-mails, and enables the deleting of voice mail messages stored on the ISG50 after they have been emailed.

```
Router# configure terminal
Router(config)# pbx extension 1000
Router(extension)# voice-mail address mailbox@mail.server
Router(extension)# voice-mail attached-voice-msg
Router(extension)# voice-mail delete-voice-msg
Router(extension)# show voice-mail
Voice Mail Configuration:
  E-mail address: mailbox@mail.server
  Attached option: enable
  Deleted option: enable
Router(extension)# exit
Router(config)# exit
Router#
```

18.10.6.48 Configure Codec Settings for an Extension

The following example adds the G.723 codec for extension 1000.

```
Router# configure terminal
Router(config)# pbx extension 1000
Router(extension)# codec g723
Router(extension)# exit
Router(config)# exit
Router#
```

18.10.6.49 Restore Default Codec Settings for an Extension

The following example removes all user-configured codec configuration for extension 1000 and restores the default value (G.729, G.711 ulaw, and G.711 alaw.

```
Router# configure terminal
Router(config)# pbx extension 1000
Router(extension)# no codec all
Router(extension)# show codec
Sequence CODEC
================================================================================
Router(extension)# codec default
Router(extension)# show codec
Sequence CODEC
================================================================================
1        g729
2        ulaw
3        alaw
Router(extension)# exit
Router(config)# exit
Router#
```

18.10.6.50 Change the Sequence of Codecs an Extension Uses

The following example has the ISG50 try the G.711 alaw codec for extension 1000's calls before trying the G.729 codec.

```
Router# configure terminal
Router(config)# pbx extension 1000
Router(extension)# show codec
Sequence CODEC
================================================================================
1        g729
2        ulaw
3        alaw
Router(extension)# codec move alaw to g729
Router(extension)# show codec
Sequence CODEC
================================================================================
1        alaw
2        g729
3        ulaw
Router(extension)# exit
Router(config)# exit
Router#
```

18.10.6.51 Mobile Extension Settings for an Extension

The following example sets the mobile extension 10001000 and dial rule SIPTrunk1 for extension 1000.

```
Router# configure terminal
Router(config)# pbx extension-mobile 1000
Router(extension-mobile)# mobile-extension extension 10001000
Router(extension-mobile)# mobile-extension dial-rule SIPTrunk1
Router(extension-mobile)# show mobile-extension
Mobile Extension:
  Option: manually
  Number: 10001000
  Dial rule: SIPTrunk1
Router(extension-mobile)# exit
Router(config)# exit
Router#
```

18.10.6.52 Show the FXS Interface Available for Configuration

The following example displays the FXS interface available for configuration.

```
Router# configure terminal
Router(config)# show pbx extension available-fxs
Sequence Interface
================================================================================
1        Slot A, Port 5
Router(config)# exit
Router#
```

18.10.6.53 Show an Extension’s Configuration

The following example displays extension 1000’s configuration.

```
Router# configure terminal
Router(config)# show pbx extension 1000
Extension: 1000
Group: AG1
Peer-Type: SIP
Slot:
Port:
Auth. Password: 1000
Auth. Name: 1000
DTMF: default
PIN: 1000
Call waiting: enable
Group Pickup: enable
MWI: enable
First Name:
Last Name:
Department:
Description:
Blind Forward: enable
Blind Forward Extension: 1001
Busy Forward: disable
Busy Forward Extension:
No Answer Forward: disable
Night Service Forward: disable
Night Service Forward Extension:
DND: enable
Black List: enable
Block Call: enable
Mobile Option: manually
Mobile Number: 10001000
Mobile Dial Rule: SIPTrunk1
VM E-mail: mailbox@mail.server
VM Attached: enable
VM Delete: enable
Router(config)# exit
Router#
```

18.10.6.54 Show an Extension's Basic Settings

The following example displays extension 1000's key configuration.

```
Router# configure terminal
Router(config)# show pbx extension 1000 basic
Extension: 1000
Group: AG1
Peer-Type: sip
Auth. Password: 1000
Auth. Name: 1000
DTMF: default
PIN: 1000
Call waiting: enable
Group Pickup: enable
MWI: enable
First Name:
Last name:
Department:
Router(config)# exit
Router#
```

18.11 Group Access Code Commands

This section covers how to enable or disable the call access code feature.

The following table describes the commands for enabling or disabling the call access code feature. Use the `enable` or `configure terminal` command to be able to use the show commands. You must use the `configure terminal` command to enter the configuration mode before you can use the configuration commands.

Table 90 Group Access Code Commands Summary

COMMAND	DESCRIPTION
`show pbx cac`	Displays the call access code feature's configuration.
`[no] pbx cac activate`	Enables or disables the call access code feature.

18.11.1 Group Access Code Command Examples

Here are some examples of configuring and displaying call access code settings.

18.11.1.1 Displaying Call Access Code Settings

The following example displays the call access code feature's configuration.

```
Router> show pbx cac
cac_enable     : enable
group_name           access_code
=====================================================================
ag001        12345
```

18.11.1.2 Enabling Call Access Code Settings

The following example turns on the call access code feature.

```
Router> configure terminal
Router(config)# pbx cac activate
```

18.12 Click To Talk Commands

This section covers how to configure Click To Talk (CTT).

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 91 Input Values for Click To Talk Commands

LABEL	DESCRIPTION
ctt_grp_name	The name of the CTT group. Use 0-29 alphanumeric characters and the underscore.
description	A description using 0-62 alphanumeric characters (A-Z, a-z, 0-9) and spaces.
ctt_extension	The name of a CTT extension. Use 0-19 alphanumeric characters and the underscore.
ctt_dialnumber	The extension number associated with this CTT extension name (1-20 digits).

The following table describes the commands for configuring CTT. Use the `enable` or `configure terminal` command to be able to use the show commands. You must use the `configure terminal` command to enter the configuration mode before you can use the configuration commands.

Table 92 Click To Talk Commands Summary

COMMAND	DESCRIPTION
`no pbx clicktotalk-group` *ctt_grp_name*	Removes the specified CTT group.
`pbx clicktotalk-group` *ctt_grp_name*	Creates the specified CTT group and enters the sub-command mode for configuring it.
`[no] descrption` *description*	Adds or removes a description for the CTT group.
`exten` *ctt_extension* `dialnum` *ctt_dialnumber* `server {`*ipv4*`|`*hostname*`}`	Adds a CTT extension to the CTT group including the address of the SIP server it uses.
`no exten` *ctt_extension*	Deletes the specified CTT extension.
`exten` *ctt_extension* `description` *description*	Adds a description for the specified CTT extension.

Table 92 Click To Talk Commands Summary (continued)

COMMAND	DESCRIPTION
no exten *ctt_extension* description	Removes the description for the specified CTT extension.
exit	Leaves the sub-command mode.
show pbx clicktotalk-group [*ctt_grp_name*]	Displays information about the specified CTT group or all of them.
show pbx clicktotalk-group *ctt_grp_name* exten	Shows all of the specified CTT group's extensions.
show pbx clicktotalk-group *ctt_grp_name* exten *ctt_extension* samplecode	Shows sample code for embedding the ZyXEL web-based IP phone client in a web page for calling the specified CTT group extension.

18.12.1 Click To Talk Command Examples

Here are some examples of configuring and displaying Click To Talk group and extension settings.

18.12.1.1 Confguring a CTT Group and Adding Extensions

The following example sets up CTT group CTT1 and adds Jason and Alex extensions.

```
Router> configure terminal
Router(config)# pbx clicktotalk-group CTT1
Router(config-cttgroup-CTT1)#description This is CTT group 1
Router(config-cttgroup-CTT1)# exten Jason dialnum 6701 server 192.168.125.167
Router(config-cttgroup-CTT1)# exten Jason description This is Jason’s CTT extension
Router(config-cttgroup-CTT1)# exten Alex dialnum 6702 server 192.168.125.167
Router(config-cttgroup-CTT1)# exten Alex description This is Alex’s CTT extension
Router(config-cttgroup-CTT1)# exit
Router(config)#
```

18.12.1.2 Removing an Extension from a CTT Group

The following example removes the Alex extension from CTT group CTT1.

```
Router> configure terminal
Router(config)# pbx clicktotalk-group CTT1
Router(config-cttgroup-CTT1)# no exten Alex
Router(config-cttgroup-CTT_g1)# exit
Router(config)#
```

18.12.1.3 Removing a CTT Group

The following example removes the CTT1 CTT group.

```
Router> configure terminal
Router(config)# no pbx clicktotalk-group CTT1
Router(config)#
```

18.12.1.4 Showing All of the CTT Groups

The following example shows all of the CTT groups.

```
Router> configure terminal
Router(config)# show pbx clicktotalk-group
name: CTT1
  description: This is CTT1 group
```

18.12.1.5 Showing a CTT Group's Extensions

The following example shows all of the CTT1 group's extensions.

```
Router> configure terminal
Router(config)# show pbx clicktotalk-group CTT1 exten
exten: Jason
  cttgrpname: CTT1
  dialnum: 6701
  server: 192.168.125.167
  description: It is test1 CTT extension
```

18.12.1.6 Showing the Sample Code for a CTT Group Extension

The following example shows the sample code for embedding the ZyXEL web-based IP phone client in a web page for calling the Jason CTT group extension.

```
Router> configure terminal
Router(config)# show pbx clicktotalk-group CTT1 exten Jason samplecode
samplecode: ZGlhbGluZ251bT02NzAxJnVzZXJuYW1lPWxhd3FxJnVzZXJzZWNyZXQ9bGF3cXEmc2Vy
dmVyaXBhZGRyPTE5Mi4xNjguMTI1LjE2Nzo1MDYwJmR0bWZtb2RlPTMmdXNlcmlkPWphc29uJnR1bm5lbG
lwPTE5Mi4xNjguMTI1LjE2NyZ0dW5uZWxwb3J0PTgw
```

18.13 Outbound Line Management Commands

This section covers how to show and configure outbound line management.

18.13.1 SIP Trunk and Trusted Peer Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 93 Input Values for SIP Trunk and Trusted Peer Commands

LABEL	DESCRIPTION
obtrunk_name	The name of the outbound trunk (0-29 characters). You can use alphanumeric characters and the underscore. It must start with a letter.
obtrunk_desc	A description using 0-64 alphanumeric characters (A-Z, a-z, 0-9) and underscores.

Table 93 Input Values for SIP Trunk and Trusted Peer Commands (continued)

LABEL	DESCRIPTION
obtrunk_rep_num	The 3-40 character outbound trunk representative number. Use alphanumeric characters, the @ character, periods (.), or underscores (_). You can also have a pluse (+) in front of the number.
obtrunk_st_mode	The outbound trunk session timer mode. originate: refuse:
obtrunk_callprefix	The outbound trunk caller ID prefix. This can be 0-20 alphanumeric characters (A-Z, a-z, 0-9), underscores (_), colons (:), periods (.), hyphens (-) and pluses (+).
obtrunk_username	The outbound trunk registered user name (0-20 characters). You can use alphanumeric characters and underscores (_).
obtrunk_passwd	The outbound trunk registered password (0-20 characters). You can use alphanumeric characters, underscores (_), and hpyhens (-).
obtrunk_codec	The codecs the outbound trunk can use, like: g729;g711u. Use 1-50 alphanumeric characters.
obtrunk_ddi_match	The outbound trunk DDI match part (1-53 characters). You can use 0-9, a, b, underscores (_), and hpyhens (-).
obtrunk_aa_name	The name of an outbound trunk auto attendant (1-30 characters). You can use alphanumeric characters and the underscore.

The following table describes the commands for configuring SIP trunks and trusted peers. Use the enable or configure terminal command to be able to use the show commands. You must use the configure terminal command to enter the configuration mode before you can use the configuration commands.

Table 94 SIP Trunk and Trusted Peer Commands Summary

COMMAND	DESCRIPTION
show pbx outbound-sip-trunk sip-trunk-list	Lists all of the SIP trunks.
show pbx outbound-sip-trunk *obtrunk_name*	Displays information about the specified SIP trunk.
show pbx outbound-sip-trunk sip-trunk-usedip	Shows the IP address each SIP trunk is using.
show pbx outbound-sip-trunk aa-info *obtrunk_name*	Displays the specified SIP trunk's auto-attendant information.
show pbx outbound-sip-trunk ddi-info *obtrunk_name*	Displays the specified SIP trunk's Direct Dial In information.
show pbx outbound-sip-trunk ddi-matchpart *obtrunk_name*	Displays the specified SIP trunk's Direct Dial In match part information.
show pbx outbound-trust-peer trust-peer-list	Displays the outbound trusted peer list.
show pbx outbound-trust-peer *obtrunk_name*	Displays information about the specified trusted peer list.
show pbx outbound-trust-peer trust-peer-usedip	Displays the IP addresses of the outbound trusted peers.
show pbx outbound-trust-peer *obtrunk_name*	Displays information about the specified trusted peer list.
show pbx outbound-trust-peer ddi-info *obtrunk_name*	Displays the specified trusted peer's Direct Dial In information.
show pbx outbound-trust-peer ddi-matchpart *obtrunk_name*	Displays the specified trusted peer's Direct Dial In match part information.

Table 94 SIP Trunk and Trusted Peer Commands Summary (continued)

COMMAND	DESCRIPTION
pbx outbound-sip-trunk *obtrunk_name*	Creates the specified outbound SIP trunk and enters the sub-command mode for configuring it.
description *obtrunk_desc*	Sets a description for the SIP trunk.
representative-number *obtrunk_rep_num*	Sets the representative number: The phone number that the called party sees if outgoing calls through this outbound line group don't match configured rules. associated with the SIP account for this SIP trunk. In the full SIP URI, this is the part before the @symbol.
sip-server-address {*ipv4*|*hostname*}	Set the IP address or domain name of the SIP server.
sip-server-port <1..65535>	Set the SIP server's listening port number.
register-server-address {*ipv4*|*hostname*}	Set the IP address or domain name of the SIP register server.
register-server-port <1..65535>	Set the SIP register server's listening port number.
service-domain-flag {disable|enable}	Sets whether or not to use a service domain.
service-domain {*ipv4*|*hostname*}	Specifies the SIP service domain name. In the full SIP URI, this is the part after the @ symbol.
outbound-proxy-flag {disable|enable}	Sets whether or not to use an outbound proxy server.
outbound-proxy {*ipv4*|*hostname*}	Specifies the IP address or domain name of the outbound proxy server.
outbound-proxy-port <1..65535>	Set the outbound proxy server's listening port number.
dtmf-mode {info|rfc2833|inband}	Sets how to handle the tones made by pressing the buttons on an extension's phone. Use the same mode as your VoIP service provider. • info - Send the DTMF tones in SIP messages. • rfc2833 - Follow the RFC 2833 standard and send the DTMF tones in RTP packets. • inband - Send the DTMF tones in the voice data stream.
privacy {disable|enable}	Use enable to replace the caller's name and number with "Anonymous". For example, "Anonymous"<Anonymous@172.1.1.253>.
proxy-require {*ipv4*|*hostname*}	Enter this to inform the SIP server that this device is behind a firewall or NAT device. Fill this field in only if you were given information by your SIP service provider.
channel-limit <1..128>	Specify the maximum number of SIP calls allowed to be made through this trunk connection at one time.
session-timer-mode *obtrunk_st_mode*	Set the outbound trunk session timer mode.
session-timer-minse <90..1800>	Set the minimum session expiry time in seconds. When an incoming call requests a session expiry time that is lower than this, the ISG50 uses this value instead.
session-timer-expires <90..86400>	Set the session expiry time in seconds for all phone connections on this trunk. Must be equal to or higher than the Minimum SE. Allows the ISG50 to automatically disconnect any phone calls on this trunk after a certain period of inactivity.

Table 94 SIP Trunk and Trusted Peer Commands Summary (continued)

COMMAND	DESCRIPTION
caller-id-prefix-flag {disable|enable}	Specify whether to add a prefix number in the caller ID name when you make calls through this trunk connection. The availability of this setting varies depending on the caller ID format.
caller-id-prefix *obtrunk_callprefix*	Set the outbound trunk caller ID prefix. This can be 0-20 alphanumeric characters (A-Z, a-z, 0-9), underscores (_), colons (:), periods (.), hyphens (-) and pluses (+).
caller-id {ext_ext|ext_rep|rep_rep|ext_rep_ddi|rep_rep_ddi}	Selt caller ID display format to use for the SIP trunk's outgoing calls. A caller ID consists of a call ID name (**A**), a caller ID number (**B**) and a SIP server IP address (**C**). The caller ID has the following format: "**A**"<**B@C**>. (In the following examples, we assume a company representative number is 12345678, their SIP server IP is 10.1.1.1, a caller extension number is 1111 and DDI/DID number 12345555 can map to the extension 1111.) • ext_ext: Displays the caller's extension number in **A** and **B**. For example, "1111"<1111@10.1.1.1>. • ext_rep: Displays the caller's extension number in **A** and the SIP trunk's representative number in **B**. For example, "1111"<12345678@10.1.1.1>. • rep_rep: Displays the SIP trunk's representative number in **A** and **B**. For example, "12345678"<12345678@10.1.1.1>. Select this format if you don't want callees to know the caller's extension number. • ext_rep_ddi: Displays the caller's extension number in **A** and the SIP trunk's DDI/DID mapped representative number in **B**. For example, "1111"<12345555@10.1.1.1>. If no DDI/DID is matched, displays the representative number in **B**. • rep_rep_ddi: Displays the SIP trunk's DDI/DID mapped representative number in both **A** and **B**. For example, "12345555"<12345555@10.1.1.1>. If no DDI/DID is matched, displays the representative number in **A** and **B**.
authentication-name *obtrunk_username*	Set the SIP user name the ISG50 must provide to the SIP server for authenticating this SIP trunk.
authentication-password *obtrunk_passwd*	Set the SIP password the ISG50 must provide to the SIP server for authenticating this SIP trunk.
codec *obtrunk_codec*	Specify the types of voice coder/decoder (codec) this trunk can use.
exit	Leaves the sub-command mode.
pbx outboundtrust-peer *obtrunk_name*	Creates the specified outbound trusted peer and enters the sub-command mode for configuring it.
description *obtrunk_desc*	Sets a description for the SIP trunk.
representative-number *obtrunk_rep_num*	Sets the representative number: The phone number that the called party sees if outgoing calls through this outbound line group don't match configured rules. associated with the SIP account for this SIP trunk. In the full SIP URI, this is the part before the @symbol.
sip-server-address {*ipv4*|*hostname*}	Set the IP address or domain name of the SIP server.
sip-server-port <1..65535>	Set the SIP server's listening port number.

Table 94 SIP Trunk and Trusted Peer Commands Summary (continued)

COMMAND	DESCRIPTION
service-domain-flag {disable|enable}	Sets whether or not to use a service domain.
service-domain {*ipv4*|*hostname*}	Specifies the SIP service domain name. In the full SIP URI, this is the part after the @ symbol.
outbound-proxy-flag {disable|enable}	Sets whether or not to use an outbound proxy server.
outbound-proxy {*ipv4*|*hostname*}	Specifies the IP address or domain name of the outbound proxy server.
outbound-proxy-port <1..65535>	Set the outbound proxy server's listening port number.
dtmf-mode {info|rfc2833|inband}	Sets how to handle the tones made by pressing the buttons on an extension's phone. Use the same mode as the peer uses. • info - Send the DTMF tones in SIP messages. • rfc2833 - Follow the RFC 2833 standard and send the DTMF tones in RTP packets. • inband - Send the DTMF tones in the voice data stream.
privacy {disable|enable}	Use enable to replace the caller's name and number with "Anonymous". For example, "Anonymous"<Anonymous@172.1.1.253>.
proxy-require {*ipv4*|*hostname*}	Enter this to inform the SIP server that this device is behind a firewall or NAT device. Fill this field in only if you were given information by your SIP service provider.
channel-limit <1..128>	Specify the maximum number of SIP calls allowed to be made through this trunk connection at one time.
session-timer-mode *obtrunk_st_mode*	Set the outbound trunk session timer mode.
session-timer-minse <90..1800>	Set the minimum session expiry time in seconds. When an incoming call requests a session expiry time that is lower than this, the ISG50 uses this value instead.
session-timer-expires <90..86400>	Set the session expiry time in seconds for all phone connections on this trunk. Must be equal to or higher than the Minimum SE. Allows the ISG50 to automatically disconnect any phone calls on this trunk after a certain period of inactivity.
caller-id-prefix-flag {disable|enable}	Specify whether to add a prefix number in the caller ID name when you make calls through this trunk connection. The availability of this setting varies depending on the caller ID format.
caller-id-prefix *obtrunk_callprefix*	Set the outbound trunk caller ID prefix. This can be 0-20 alphanumeric characters (A-Z, a-z, 0-9), underscores (_), colons (:), periods (.), hyphens (-) and pluses (+).

Table 94 SIP Trunk and Trusted Peer Commands Summary (continued)

COMMAND	DESCRIPTION
caller-id {ext_ext|ext_rep|rep_rep|ext_rep_ddi|rep_rep_ddi}	Selt caller ID display format to use for the SIP trunk's outgoing calls. A caller ID consists of a call ID name (**A**), a caller ID number (**B**) and a SIP server IP address (**C**). The caller ID has the following format: "**A**"<**B@C**>. (In the following examples, we assume a company representative number is 12345678, their SIP server IP is 10.1.1.1, a caller extension number is 1111 and DDI/DID number 12345555 can map to the extension 1111.) • ext_ext: Displays the caller's extension number in **A** and **B**. For example, "1111"<1111@10.1.1.1>. • ext_rep: Displays the caller's extension number in **A** and the SIP trunk's representative number in **B**. For example, "1111"<12345678@10.1.1.1>. • rep_rep: Displays the SIP trunk's representative number in **A** and **B**. For example, "12345678"<12345678@10.1.1.1>. Select this format if you don't want callees to know the caller's extension number. • ext_rep_ddi: Displays the caller's extension number in **A** and the SIP trunk's DDI/DID mapped representative number in **B**. For example, "1111"<12345555@10.1.1.1>. If no DDI/DID is matched, displays the representative number in **B**. • rep_rep_ddi: Displays the SIP trunk's DDI/DID mapped representative number in both **A** and **B**. For example, "12345555"<12345555@10.1.1.1>. If no DDI/DID is matched, displays the representative number in **A** and **B**.
codec *obtrunk_codec*	Specify the types of voice coder/decoder (codec) this trunk can use.
exit	Leaves the sub-command mode.
no pbx outbound-sip-trunk *obtrunk_name* proxy-require	Removes the specified SIP trunk's proxy require configuration.
no pbx outbound-sip-trunk *obtrunk_name*	Removes the specified SIP trunk.
no pbx outbound-trust-peer *obtrunk_name* proxy-require	Removes the specified trusted peer's proxy require configuration.
no pbx outbound-trust-peer *obtrunk_name*	Removes the specified trusted peer.
pbx outbound-sip-trunk *obtrunk_name*	Enters the sub-command mode for configuring the specified outbound SIP trunk's setting.
ddi-match-digit <0..4>	Sets the number of digits for the outbound trunk DDI match part.
ddi-mapping *obtrunk_ddi_match*	Sets the outbound trunk DDI match part.
no ddi-mapping {*obtrunk_ddi_match*|all}	Removes the specified outbound trunk DDI match part or all of the outbound trunk's DDI settings.
exit	Leaves the sub-command mode.
pbx outbound-trust-peer *obtrunk_name*	Enters the sub-command mode for configuring the specified outbound trusted peer trunk's settings.

Table 94 SIP Trunk and Trusted Peer Commands Summary (continued)

COMMAND	DESCRIPTION
ddi-flag {disable|enable}	Use enable to map a dialed number through this outbound line group to an extension or direct it to the auto attendant for incoming calls. Use disable to forward all incoming calls through this outbound line group directly to their called numbers.
ddi-match-digit <0..4>	Sets the number of digits for the outbound trunk DDI match part.
ddi-rewrite-callerid {disable|enable}	Use enable to rewrite the caller ID for calls going out through this outbound line group.
ddi-mapping *obtrunk_ddi_match*	Sets the outbound trunk DDI match part.
no ddi-mapping {*obtrunk_ddi_match*|all}	Removes the specified outbound trunk DDI match part or all of the outbound trunk's DDI settings.
exit	Leaves the sub-command mode.
pbx outbound-sip-trunk *obtrunk_name*	Enters the sub-command mode for configuring the specified outbound SIP trunk's settings.
auto-attendant {aa|fax|ext|acd} *obtrunk_aa_name*	Configures the outbound trunk's auto attendant setting. aa: specify an auto attendant to which to forward all incoming calls on this outbound line group . fax: forward all incoming calls on this outbound line group to a fax machine located at a specific extension. ext: directly forward all incoming calls through this outbound line group to an extension or a hunting group number. acd: forward all incoming calls on this outbound line group to the group of agents associated with a specific skill name.
exit	Leaves the sub-command mode.
pbx outbound-trust-peer *obtrunk_name*	Enters the sub-command mode for configuring the specified outbound trusted peer trunk's settings.
auto-attendant {aa|fax|ext|acd} *obtrunk_aa_name*	Configures the outbound trunk's auto attendant setting. aa: specify an auto attendant to which to forward all incoming calls on this outbound line group . fax: forward all incoming calls on this outbound line group to a fax machine located at a specific extension. ext: directly forward all incoming calls through this outbound line group to an extension or a hunting group number. acd: forward all incoming calls on this outbound line group to the group of agents associated with a specific skill name.
exit	Leaves the sub-command mode.

18.13.2 SIP Trunk and Trusted Peer Command Examples

Here are some examples of configuring and displaying SIP trunk and trusted peer settings.

18.13.2.1 Displaying PBX Outbound SIP Trunk Details

The following example displays the list of SIP trunks.

```
Router> show pbx outbound-sip-trunk sip-trunk-list
Trunk Name                              Descrption
================================================================================
mike_st881
```

18.13.2.2 Displaying PBX Trusted Peer Details

The following example displays the list of trusted peers.

```
Router> show pbx outbound-trust-peer trust-peer-list
Trunk Name                              Descrption
================================================================================
mike_tp881
mike_tp882
```

18.13.2.3 Configuring PBX Outbound SIP Trunk Settings

The following example configures a SIP trunk.

```
Router> configure terminal
Router(config)#pbx outbound-sip-trunk AAA
Router(pbx outbound-sip-trunk-AAA)#representative-number 1234
Router(pbx outbound-sip-trunk-AAA)#sip-server-address 1.1.1.1
Router(pbx outbound-sip-trunk-AAA)#register-server-address 1.1.1.1
Router(pbx outbound-sip-trunk-AAA)#authentication-name 1234
Router(pbx outbound-sip-trunk-AAA)#authentication-password 1234
Router(pbx outbound-sip-trunk-AAA)# exit
Router(config)# exit
Router#
```

18.13.2.4 Configuring PBX Trusted Peer Settings

The following example configures a trusted peer.

```
Router> configure terminal
Router(config)#pbx outbound-trust-peer AAA
Router(pbx outbound-trust-peer-AAA)#representative-number 1234
Router(pbx outbound-trust-peer-AAA)#sip-server-address 1.1.1.1
Router(pbx outbound-trust-peer-AAA)# exit
Router(config)# exit
Router#
```

18.13.2.5 Configuring PBX Outbound SIP Trunk DDI Settings

The following example configures DDI settings for a SIP trunk.

```
Router> configure terminal
Router(config)#pbx outbound-sip-trunk AAA
Router(pbx outbound-sip-trunk-AAA)#ddi-match-digit 2
Router(pbx outbound-sip-trunk-AAA)#ddi-mapping 01-02_1001-1002
Router(pbx outbound-sip-trunk-AAA)# exit
Router(config)# exit
Router#
```

18.13.2.6 Configuring PBX Trusted Peer DDI Settings

The following example configures DDI settings for a trusted peer.

```
Router> configure terminal
Router(config)#pbx outbound-trust-peer AAA
Router(pbx outbound-trust-peer-AAA)#no ddi-mapping all
Router(pbx outbound-trust-peer-AAA)# exit
Router(config)# exit
Router#
```

18.13.2.7 Configuring PBX Outbound SIP Trunk Auto Attendant Settings

The following example configures auto attendant settings for the AAA SIP trunk.

```
Router> configure terminal
Router(config)#pbx outbound-sip-trunk AAA
Router(pbx outbound-sip-trunk-AAA)#auto-attendant aa aa_test
Router(pbx outbound-sip-trunk-AAA)# exit
Router(config)# exit
Router#
```

18.13.2.8 Configuring PBX Trusted Peer Auto Attendant Settings

The following example configures auto attendant settings for the AAA trusted peer.

```
Router> configure terminal
Router(config)#pbx outbound-trust-peer AAA
Router(pbx outbound-trust-peer-AAA)#auto-attendant aa aa_test
Router(pbx outbound-trust-peer-AAA)# exit
Router(config)# exit
Router#
```

18.13.3 FXO Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 95 Input Values for FXO Commands

LABEL	DESCRIPTION
obtrunk_name	The name of the outbound trunk (0-29 characters). You can use alphanumeric characters and the underscore. It must start with a letter.
obtrunk_desc	A description using 0-64 alphanumeric characters (A-Z, a-z, 0-9) and underscores.
obtrunk_aa_name	The name of an outbound trunk auto attendant (1-30 characters). You can use alphanumeric characters and the underscore.
obtrunk_slot	The outbound group slot (A).
obtrunk_port	The outbound group port (1-9).

The following table describes the commands for configuring FXO groups. Use the `enable` or `configure terminal` command to be able to use the show commands. You must use the `configure terminal` command to enter the configuration mode before you can use the configuration commands.

Table 96 FXO Commands Summary

COMMAND	DESCRIPTION
`show pbx outbound-fxo {all | obtrunk_name}`	Displays information about the specified FXI trunk or all of them.
`[no] pbx outbound-fxo obtrunk_name`	Creates the specified outbound FXO group and enters the sub-command mode for configuring it. The `no` command deletes the FXO group.
`description obtrunk_desc`	Sets a description for the group.
`no description`	Removes the group's description.
`auto-attendant {aa|acd|ext|fax} obtrunk_aa_name`	Configures the outbound group's auto attendant setting. `aa`: specify an auto attendant to which to forward all incoming calls on this outbound line group . `acd`: forward all incoming calls on this outbound line group to the group of agents associated with a specific skill name. `ext`: directly forward all incoming calls through this outbound line group to an extension or a hunting group number. `fax`: forward all incoming calls on this outbound line group to a fax machine located at a specific extension.
`no auto-attendant`	Removes the outbound group's auto attendant setting.
`[no] slot obtrunk_slot port obtrunk_port`	Specifies a slot and port that belongs to the outbound group. The `no` command removes the slot and port from the outbound group.
`no slot all`	Removes all slots and ports from the outbound group.
`show`	Displays the outbound group's configuration.
`exit`	Leaves the sub-command mode.
`no pbx outbound-fxo all`	Deletes all of the FXO groups.

18.13.4 FXO Command Examples

Here are some examples of displaying and configuring FXO trunk settings.

18.13.4.1 Displaying the Configuration of All FXO Outbound Groups

The following example displays all of the FXO outbound groups.

```
Router> show pbx outbound-fxo all
fxo: fxo1
  description:
  aa-type: aa
  aa-name: default
  line: 0
    slot: A
    port: 1
fxo: fxo2
  description:
  aa-type: aa
  aa-name: default
  line: 2
    slot: A
    port: 3
  line: 3
    slot: A
    port: 4
```

18.13.4.2 Displaying the Configuration of a Specific FXO Outbound Group

The following example displays a specific FXO outbound group's configuration.

```
Router> show pbx outbound-fxo fxo1
fxo: fxo1
  description:
  aa-type: aa
  aa-name: default
  line: 0
    slot: A
    port: 1
```

18.13.4.3 Configuring an FXO Outbound Group

The following example configures an FXO outbound group named “fxo1”.

```
Router> configure terminal
Router(config)# pbx outbound-fxo fxo1
Router(config-bri01)# description fxo1
Router(config-bri01)# option aa
Router(config-bri01)# auto-attendant aa default
Router(config-bri01)# slot A port 1
Router(config-bri01)# exit
Router(config)#
```

18.13.5 BRI Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 97 Input Values for BRI Commands

LABEL	DESCRIPTION
obtrunk_name	The name of the outbound trunk (0-29 characters). You can use alphanumeric characters and the underscore. It must start with a letter.
obtrunk_desc	A description using 0-64 alphanumeric characters (A-Z, a-z, 0-9) and underscores.
obtrunk_aa_name	The name of an outbound trunk auto attendant (1-30 characters). You can use alphanumeric characters and the underscore.
obtrunk_ddi_match	The outbound trunk DDI match part (1-53 characters). You can use 0-9, a, b, underscores (_), and hpyhens (-).
obtrunk_slot	The outbound group slot (A).
obtrunk_port	The outbound group port (1-9).
obtrunk_msn_port	The outbound group’s ten-digit, MSN port number.
obtrunk_cpn_prefix	The outbound group’s 1-20 digit, calling party number prefix.
obtrunk_cpn_num	The outbound group’s 4-20 digit, calling party number or user defined number.

The following table describes the commands for configuring BRI outbound groups. Use the `enable` or `configure terminal` command to be able to use the show commands. You must use the `configure terminal` command to enter the configuration mode before you can use the configuration commands.

Table 98 BRI Commands Summary

COMMAND	DESCRIPTION
`show pbx outbound-bri {ddi | line}` *obtrunk_name*	Displays DDI or line settings for the specified BRI outbound group.
`show pbx outbound-bri {all |` *obtrunk_name*`}`	Displays information about the specified BRI outbound group or all of them.
`[no] pbx outbound-bri` *obtrunk_name*	Creates the specified outbound BRI group and enters the sub-command mode for configuring it. The `no` command deletes the BRI group.
`description` *obtrunk_desc*	Sets a description for the group.
`no description`	Removes the group’s description.

Table 98 BRI Commands Summary (continued)

COMMAND	DESCRIPTION
auto-attendant {aa|acd|ext|fax} *obtrunk_aa_name*	Configures the outbound group's auto attendant setting. aa: specify an auto attendant to which to forward all incoming calls on this outbound line group . acd: forward all incoming calls on this outbound line group to the group of agents associated with a specific skill name. ext: directly forward all incoming calls through this outbound line group to an extension or a hunting group number. fax: forward all incoming calls on this outbound line group to a fax machine located at a specific extension.
no auto-attendant	Removes the outbound group's auto attendant setting.
option { ddi | aa | direct | msn }	Sets the service type for this BRI trunk. ddi: people use a "direct number" to dial an outgoing call. You can also specify a prefix number in the caller number that might be required by your telephone company for outgoing calls using DDI/DID. aa: switch all calls coming through this interface to the Auto-Attendant system first. direct: forward all calls coming through this interface and from trusted callers to extensions. msn: switch all calls coming through this interface to Multiple Subscribe Numbers (MSNs) to the Auto-Attendant system first.
no option	Removes the service type setting.
directory-num *obtrunk_dir_num*	Enter your ISDN number registered with your telephone company. This number is used for the caller number when you make an outgoing call through the trunk from the extension which cannot be found in the DDI mapping table. This field can be 3-20 digits in length.
no directory-num	Removes the directory number setting.
ddi-mask <0..20>	Sets the number (0~20) of extension mapping digits from right to left. A DDI mask of 2 applied to the incoming ISDN number 555-123456 would identify the numbers 56.
ddi-mapping *obtrunk_ddi_match*	Sets the outbound trunk DDI match part.
no ddi-mapping {*obtrunk_ddi_match*|all}	Removes the specified outbound trunk DDI match part or all of the outbound trunk's DDI settings.
[no] slot *obtrunk_slot* port *obtrunk_port*	Specifies a slot and port that belongs to the outbound group. The no command removes the slot and port from the outbound group.
slot *obtrunk_slot* port *obtrunk_port* msn *obtrunk_msn_port*	Sets the specified slot and port to use the specified ten-digit, MSN port number.

Table 98 BRI Commands Summary (continued)

COMMAND	DESCRIPTION
calling-party-num {directory-num | user-define | extension | force-directory-num | force-user-define}	Sets the outbound group's outgoing calling party numbers. These are what the callee sees when the ISG50 sends a call out through this BRI trunk. directory-num: calls going out through this BRI trunk use the DDI/DID if the outgoing call matches it or the directory number if the outgoing call does not match the DDI/DID. user-define: calls going out through this BRI trunk use the DDI/DID if the outgoing call matches it or another number that you specify if the outgoing call does not match the DDI/DID. force-directory-num: calls going out through this BRI trunk use the trunk's directory number. force-user-define: calls going out through this BRI trunk use a calling party number that you specify. extension: calls going out through this BRI trunk use the caller's extension number.
calling-party-num-define *obtrunk_cpn_num*	Sets the BRI group's calling party number.
no calling-party-num-define	Removes the BRI group's calling party number setting.
calling-party-num-prefix *obtrunk_cpn_prefix*	Sets a calling party number prefix. A number to add in the beginning of the outgoing caller's numbers using this trunk line.
no calling-party-num-prefix	Removes the BRI group's calling party number prefix setting.
[no] calling-party-num-hide activate	Has your calling party number not display on the callee's caller ID. This only applies to calls going out through this BRI trunk that do not match the DDI/DID.
show	Displays the outbound group's configuration.
exit	Leaves the sub-command mode.

18.13.6 BRI Command Examples

Here are some examples of displaying and configuring BRI group settings.

18.13.6.1 Displaying All BRI Outbound Groups

The following example displays all of the BRI outbound groups.

```
Router> show pbx outbound-bri all
name: bri01
  description: BRI_01
name: bri02
  description: BRI_02
```

18.13.6.2 Displaying a Specific BRI Outbound Group

The following example displays the “bri01” BRI outbound group’s settings.

```
Router> show pbx outbound-bri bri01
name: bri01
  description: bri01
  option: aa
  directory-num:
  ddi-mask: 0
  aa-type: aa
  aa-name: default
  calling-party-num-prefix:
  calling-party-num: directory-num
  calling-party-num-define:
  calling-party-num-hide: false
```

18.13.6.3 Displaying a BRI Outbound Group’s DDI Settings

The following example displays the “bri02” BRI outbound group’s DDI settings.

```
Router> show pbx outbound-bri ddi bri02
ddi-mapping: 0
  number: 12
  extension: 2345
```

18.13.6.4 Displaying a BRI Outbound Group’s Line Settings

The following example displays the “bri01” BRI outbound group’s line settings.

```
Router> show pbx outbound-bri line bri01
line: 0
  slot: A
  port: 1
```

18.13.6.5 Configuring a BRI Outbound Group

The following example configures the “bri01” BRI outbound group.

```
Router> configure terminal
Router(config)# pbx outbound-bri bri01
Router(config-bri01)# description bri01
Router(config-bri01)# option aa
Router(config-bri01)# auto-attendant ext 1000
Router(config-bri01)# slot A port 1
Router(config-bri01)# exit
Router(config)#
```

18.14 Auto Attendant Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 99 Input Values for Auto Attendant Commands

LABEL	DESCRIPTION
pbx_operator_key	The number (0 or 9) for dialing the operator.
pbx_exten_num	A 3-10 digit extension number.
pbx_acd_num	A 3-10 digit Automatic Call Distribution (ACD) number.
pbx_page_num	A 3-10 digit paging group number.
pbx_hunt_num	A 3-10 digit hunt group number.
pbx_grp_name	The name of a PBX group such as an auto attendant. Use 0-29 alphanumeric characters and the underscore. It must start with a letter.
pbx_other_num	A 3-20 user-defined number.
pbx_description	A description using 0-62 alphanumeric characters (A-Z, a-z, 0-9) and spaces.
pbx_aa_path	The option sequence. [0-9]{1,2}(_[0-9]{1,2}){0,8}
pbx_aa_option	The one or two digit AA option key.
pbx_aa_schedule_option	A schedule item (1-6).

The following table describes the commands for configuring auto attendant settings. Use the `enable` or `configure terminal` command to be able to use the show commands. You must use the `configure terminal` command to enter the configuration mode before you can use the configuration commands.

Table 100 Auto Attendant Commands Summary

COMMAND	DESCRIPTION
`pbx auto-attendant default`	Enters the sub-command mode for configuring the default auto attendant's settings.
`operator` *pbx_operator_key* `extension` *pbx_exten_num*	Sets the key for dialing the operator and the operator's extension number.
`no operator`	Removes the operator configuration.
`timeout-action {hangup|operator}`	Sets the action for a call that times out. *hangup*: disconnects the call. *operator*: forwards the call to the operator.
`timeout-action extension` *pbx_exten_num*	Routes calls that time out to the specified extension.
`timeout-action acd` *pbx_acd_num*	Routes calls that time out to the specified ACD number.
`timeout-action page` *pbx_page_num*	Routes calls that time out to the specified page group.
`timeout-action hunt` *pbx_hunt_num*	Routes calls that time out to the specified hunt group.
`timeout-action aa` *pbx_grp_name*	Routes calls that time out to the specified auto attendant.
`timeout-action other` *pbx_other_num*	Routes calls that time out to the specified number.
`exit`	Leaves the sub-command mode.

Table 100 Auto Attendant Commands Summary (continued)

COMMAND	DESCRIPTION
no pbx auto-attendant *pbx_grp_name*	Removes the specified auto attendant.
pbx auto-attendant *pbx_grp_name*	Creates the specified auto attendant and enters the sub-command mode for configuring it.
description *pbx_description*	Configures the auto attendant's description.
no description	Removes the auto attendant's description.
exit	Leaves the sub-command mode.
pbx auto-attendant office-hour *pbx_grp_name*	Creates the specified office hours auto attendant and enters the sub-command mode for configuring it.
operator *pbx_operator_key* extension *pbx_exten_num*	Sets the key for dialing the operator and the operator's extension number.
no operator	Removes the operator configuration.
timeout-action {hangup|operator}	Sets the action for a call that times out. *hangup*: disconnects the call. *operator*: forwards the call to the operator.
timeout-action extension *pbx_exten_num*	Routes calls that time out to the specified extension.
timeout-action acd *pbx_acd_num*	Routes calls that time out to the specified ACD number.
timeout-action page *pbx_page_num*	Routes calls that time out to the specified page group.
timeout-action hunt *pbx_hunt_num*	Routes calls that time out to the specified hunt group.
timeout-action aa *pbx_grp_name*	Routes calls that time out to the specified auto attendant.
timeout-action other *pbx_other_num*	Routes calls that time out to the specified number.
direct-forward active	Forward all calls that come into this auto attendant to the extension, ACD, page group, hunt group, or user defined number specified by the directfw-action command.
no direct-forward active	Use the auto attendant's normal behavior.
directfw-action extension *pbx_exten_num*	Has the auto attendant forward all calls coming into it to the specified extension whenever direct-forward is active.
no directfw-action extension	Removes the direct forward to extension action configuration.
directfw-action acd *pbx_acd_num*	Has the auto attendant forward all calls coming into it to the specified ACD number whenever direct-forward is active.
no directfw-action acd	Removes the direct forward to ACD action configuration.
directfw-action page *pbx_page_num*	Has the auto attendant forward all calls coming into it to the specified page group whenever direct-forward is active.
no directfw-action page	Removes the direct forward to page group action configuration.
directfw-action hunt *pbx_hunt_num*	Has the auto attendant forward all calls coming into it to the specified hunt group whenever direct-forward is active.
no directfw-action hunt	Removes the direct forward to hunt group action configuration.

Table 100 Auto Attendant Commands Summary (continued)

COMMAND	DESCRIPTION
directfw-action other *pbx_other_num*	Has the auto attendant forward all calls coming into it to the specified number whenever direct-forward is active.
play-audio-file active	Has the auto attendant play its uploaded audio file before using direct forwarding to forward calls.
no play-audio-file active	Has the auto attendant not play its uploaded audio file before using direct forwarding to forward calls.
dial-extension active	Allow incoming calls to dial extensions that are not associated with specific key codes on the configured options list.
no dial-extension active	Allow incoming calls to only dial extensions configured in the options list.
option *pbx_aa_option* action forward-to-acd *pbx_exten_num*	Creates the specified auto attendant option for the user to forward the call to the specified ACD number.
option *pbx_aa_option* action forward-to-extension *pbx_exten_num*	Creates the specified auto attendant option for the user to forward the call to the specified extension number.
option *pbx_aa_option* action {forward-to-operator|repeat|sub-menu}	Creates the specified auto attendant option for the user to forward the call to the operator, repeat the menu options, or go to a sub-menu.
option *pbx_aa_option* action forward-to-page *pbx_page_num*	Creates the specified auto attendant option for the user to forward the call to the specified page group.
option *pbx_aa_option* action forward-to-hunt *pbx_hunt_num*	Creates the specified auto attendant option for the user to forward the call to the specified hunt group.
option *pbx_aa_option* action forward-to-aa *pbx_grp_name*	Creates the specified auto attendant option for the user to forward the call to the specified auto attendant.
option *pbx_aa_option* action forward-to-other *pbx_other_num*	Creates the specified auto attendant option for the user to forward the call to the specified number.
option *pbx_aa_option* description *pbx_description*	Configures the specified auto attendant option's description.
no option *pbx_aa_option* description	Removes the specified auto attendant option's description.
no option *pbx_aa_option*	Removes the specified auto attendant option.
exit	Leaves the sub-command mode.
pbx auto-attendant office-hour *pbx_grp_name* path *pbx_aa_path*	Creates the specified office hours auto attendant option path and enters the sub-command mode for configuring it.
[no] dial-extension active	Allow incoming calls to dial extensions that are not associated with specific key codes on the configured options list.
option *pbx_aa_option* description *pbx_description*	Configures a description for the specified auto attendant option.
no option *pbx_aa_option* description	Removes the description for the specified auto attendant option.
option *pbx_aa_option* action forward-to-extension *pbx_exten_num*	Creates the specified auto attendant option for the user to forward the call to the specified extension number.

Table 100 Auto Attendant Commands Summary (continued)

COMMAND	DESCRIPTION
option *pbx_aa_option* action sub-menu	Creates the specified auto attendant option for the user to go to a sub-menu.
option *pbx_aa_option* action forward-to-acd *pbx_exten_num*	Creates the specified auto attendant option for the user to forward the call to the specified ACD number.
option *pbx_aa_option* action forward-to-operator	Creates the specified auto attendant option for the user to forward the call to the operator.
option *pbx_aa_option* action repeat	Creates the specified auto attendant option for the user to repeat the menu options.
option *pbx_aa_option* action return-previous-menu	Creates the specified auto attendant option for the user to return to the previous menu.
option *pbx_aa_option* action forward-to-page *pbx_page_num*	Creates the specified auto attendant option for the user to forward the call to the specified page group.
option *pbx_aa_option* action forward-to-hunt *pbx_hunt_num*	Creates the specified auto attendant option for the user to forward the call to the specified hunt group.
option *pbx_aa_option* action forward-to-aa *pbx_grp_name*	Creates the specified auto attendant option for the user to forward the call to the specified auto attendant.
option *pbx_aa_option* action forward-to-other *pbx_other_num*	Creates the specified auto attendant option for the user to forward the call to the specified number.
no option *pbx_aa_option*	Removes the specified auto attendant option.
exit	Leaves the sub-command mode.
pbx auto-attendant greeting *pbx_grp_name*	Enters the sub-command mode for configuring a scheduled or temporary greeting for the specified auto attendant.
[no] temp-voice-file active	Enables or disables the temporary greeting. The temporary greeting can be played before the normal auto-attendant greeting to broadcast special messages, like:“We’re sorry but the Acme Mail Order Company is closed today to observe the holiday.”
[no] schedule active *pbx_aa_schedule_option*	Enables or disables the specified greeting schedule.
schedule {time1|time2|time3|time4|time5|time6} *oh_time*	Configures time ranges for scheduled greetings. A scheduled greeting can be played during specific time range severy day. This can be used to broadcast to highlight certain information only at certain hours, such as lunch time hours for the office building (“Thank you for calling the Acme Mail Order Company. As it is currently lunch time, representatives may be unavailable until 1 PM.”) time1|time2|time3|time4|time5|time6: These are the time ranges. *oh_time*: Enter the time range using 24-hour notation with the two times separated by a hyphen (hh:mm-hh:mm).
no schedule {time1|time2|time3|time4|time5|time6}	Removes the specified time range’s settings.
show	Displays the auto attendant’s scheduled and temporary greeting settings.
exit	Leaves the sub-command mode.

Table 100 Auto Attendant Commands Summary (continued)

COMMAND	DESCRIPTION
pbx auto-attendant night-service *pbx_grp_name*	Enters the sub-command mode for configuring night service settings for the specified auto attendant.
[no] night-service active	Enables or disables night service settings.
operator *pbx_operator_key* extension *pbx_exten_num*	Sets the key for dialing the operator and the operator's extension number.
no operator	Removes the operator configuration.
timeout-action {hangup|operator}	Sets the action for a call that times out. *hangup*: disconnects the call. *operator*: forwards the call to the operator.
timeout-action extension *pbx_exten_num*	Routes calls that time out to the specified extension.
timeout-action acd *pbx_exten_num*	Routes calls that time out to the specified ACD number.
timeout-action page *pbx_page_num*	Routes calls that time out to the specified page group.
timeout-action hunt *pbx_hunt_num*	Routes calls that time out to the specified hunt group.
timeout-action aa *pbx_grp_name*	Routes calls that time out to the specified auto attendant.
timeout-action other *pbx_other_num*	Routes calls that time out to the specified number.
direct-forward active	Forward all calls that come into this auto attendant during night hours to the extension, ACD, page group, hunt group, or user defined number specified by the directfw-action command.
no direct-forward active	Use the auto attendant's normal behavior.
directfw-action extension *pbx_exten_num*	Has the auto attendant forward all calls coming into it during night hours to the specified extension whenever direct-forward is active.
no directfw-action extension	Removes the night service direct forward to extension action configuration.
directfw-action acd *pbx_acd_num*	Has the auto attendant forward all calls coming into it during night hours to the specified ACD number whenever direct-forward is active.
no directfw-action acd	Removes the night service direct forward to ACD action configuration.
directfw-action page *pbx_page_num*	Has the auto attendant forward all calls coming into it during night hours to the specified page group whenever direct-forward is active.
no directfw-action page	Removes the night service direct forward to page group action configuration.
directfw-action hunt *pbx_hunt_num*	Has the auto attendant forward all calls coming into it during night hours to the specified hunt group whenever direct-forward is active.
no directfw-action hunt	Removes the night service direct forward to hunt group action configuration.
directfw-action other *pbx_other_num*	Has the auto attendant forward all calls coming into it during night hours to the specified number whenever direct-forward is active.
play-audio-file active	Has the auto attendant play its uploaded audio file before using direct forwarding to forward calls during night hours.

Table 100 Auto Attendant Commands Summary (continued)

COMMAND	DESCRIPTION
no play-audio-file active	Has the auto attendant not play its uploaded audio file before using direct forwarding to forward calls during night hours.
[no] dial-extension active	Allow incoming calls during night hours to dial extensions that are not associated with specific key codes on the configured options list.
option *pbx_aa_option* action forward-to-acd *pbx_exten_num*	Creates the specified auto attendant option for the user to forward the call to the specified ACD number during night hours.
option *pbx_aa_option* action forward-to-extension *pbx_exten_num*	Creates the specified auto attendant option for the user to forward the call to the specified extension number during night hours.
option *pbx_aa_option* action {forward-to-operator|repeat|sub-menu}	Creates the specified auto attendant option for the user to forward the call to the operator, repeat the menu options, or go to a sub-menu during night hours.
option *pbx_aa_option* action forward-to-page *pbx_page_num*	Creates the specified auto attendant option for the user to forward the call to the specified page group during night hours.
option *pbx_aa_option* action forward-to-hunt *pbx_hunt_num*	Creates the specified auto attendant option for the user to forward the call to the specified hunt group during night hours.
option *pbx_aa_option* action forward-to-aa *pbx_grp_name*	Creates the specified auto attendant option for the user to forward the call to the specified auto attendant during night hours.
option *pbx_aa_option* action forward-to-other *pbx_other_num*	Creates the specified auto attendant option for the user to forward the call to the specified number during night hours.
option *pbx_aa_option* description *pbx_description*	Configures the specified auto attendant night service option's description.
no option *pbx_aa_option* description	Removes the specified auto attendant night service option's description.
no option *pbx_aa_option*	Removes the specified auto attendant night service option.
exit	Leaves the sub-command mode.
pbx auto-attendant night-service *pbx_grp_name* path *pbx_aa_path*	Creates the specified night service hours auto attendant option path and enters the sub-command mode for configuring it.
[no] dial-extension active	Allow incoming calls during night hours to dial extensions that are not associated with specific key codes on the configured options list.
option *pbx_aa_option* description *pbx_description*	Configures a description for the specified auto attendant night service option.
no option *pbx_aa_option* description	Removes the description for the specified auto attendant night service option.
option *pbx_aa_option* action forward-to-extension *pbx_exten_num*	Creates the specified auto attendant option for the user to forward the call to the specified extension number.
option *pbx_aa_option* action sub-menu	Creates the specified auto attendant night service option for the user to go to a sub-menu.

Table 100 Auto Attendant Commands Summary (continued)

COMMAND	DESCRIPTION
option *pbx_aa_option* action forward-to-acd *pbx_exten_num*	Creates the specified auto attendant night service option for the user to forward the call to the specified ACD number.
option *pbx_aa_option* action forward-to-operator	Creates the specified auto attendant night service option for the user to forward the call to the operator.
option *pbx_aa_option* action repeat	Creates the specified auto attendant night service option for the user to repeat the menu options.
option *pbx_aa_option* action return-previous-menu	Creates the specified auto attendant night service option for the user to return to the previous menu.
option *pbx_aa_option* action forward-to-page *pbx_page_num*	Creates the specified auto attendant night service option for the user to forward the call to the specified page group.
option *pbx_aa_option* action forward-to-hunt *pbx_hunt_num*	Creates the specified auto attendant night service option for the user to forward the call to the specified hunt group.
option *pbx_aa_option* action forward-to-aa *pbx_grp_name*	Creates the specified auto attendant night service option for the user to forward the call to the specified auto attendant.
option *pbx_aa_option* action forward-to-other *pbx_other_num*	Creates the specified auto attendant night service option for the user to forward the call to the specified number.
no option *pbx_aa_option*	Removes the specified auto attendant night service option.
exit	Leaves the sub-command mode.
show pbx auto-attendant file space usage	Displays the auto attendant audio file space usage.
show pbx auto-attendant greeting *pbx_grp_name*	Displays the greeting configuration of the specified auto attendant.
show pbx auto-attendant night-service *pbx_grp_name*	Displays the night service configuration of the specified auto attendant.
show pbx auto-attendant night-service *pbx_grp_name* path *pbx_aa_path_show*	Displays the night service option path of the specified auto attendant.
show pbx auto-attendant night-service *pbx_grp_name* option	Displays the night service option menu configuration of the specified auto attendant.
show pbx auto-attendant office-hour *pbx_grp_name*	Displays the office hour configuration of the specified auto attendant.
show pbx auto-attendant office-hour *pbx_grp_name* path *pbx_aa_path_show*	Displays the office hour option path of the specified auto attendant.
show pbx auto-attendant office-hour *pbx_grp_name* option	Displays the office hour option menu configuration of the specified auto attendant.

18.14.1 Auto Attendant Command Examples

Here are some examples of displaying and configuring auto attendant settings.

18.14.1.1 Operator Key and Extension for the Default Auto Attendant

The following example assigns the key 0 and extension 1000 to be the operator for the default auto attendant.

```
Router# configure terminal
Router(config)# pbx auto-attendant default
Router(default-aa)# operator 0 extension 1000
Router(default-aa)# exit
Router(config)# exit
Router#
```

The following example removes the defaut auto attendant's operator configuration.

```
Router# configure terminal
Router(config)# pbx auto-attendant default
Router(default-aa)# no operator
Router(default-aa)# exit
Router(config)# exit
Router#
```

18.14.1.2 Timeout Action for the Default Auto Attendant

The following example sets the default auto attendant to hang up calls that time out.

```
Router# configure terminal
Router(config)# pbx auto-attendant default
Router(default-aa)# timeout-action hangup
Router(default-aa)# exit
Router(config)# exit
Router#
```

The following example sets the default auto attendant to forward calls that time out to ACD number 3333.

```
Router# configure terminal
Router(config)# pbx auto-attendant default
Router(default-aa)# timeout-action acd 3333
Router(default-aa)# exit
Router(config)# exit
Router#
```

18.14.1.3 Create or Remove a Custom Auto Attendant

The following example creates a customized auto attendant named “AA1”.

```
Router# configure terminal
Router(config)# pbx auto-attendant AA1
Router(customized-aa)# exit
Router(config)# exit
Router#
```

The following example deletes a customized auto attendant named “AA1”.

```
Router# configure terminal
Router(config)# no pbx auto-attendant AA1
Router(config)# exit
Router#
```

18.14.1.4 Set or Remove a Custom Auto Attendant Description

The following example sets the description for the custom “AA1” auto attendant to be “1st AA”.

```
Router# configure terminal
Router(config)# pbx auto-attendant AA1
Router(customized-aa)# description 1st AA
Router(customized-aa)# exit
Router(config)# exit
Router#
```

The following example removes the description for the custom “AA1” auto attendant to be “1st AA”.

```
Router# configure terminal
Router(config)# pbx auto-attendant AA1
Router(customized-aa)# no description
Router(customized-aa)# exit
Router(config)# exit
Router#
```

18.14.1.5 Office-hour Operator Key and Extension for a Custom Auto Attendant

The following example assigns the key 0 and extension 1000 to be the office-hour operator for the customized auto attendant “AA1”.

```
Router# configure terminal
Router(config)# pbx auto-attendant office-hour AA1
Router(customized-aa-oh)# operator 0 extension 1000
Router(customized-aa-oh)# exit
Router(config)# exit
Router#
```

The following example removes the office-hour, operator configuration from the customized auto attendant “AA1”.

```
Router# configure terminal
Router(config)# pbx auto-attendant office-hour AA1
Router(customized-aa-oh)# no operator
Router(customized-aa-oh)# exit
Router(config)# exit
Router#
```

18.14.1.6 Office-hour Timeout Action for a Custom Auto Attendant

The following example sets the “AA1” custom auto attendant to hang up calls that time out during office hours.

```
Router# configure terminal
Router(config)# pbx auto-attendant office-hour AA1
Router(customized-aa-oh)# timeout-action hangup
Router(customized-aa-oh)# exit
Router(config)# exit
Router#
```

The following example sets the “AA1” custom auto attendant to forward calls that time out during office hours to ACD number 3333.

```
Router# configure terminal
Router(config)# pbx auto-attendant office-hour AA1
Router(customized-aa-oh)# timeout-action acd 3333
Router(customized-aa-oh)# exit
Router(config)# exit
Router#
```

18.14.1.7 Office-hour Direct Forwarding for a Custom Auto Attendant

The following example enables direct forwarding for incoming calls for the “AA1” custom auto attendant during office hours.

```
Router# configure terminal
Router(config)# pbx auto-attendant office-hour AA1
Router(customized-aa-oh)# direct-forward active
Router(customized-aa-oh)# exit
Router(config)# exit
Router#
```

The following example has the “AA1” custom auto attendant play the audio file before directly forwarding incoming calls during office hours.

```
Router# configure terminal
Router(config)# pbx auto-attendant office-hour AA1
Router(customized-aa-oh)# play-audio-file active
Router(customized-aa-oh)# exit
Router(config)# exit
Router#
```

The following example has the “AA1” custom auto attendant directly forward incoming calls to paging number 2222 during office hours.

```
Router# configure terminal
Router(config)# pbx auto-attendant office-hour AA1
Router(customized-aa-oh)# directfw-action page 2222
Router(customized-aa-oh)# exit
Router(config)# exit
Router#
```

The following example removes the “AA1” custom auto attendant’s configuration for directly forwarding incoming calls to an ACD number during office hours.

```
Router# configure terminal
Router(config)# pbx auto-attendant office-hour AA1
Router(customized-aa-oh)# no directfw-action acd
Router(customized-aa-oh)# exit
Router(config)# exit
Router#
```

18.14.1.8 Office-hour Dial Extension Option for a Custom Auto Attendant

The following example enables the dial extension option for incoming calls for the “AA1” custom auto attendant during office hours.

```
Router# configure terminal
Router(config)# pbx auto-attendant office-hour AA1
Router(customized-aa-oh)# dial-extension active
Router(customized-aa-oh)# exit
Router(config)# exit
Router#
```

The following example disables the dial extension option for incoming calls for the “AA1” custom auto attendant during office hours.

```
Router# configure terminal
Router(config)# pbx auto-attendant office-hour AA1
Router(customized-aa-oh)# no dial-extension active
Router(customized-aa-oh)# exit
Router(config)# exit
Router#
```

18.14.1.9 Office-hour Option Key and Action for a Custom Auto Attendant

The following example adds option key 5 to forward a call to extension 1000 for the “AA1” custom auto attendant during office hours.

```
Router# configure terminal
Router(config)# pbx auto-attendant office-hour AA1
Router(customized-aa-oh)# option 5 action forward-to-extension 1000
Router(customized-aa-oh)# exit
Router(config)# exit
Router#
```

The following example removes option key 5 for the “AA1” custom auto attendant during office hours.

```
Router# configure terminal
Router(config)# pbx auto-attendant office-hour AA1
Router(customized-aa-oh)# no option 5
Router(customized-aa-oh)# exit
Router(config)# exit
Router#
```

18.14.1.10 Office-hour Sub-menu Dial Extension Option for a Custom Auto Attendant

The following example enables the dial extension option for sub-menu 5_5 for incoming calls for the “AA1” custom auto attendant during office hours.

```
Router# configure terminal
Router(config)# pbx auto-attendant office-hour AA1 path 5_5
Router(customized-aa-oh-sub)# dial-extension active
Router(customized-aa-oh)# exit
Router(config)# exit
Router#
```

The following example disables the dial extension option for sub-menu 5_5 for incoming calls for the “AA1” custom auto attendant during office hours.

```
Router# configure terminal
Router(config)# pbx auto-attendant office-hour AA1 path 5_5
Router(customized-aa-oh-sub)# no dial-extension active
Router(customized-aa-oh)# exit
Router(config)# exit
Router#
```

18.14.1.11 Office-hour Sub-menu Option Key and Action for a Custom Auto Attendant

The following example adds option key 3 to forward a call to extension 1000 for sub-menu 5_5 for incoming calls for the “AA1” custom auto attendant during office hours.

```
Router# configure terminal
Router(config)# pbx auto-attendant office-hour AA1 path 5_5
Router(customized-aa-oh-sub)# option 3 action forward-to-extension 1000
Router(customized-aa-oh)# exit
Router(config)# exit
Router#
```

The following example removes option key 4 from sub-menu 5_5 for incoming calls for the “AA1” custom auto attendant during office hours.

```
Router# configure terminal
Router(config)# pbx auto-attendant office-hour AA1 path 5_5
Router(customized-aa-oh-sub)# no option 4
Router(customized-aa-oh)# exit
Router(config)# exit
Router#
```

18.14.1.12 Greeting for a Custom Auto Attendant

The following example enables the temporary greeting for the "AA1" custom auto attendant.

```
Router# configure terminal
Router(config)# pbx auto-attendant greeting AA1
Router(customized-aa-greeting)# temp-voice-file active
Router(customized-aa-greeting)# exit
Router(config)# exit
Router#
```

The following example enables the 1st scheduled greeting for the "AA1" custom auto attendant.

```
Router# configure terminal
Router(config)# pbx auto-attendant greeting AA1
Router(customized-aa-greeting)# schedule active 1
Router(customized-aa-greeting)# exit
Router(config)# exit
Router#
```

The following example sets a time range of 12:00-13:00 for the 1st scheduled greeting for the "AA1" custom auto attendant.

```
Router# configure terminal
Router(config)# pbx auto-attendant greeting AA1
Router(customized-aa-greeting)# schedule time1 12:00-13:00
Router(customized-aa-greeting)# exit
Router(config)# exit
Router#
```

18.14.1.13 Enable or Disable Night Service for a Custom Auto Attendant

The following example enables the night service settings for the "AA1" custom auto attendant.

```
Router# configure terminal
Router(config)# pbx auto-attendant night-service AA1
Router(customized-aa-ns)# night-service active
Router(customized-aa-ns)# exit
Router(config)# exit
Router#
```

The following example disables the night service settings for the “AA1” custom auto attendant.

```
Router# configure terminal
Router(config)# pbx auto-attendant night-service AA1
Router(customized-aa-ns)# no night-service active
Router(customized-aa-ns)# exit
Router(config)# exit
Router#
```

18.14.1.14 Night-service Operator Key and Extension for a Custom Auto Attendant

The following example assigns the key 0 and extension 1000 to be the night-service operator for the customized auto attendant “AA1”.

```
Router# configure terminal
Router(config)# pbx auto-attendant night-servce AA1
Router(customized-aa-ns)# operator 0 extension 1000
Router(customized-aa-ns)# exit
Router(config)# exit
Router#
```

The following example removes the night-service operator configuration for the customized auto attendant “AA1”.

```
Router# configure terminal
Router(config)# pbx auto-attendant night-service AA1
Router(customized-aa-ns)# no operator
Router(customized-aa-ns)# exit
Router(config)# exit
Router#
```

18.14.1.15 Night-service Timeout Action for a Custom Auto Attendant

The following example sets the “AA1” custom auto attendant to hang up calls that time out during night-service hours.

```
Router# configure terminal
Router(config)# pbx auto-attendant night-service AA1
Router(customized-aa-ns)# timeout-action hangup
Router(customized-aa-ns)# exit
Router(config)# exit
Router#
```

The following example sets the “AA1” custom auto attendant to forward calls that time out during night-service hours to ACD number 3333.

```
Router# configure terminal
Router(config)# pbx auto-attendant night-service AA1
Router(customized-aa-ns)# timeout-action acd 3333
Router(customized-aa-ms)# exit
Router(config)# exit
Router#
```

18.14.1.16 Night-service Direct Forwarding for a Custom Auto Attendant

The following example enables direct forwarding for incoming calls for the “AA1” custom auto attendant during night-service hours.

```
Router# configure terminal
Router(config)# pbx auto-attendant night-service AA1
Router(customized-aa-ns)# direct-forward active
Router(customized-aa-ns)# exit
Router(config)# exit
Router#
```

The following example has the “AA1” custom auto attendant play the audio file before directly forwarding incoming calls during night-service hours.

```
Router# configure terminal
Router(config)# pbx auto-attendant night-service AA1
Router(customized-aa-ns)# play-audio-file active
Router(customized-aa-ns)# exit
Router(config)# exit
Router#
```

The following example has the “AA1” custom auto attendant directly forward incoming calls to paging number 2222 during night-service hours.

```
Router# configure terminal
Router(config)# pbx auto-attendant night-service AA1
Router(customized-aa-ns)# directfw-action page 2222
Router(customized-aa-ns)# exit
Router(config)# exit
```

The following example removes the “AA1” custom auto attendant’s configuration for directly forwarding incoming calls to an ACD number during night-service hours.

```
Router# configure terminal
Router(config)# pbx auto-attendant night-service AA1
Router(customized-aa-ns)# no directfw-action acd
Router(customized-aa-ns)# exit
Router(config)# exit
Router#
```

18.14.1.17 Night-service Dial Extension Option for a Custom Auto Attendant

The following example enables the dial extension option for incoming calls for the “AA1” custom auto attendant during night-service hours.

```
Router# configure terminal
Router(config)# pbx auto-attendant night-service AA1
Router(customized-aa-ns)# dial-extension active
Router(customized-aa-ns)# exit
Router(config)# exit
Router#
```

The following example disables the dial extension option for incoming calls for the “AA1” custom auto attendant during night-service hours.

```
Router# configure terminal
Router(config)# pbx auto-attendant night-service AA1
Router(customized-aa-ns)# no dial-extension active
Router(customized-aa-ns)# exit
Router(config)# exit
Router#
```

18.14.1.18 Night-service Option Key and Action for a Custom Auto Attendant

The following example adds option key 5 to forward a call to extension 1000 for the “AA1” custom auto attendant during night-service hours.

```
Router# configure terminal
Router(config)# pbx auto-attendant night-service AA1
Router(customized-aa-ns)# option 5 action forward-to-extension 1000
Router(customized-aa-ns)# exit
Router(config)# exit
Router#
```

The following example removes option key 5 for the “AA1” custom auto attendant during night-service hours.

```
Router# configure terminal
Router(config)# pbx auto-attendant night-service AA1
Router(customized-aa-ns)# no option 5
Router(customized-aa-ns)# exit
Router(config)# exit
Router#
```

18.14.1.19 Night-service Sub-menu Dial Extension Option for a Custom Auto Attendant

The following example enables the dial extension option for sub-menu 5_5 for incoming calls for the “AA1” custom auto attendant during night-service hours.

```
Router# configure terminal
Router(config)# pbx auto-attendant night-service AA1 path 5_5
Router(customized-aa-ns-sub)# dial-extension active
Router(customized-aa-ns-sub)# exit
Router(config)# exit
Router#
```

The following example disables the dial extension option for sub-menu 5_5 for incoming calls for the “AA1” custom auto attendant during night-service hours.

```
Router# configure terminal
Router(config)# pbx auto-attendant night-service AA1 path 5_5
Router(customized-aa-ns-sub)# no dial-extension active
Router(customized-aa-ns-sub)# exit
Router(config)# exit
Router#
```

18.14.1.20 Night-service Sub-menu Option Key and Action for a Custom Auto Attendant

The following example adds option key 3 to forward a call to extension 1000 for sub-menu 5_5 for incoming calls for the “AA1” custom auto attendant during night-service hours.

```
Router# configure terminal
Router(config)# pbx auto-attendant night-service AA1 path 5_5
Router(customized-aa-ns-sub)# option 3 action forward-to-extension 1000
Router(customized-aa-ns-sub)# exit
Router(config)# exit
Router#
```

The following example removes option key 4 from sub-menu 5_5 for incoming calls for the "AA1" custom auto attendant during night-service hours.

```
Router# configure terminal
Router(config)# pbx auto-attendant night-service AA1 path 5_5
Router(customized-aa-ns-sub)# no option 4
Router(customized-aa-ns-sub)# exit
Router(config)# exit
Router#
```

18.14.1.21 Auto Attendant Show Commands

The following example displays the auto attendant audio file space usage.

```
Router# configure terminal
Router(config)# show pbx auto-attendant file space usage
Total: 30 min.
Used: 0 min. 4 sec.
Free: 29 min. 55 sec.
Used Persentage: 0%
Router(config)# exit
Router#
```

The following example displays the settings of sub-menu 5_5 in custom auto attendant "AA1" during office hours.

```
Router# configure terminal
Router(config)# show pbx auto-attendant office-hour AA1 path 5_5
AA Name: AA1
Dial Extension: enable
Description:
Path: 5
File Status: Inexistent
File Size:
File Date:
Router(config)# exit
Router#
```

18.15 LCR Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 101 Input Values for LCR Commands

LABEL	DESCRIPTION
lcr_name	The Least Cost Routing (LCR) entry name. Use 1-20 alphanumeric characters and the underscore. The first character must be a letter.
lcr_desc	A description for the LCR. Use 0-64 alphanumeric characters (A-Z, a-z, 0-9) and the underscore.
lcr_maxcalltime	The maximum call time in seconds (0-9999).
lcr_channel	The outbound channel. [0-9a-zA-Z:/_%]+
lcr_dialcond	A 1-20 character dial condition criteria for using the outbound dialing rule. The criteria can be • a specific number - for example “55555555”; in this case the number dialed by users must match this string exactly. • any number starting with a specified pattern of digits - for example “0.”, “555.”, “011.” and so on; in this case the number dialed must match the digits before the period “.” and it doesn’t matter what follows. For example dialing “0222-2222” matches the dialing condition “0.”. You can also specify a range for digits within a dial condition. You can: • use the letters **X**, **Z**, **N** to specify a range of numbers to match. **X** represents the range **0**-**9**, **Z** represents the range **1**-**9** and **N** represents the range **2**-**9**. • use brackets to specify an allowed range for a dialed digit. For example **[0-8]** or **[0-46-9]**, in the second example **5** is not allowed. Use the **Right** button to test if the dial condition is in acceptable format. Note: Create unique dial conditions for each LCR. The ISG50 is not able to distinguish between LCRs if they have the same dial condition.
lcr_offset	Specify how many initial digits of the dialed number should not be included in the number going out of the ISG50. (0-99)
lcr_length	Specify the maximum length for the number dialed. If you set a limit, the ISG50 cuts off numbers which extend beyond the limit .
lcr_prefix	The dial number prefix. Use 0-8 alphanumeric characters (0-9, a-z) asterisks (*), and pluses (+). Specify a number which should be inserted at the beginning of the dialed number before it is sent out from the ISG50. Use a “p” to have a 0.5 second pause between dialing numbers. For example, enter “0p5” to have the ISG50 wait 0.5 second after dialing 0 and then dial 5.
lcr_postfix	The dial number postfix. Use 0-8 alphanumeric characters (0-9, a-z) asterisks (*), and pluses (+). Specify a number which should be appended to the end of the dialed number before it is sent out from the ISG50. Use a “p” to have a 0.5 second pause between dialing numbers. For example, enter “0p5” to have the ISG50 wait 0.5 second after dialing 0 and then dial 5.

The following table describes the commands for configuring least cost routing settings. Use the `enable` or `configure terminal` command to be able to use the show commands. You must use the

`configure terminal` command to enter the configuration mode before you can use the configuration commands.

Table 102 LCR Commands Summary

COMMAND	DESCRIPTION
`show pbx lcr {all|`*`lcr_name`*`}`	Displays the specified or all LCR configurations.
`move pbx lcr LCR_NAME to` *`lcr_name`*	Moves the first listed LCR to the position of the second listed LCR.
`no pbx lcr {all|` *`lcr_name`*`}`	Removes all LCRs in the PBX or the specified LCR.
`pbx lcr %` *`lcr_name`*	Enters the sub-command mode for configuring the specified LCR.
`show`	Displays the LCR's configuration.
`description` *`lcr_desc`*	Adds a description for this LCR.
`no description`	Removes the description from this LCR.
`max-call-time` *`lcr_maxcalltime`*	Adds a maximum call time setting for this LCR.
`no max-call-time`	Removes the maximum call time setting for this LCR.
`channel` *`lcr_channel`*	Adds a channel to this LCR.
`no channel { all|`*`lcr_channel`*` }`	Removes one or all channels from this LCR.
`move channel` *`lcr_channel`* `to` *`lcr_channel`*	Moves the first listed channel to the position of the second listed channel.
`dial-condition` *`lcr_dialcond`*	Adds a dial condition to this LCR.
`no dial-condition { all|`*`lcr_dialcond`*` }`	Removes one or all dial conditions from this LCR.
`move dial-condition` *`lcr_dialcond`* `to` *`lcr_dialcond`*	Moves the first listed dial condition to the position of the second listed dial condition.
`param dial-condition` *`lcr_dialcond`* `channel` *`lcr_channel`* `[offset` *`lcr_offset`*`] [length` *`lcr_length`*`] [prefix` *`lcr_prefix`*`] [postfix` *`lcr_postfix`*`]`	Adds dial parameters for specified dial condition and channel.
`no param dial-condition` *`lcr_dialcond`* `channel` *`lcr_channel`*	Removes dial parameters for the specified dial condition and channel.
`no param all`	Removes all dial parameters in this LCR.
`exit`	Leaves the sub-command mode.

18.15.1 LCR Command Examples

Here are some examples of displaying and configuring LCRs.

18.15.1.1 Display LCRs

The following example displays all the PBX LCRs in the system.

```
Router# configure terminal
Router(config)# show pbx lcr all

lcr: ooo
  description: hello ooo
  max-call-time: 88
  dc: 02XXXXXXXX
  dc: 0922XXXXXX
  ch: fxo
  ch: pri
  param: 0
    dial-condition: 02XXXXXXXX
    channel: fxo
    offset: 1
    length:
    prefix: 886
    postfix:
  param: 1
    dial-condition: 0922XXXXXX
    channel: pri
    offset:
    length:
    prefix: 9
    postfix:
Router(config)# exit
Router#
```

18.15.1.2 Move an LCR

The following example moves the xxx LCR to the position of the ooo LCR.

```
Router# configure terminal
Router(config)# move pbx lcr xxx to ooo
```

18.15.1.3 Configure an LCR

The following example configures LCR ooo.

```
Router(config)# pbx lcr ooo
Router(lcr ooo)# description hello ooo
Router(lcr ooo)# max-call-time 88
Router(lcr ooo)# channel xo1
Router(lcr ooo)# channel xo2
Router(lcr ooo)# channel bri1
Router(lcr ooo)# dial-condition 035XXXXXX
Router(lcr ooo)# dial-condition 02XXXXXXX
Router(lcr ooo)# dial-condition 0922XXXXXX
Router(lcr ooo)# param dial-condition 035XXXXXX channel xo1 offset 0 prefix 9
postfix b
Router(lcr ooo)# param dial-condition 02XXXXXXX channel xo2 prefix c postfix x
Router(lcr ooo)# param dial-condition 0922XXXXXX channel bri1 prefix 9 postfix xx
Router(lcr ooo)# exit
Router(config)# exit
Router#
```

18.16 Group Management Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 103 Input Values for Group Management Commands

LABEL	DESCRIPTION
pbx_grp_name	The name of the authority group. Use 0-29 alphanumeric characters and the underscore (_). It must begin with a letter.

The following table describes the commands for configuring group management settings. Use the `enable` or `configure terminal` command to be able to use the show commands. You must use the `configure terminal` command to enter the configuration mode before you can use the configuration commands.

Table 104 Group Management Commands Summary

COMMAND	DESCRIPTION
`pbx group-management` *pbx_grp_name*	Enters the sub-command mode for configuring the specified authority group.
`[no] associate authority-group` *pbx_grp_name*	Associates the authority group being configured with the specified authority group. This gives the authority group being configured the specified group's access rights. The `no` command removes the association.
`associate authority-group all`	Associates all created authority groups with the group being configured.
`[no] associate lcr` *pbx_grp_name*	Associates the authority group being configured with the specified authority group's LCRs. This lets the authority group being configured use the LCRs to which the specified group has access. The `no` command removes the association.

Table 104 Group Management Commands Summary (continued)

COMMAND	DESCRIPTION
no associate lcr all	Removes the association of the authority group being configured to any other LCRs.
show	Displays the authority group's association configuration.
exit	Leaves the sub-command mode.
show pbx group-management	Lists all the configured authority groups.
show pbx group-management *pbx_grp_name*	Displays the specified authority group's association configuration.

18.16.1 Group Management Command Examples

Here are some examples of displaying and configuring group management.

18.16.1.1 Associate Authority Groups

This example associates authority group AG2 to authority group AG1.

```
Router# configure terminal
Router(config)# pbx group-management AG1
Router(grp-mng)# associate authority-group AG2
Router(grp-mng)# exit
Router(config)# exit
Router#
```

This example removes the association of authority group AG2 from authority group AG1.

```
Router# configure terminal
Router(config)# pbx group-management AG1
Router(grp-mng)# no associate authority-group AG2
Router(grp-mng)# exit
Router(config)# exit
Router#
```

This example associates all authority groups with authority group AG1.

```
Router# configure terminal
Router(config)# pbx group-management AG1
Router(grp-mng)# associate authority-group all
Router(grp-mng)# exit
Router(config)# exit
Router#
```

18.16.1.2 Display Authority Groups

This example displays all the created authority groups in the system.

```
Router# configure terminal
Router(config)# show pbx group-management
Sequence Type       Group Name                 Description
================================================================================
1    Authority Group  AG1
2       Authority Group  AG2
…
Router(config)# exit
Router#
```

This example displays the association configuration of authority group AG1.

```
Router# configure terminal
Router(config)# show pbx group-management AG1
Sequence Group Type   Ass.   Group Name               Description
================================================================================
1     Authority Group Allow   AG1
2        Authority Group Allow    AG2
…
Router(config)# exit
Router#
```

This example shows another way to display the association configuration of authority group AG1.

```
Router# configure terminal
Router(config)# pbx group-management AG1
Router(grp-mng)# show
Sequence Group Type   Ass.   Group Name               Description
================================================================================
1     Authority Group Allow   AG1
2        Authority Group Allow    AG2
Router(grp-mng)# exit
Router(config)# exit
Router#
```

18.17 Call Service Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 105 Input Values for Call Service Commands

LABEL	DESCRIPTION
exten_num	An extension number already configured in the ISG50.
emer_outboundline	The name of an outbound line. Use 1-50 alphanumeric characters, the underscore (_), and hyphen (-).

Table 105 Input Values for Call Service Commands (continued)

LABEL	DESCRIPTION
emer_prefix	This is any prefix that must be added to emergency calls when using this outside line. Specify a number which should be inserted at the beginning of the dialed number before it is sent out from the ISG50. For example, if the ISG50 is behind another PBX and calls to the outside require a “0” to be dialed first, specify it here. Use 0-32 alphanumeric characters, asterisk (*), and plus (+).
emer_num	The 3-10 digit emergency number. This is the number (such as 911) a person dials in case of emergency.
moh_name	A custom music on hold name. Use 2-19 alphanumeric characters, the underscore (_), and hyphen (-). It must start with a letter.
description2	The description for custom music on hold. Use 1-60 alphanumeric characters, the underscore (_), hyphen (-), and spaces. It must start with a letter.
cb_bkid	This is a 1-20 digit telephone number the ISG50 blocks from calling extensions in your telephone network. When adding or editing an entry, type the telephone number. You can also use the letters X, Z and N to represent numbers you want to block. The letter “X” represents any digit from 0-9, Z any digit from 1-9 and N any digit from 2-9. For example, enter 023XXXXXX to block any 9 digit number that starts with 023 from calling the extensions configured on the ISG50. Furthermore, you can use the period (.) as a wildcard, to block any numbers that begin with a pattern of digits you specify. For example, enter 555. to block any numbers starting with the string 555 from calling the extensions configured on the ISG50.

The following table describes the commands for configuring call service settings. Use the `enable` or `configure terminal` command to be able to use the show commands. You must use the `configure terminal` command to enter the configuration mode before you can use the configuration commands.

Table 106 Call Service Commands Summary

COMMAND	DESCRIPTION
`show pbx autocallback`	Displays the auto callback configuration.
`pbx autocallback`	Enters the sub-command mode for configuring the auto callback settings.
`[no] activate`	Turns auto callback on or off.
`queue-size <1..5>`	Sets a limit to the number of auto callback requests for each extension.
`show pbx callpark`	Displays the call park configuration.
`pbx callpark`	Enters the sub-command mode for configuring the call park settings.
`rep-extension <100-99999999> slot-number <1-99>`	Sets the 3-8 digit telephone number users should dial to park a telephone call and the number of call parking slot extensions available.
`expire <60..300>`	Sets the maximum number of seconds that a call can be parked. After a parked call exceeds this amount of time, it will ring back to the extension that parked the call.
`show pbx callwait`	Displays the call waiting configuration.

Table 106 Call Service Commands Summary (continued)

COMMAND	DESCRIPTION
pbx callwait	Enters the sub-command mode for configuring the call waiting settings.
[no] extension *exten_num*	Turns call waiting on or off for the specified extension.
pbx emergency-call	Enters the sub-command mode for configuring the emergency call settings.
outbound-line sip-trunk *emer_outboundline* prefix {none|*emer_prefix*}	Adds the specified SIP trunk outbound line group and any required prefix to be used for emergency calls.
no outbound-line sip-trunk *emer_outboundline*	Removes the specified SIP trunk outbound line group from emergency call use.
outbound-line fxo <1..4> prefix {none|*emer_prefix*}	Adds the specified FXO port and any required prefix to be used for emergency calls.
no outbound-line fxo <1..4>	Removes the specified FXO port from emergency call use.
outbound-line bri <1..4> prefix {none|*emer_prefix*}	Adds the specified BRI port and any required prefix to be used for emergency calls.
no outbound-line bri <1..4>	Removes the specified BRI port from emergency call use.
[no] number *emer_num*	Adds or removes an emergency number.
show all-outbound-line	Displays all the outbound lines.
exit	Leaves the sub-command mode.
show pbx emergency-call number	Displays all the configured emergency call numbers.
show pbx emergency-call outbound-line	Displays all the outbound lines configured to be used for emergency calls.
[no] pbx moh *moh_name*	Creates the specified custom music on hold profile and enters the sub-command mode for configuring it. The no command deletes the specified custom music on hold profile.
description *description2*	Adds a description for the custom music on hold profile.
no description	Removes the description for the custom music on hold profile.
show	Displays the custom music on hold profile's configuration.
exit	Leaves the sub-command mode.
pbx moh set-default { built-in | *moh_name* }	Sets which music on hold profile to use as the system default. Use either the built-in music on hold profile or a customized music on hold profile that you created.
show pbx moh list	Displays the details of the custom music on hold profiles.
show pbx moh default	Displays the details of the music on hold profile the system is set to use as the default.
show pbx moh usage	Displays music on hold audio file storage space usage details.
show pbx callxfer digit-timeout	Displays the maximum number of seconds the ISG50 waits for each digit input of a complete callee number after you press the flash key on the phone.

Table 106 Call Service Commands Summary (continued)

COMMAND	DESCRIPTION
show pbx callxfer local-handling	Displays whether or not the ISG50 allows a caller to transfer a current external call (via an outbound line group) to another extension.
pbx callxfer digit-timeout <1..99>	Sets the maximum number of seconds the ISG50 waits for each digit input of a complete callee number after you press the flash key on the phone. If the ISG50 does not receive another digit within this time period, the ISG50 processes digits you have dialed.
[no] pbx callxfer local-handling activate	Sets whether or not the ISG50 allows a caller to transfer a current external call (via an outbound line group) to another extension.
pbx call-block black-list	Enters the sub-command mode for configuring the system-wide call blocking black list settings.
[no] activate	Turns call blocking on or off.
[no] rule *cb_bkid*	Adds or removes a rule for blocking calls to the ISG50's extensions.
no rule all	Removes all rules for blocking calls to the ISG50's extensions.
[no] pbx call-block anonymous-block activate	Sets whether or not to block incoming calls without caller ID.
show	Displays the system-wide call blocking rules.
exit	Leaves the sub-command mode.
show pbx call-block	Shows whether call blocking and anonymous call blocking are enabled.
show pbx call-block black-list	Displays the system-wide call blocking rules.

18.17.1 Call Service Command Examples

Here are some examples of displaying and configuring call service settings.

18.17.1.1 Display Auto Callback Settings

This example displays the auto callback configuration.

```
Router> show pbx autocallback
activate: yes
queue size: 5
Router#
```

18.17.1.2 Configure Auto Callback

This example turns on the auto callback feature.

```
Router> configure terminal
Router(config)# pbx autocallback
Router(autocallback)# activate
Router(autocallback)# exit
Router(config)# exit
Router#
```

This example sets a limit of five auto callback requests for each extension.

```
Router> configure terminal
Router(config)# pbx autocallback
Router(autocallback)# queue-size 5
Router(autocallback)# exit
Router(config)# exit
Router#
```

18.17.1.3 Display Call Park Settings

This example displays the call parking configuration.

```
Router> show pbx callpark
rep extension: 800
slot number: 16
expire: 180
Router#
```

18.17.1.4 Configure Call Parking

This example sets 800 as the call parking representative extension number users dial to park a telephone call and limits the total number of parked calls to 20. It also sets the maximum number of seconds that a call can be parked to 200.

```
Router> configure terminal
Router(config)# pbx callpark
Router(callpark)# rep-extension 800 slot-number 20
Router(callpark)# expire 200
Router(callpark)# exit
Router(config)# exit
Router#
```

18.17.1.5 Display Call Waiting Settings

This example displays the call waiting configuration.

```
Router> show pbx callwait
Index    Extension
============================
1        7141
2        7131
3        7132
Router#
```

18.17.1.6 Configure Call Waiting

This example enables call waiting for extension 7141.

```
Router> configure terminal
Router(config)# pbx callwait
Router(callwait)# extension 7141
Router(callwait)# exit
Router(config)# exit
Router#
```

18.17.1.7 Configure Emergency Call Settings

This example configures the ISG50 to use siptrunk1 with no prefix and FXO port 1 with prefix 1 for emergency calls. It also has add 911 as an emergency call number.

```
Router> configure terminal
Router(config)#pbx emergency-call
Router(config)# outbound-line sip-trunk siptrunk1 prefix none
Router(config)# outbound-line fxo prefix 1
Router(config)# number 911
Router(config)# exit
Router#
```

18.17.1.8 Display Emergency Call Settings

This example displays the emergency call numbers.

```
Router> show pbx emergency-call number
number
================================================================================
911
Router#
```

This example displays the outbound lines the ISG50 uses for emergency calls.

```
Router> show pbx emergency-call outbound-line
index: 0
  outbound line: fxo:Port1
  prefix:
index: 1
  outbound line: siptrunk1
  prefix:
Router#
```

18.17.1.9 Configure Music on Hold Settings

This example creates a music on hold profile named mymoh1 and adds a description for it.

```
Router> configure terminal
Router(config)#pbx moh mymoh1
Router(config-moh-mymoh1)#description mymoh
Router(config-moh-mymoh1)# exit
Router(config)# exit
Router#
```

This example has the ISG50 use the built-in music on hold profile as the system default.

```
Router> configure terminal
Router(config)# pbx moh set-default built-in
Router(config)# exit
Router#
```

18.17.1.10 Display Music on Hold Settings

This example displays the details of the custom music on hold profiles.

```
Router> show pbx moh list
number: 1
  name: mymoh1
  file: none
  system:
  description: mymoh1
number: 2
  name: mymoh2
  file: none
  system:
  description: mymoh1
Router#
```

This example displays the details of the music on hold profile the system is set to use as the default.

```
Router> show pbx moh default
number: 0
  name: built-in
  file: built-in
  system: used
  description: built-in
Router#
```

This example displays music on hold audio file storage space usage details.

```
Router> show pbx moh usage
total: 30 min.
used: 0 min.
free: 30 min.
usage: 0%
Router#
```

18.17.1.11 Display Call Transfer Settings

This example displays the maximum number of seconds the ISG50 waits for each digit input of a complete callee number after you press the flash key on the phone.

```
Router> show pbx callxfer digit-timeout
digit-timeout  : 5
Router#
```

This example displays whether or not the ISG50 allows a caller to transfer a current external call (via an outbound line group) to another extension.

```
Router> show pbx callxfer digit-timeout
local-handling : disable
Router#
```

18.17.1.12 Configure Call Transfer Settings

This example sets 10 seconds as the maximum time the ISG50 waits for each digit input of a complete callee number after you press the flash key on the phone.

```
Router> configure terminal
Router(config)# pbx callxfer digit-timeout 10
Router(config)# exit
Router#
```

This example sets the ISG50 to allow callers to transfer current external calls (via an outbound line group) to other extensions.

```
Router> configure terminal
Router(config)# pbx callxfer local-handling activate
Router(config)# exit
Router#
```

18.17.1.13 Configure System-wide Call Block Settings

This example turns on system-wide call blocking and adds 30XX (3000-3099) and 40XX (4000-4099) as black list rules.

```
Router# configure terminal
Router(config)# pbx call-block black-list
Router(System BlackList)# activate
Router(System BlackList)# rule 30XX
Router(System BlackList)# rule 40XX
Router(System BlackList)# show
  System-wide Black List:
rule0: 30XX
rule1: 40XX
Router(System BlackList)# exit
Router(config)# exit
Router#
```

This example removes all of the system-wide call blocking, black list rules.

```
Router#
Router# configure terminal
Router(config)# pbx call-block black-list
Router(System BlackList)# show
  System-wide Black List:
rule0: 40XX
rule1: 30XX
Router(System BlackList)# no rule all
Router(System BlackList)# show
  System-wide Black List:
Router(System BlackList)# exit
Router(config)# exit
Router#
```

This example turns on system-wide blocking of incoming calls that have no caller ID.

```
Router#
Router# configure terminal
Router(config)# pbx call-block anonymous-block activate
Router(config)# show pbx call-block
blacklist: yes
anonymous block: yes
Router(config)# exit
Router#
```

This example displays whether call blocking and anonymous call blocking are enabled.

```
Router# configure terminal
Router(config)# show pbx call-block
blacklist: yes
anonymous block: yes
Router(config)# exit
Router#
```

This example displays the system-wide call blocking black-list rules.

```
Router# configure terminal
Router(System BlackList)# show
  System-wide Black List:
rule0: 40XX
rule1: 30XX
Router(System BlackList)# exit
Router(config)# exit
Router#
```

This example shows another way to display the system-wide call blocking black-list rules.

```
Router# configure terminal
Router(config)# show pbx call-block black-list
  System-wide Black List:
rule0: 40XX
rule1: 30XX
Router(config)# exit
Router#
```

18.18 Call Recording Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 107 Input Values for Call Recording Commands

LABEL	DESCRIPTION
callrecord_quota	The maximum total number of minutes of call recording on the ISG50. 0-9999999999, 0 is unlimited.
trunk_name	The name of a trunk already configured in the ISG50. You can use 1-30 alphanumeric characters and the underscore.
exten_num	An extension number already configured in the ISG50.

The following table describes the commands for configuring call recording settings. Use the `enable` or `configure terminal` command to be able to use the show commands. You must use the

`configure terminal` command to enter the configuration mode before you can use the configuration commands.

Table 108 Call Recording Commands Summary

COMMAND	DESCRIPTION
`show pbx callrecord global`	Displays the global call recording configuration.
`pbx callrecord global`	Enters the sub-command mode for configuring the global call recording settings.
`quota` *`callrecord_quota`*	Sets the maximum total number of minutes of call recording on the ISG50.
`[no] on-demand activate`	Turns user-activated, on-demand call recording on or off.
`[no] prompt activate`	Sets whether or not the ISG50 plays a recording notification message at the beginning of calls that it records.
`beep-frequency <0 or 5-60>`	Sets the interval in seconds for the ISG50 to play a beep to remind the call participants about the recording. 0 means there is no beep.
`exit`	Leaves the sub-command mode.
`show pbx callrecord full-time`	Displays the full-time call recording configuration.
`pbx callrecord full-time`	Enters the sub-command mode for configuring the full-time call recording settings.
`[no] trunk` *`trunk_name`*	Sets whether or not the ISG50 records all of the specified trunk's outgoing and incoming calls.
`[no] extension` *`ext_number`*	Sets whether or not the ISG50 records all of the specified extension's outgoing and incoming calls.
`exit`	Leaves the sub-command mode.

18.18.1 Call Recording Command Examples

Here are some examples of displaying and configuring call recording settings.

18.18.1.1 Display Global Call Recording Settings

This example displays the call recording settings that apply to the whole system.

```
Router> show pbx callrecord global
callrecord quota: 0
callrecord usage: 0%
od activate: yes
prompt activate: yes
beep frequency: 3
Router#
```

18.18.1.2 Configure Global Call Recording Settings

This example sets the ISG50 to play the call recording reminder beep every 15 seconds and turns on on-demand call recording.

```
Router> configure terminal
Router(config)# pbx callrecord global
Router(callrecord-global)# beep-frequency 5
Router(callrecord-global)# on-demand activate
Router(callrecord-global)# exit
Router(config)#
```

18.18.1.3 Display Full-time Call Recording Settings

This example displays for which trunks and extensions the ISG50 records all outgoing and incoming calls.

```
Router> show pbx callrecord full-time
Index    Trunk
============================
1        siptk7101
Index    Extension
============================
1        7141
2        7132
3        7133
```

18.18.1.4 Configure Full-time Call Recording Settings

This example has the ISG50 record all outgoing and incoming calls for trunk siptk7101 and extensions 7141 and 7132.

```
Router(config)# pbx callrecord full-time
Router(callrecord-full-time)# trunk siptk7101
Router(callrecord-full-time)# extension 7141
Router(callrecord-full-time)# extension 7132
Router(config)# exit
Router#
```

18.19 Meet-me Conference Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 109 Input Values for Meet-me Conference Commands

LABEL	DESCRIPTION
meetme_num	The 3-10 digit extension callers dial to enter a specific conference room.
description2	The description for a conference room. Use 1-61 of the following characters [a-zA-Z0-9 '()+,/:=?;!*#@$_%-].

Table 109 Input Values for Meet-me Conference Commands (continued)

LABEL	DESCRIPTION
max_conference_seats	The maximum number of participants (3-5) for this conference room.
meetme_pincode	The 3-10 digit numeric password callers need to enter to join a conference room.

The following table describes the commands for configuring meet-me conference settings. Use the enable or configure terminal command to be able to use the show commands. You must use the configure terminal command to enter the configuration mode before you can use the configuration commands.

Table 110 Meet-me Conference Commands Summary

COMMAND	DESCRIPTION
[no] pbx meetme *meetme_num*	Enters the sub-command mode for configuring a conference room of the specified name. The no command deletes the specified conference room.
description *description2*	Adds a description for the conference room.
no description	Removes the conference room's description.
max-members *max_conference_seats*	Sets the maximum number of participants that can join the conference room.
no max-members	Removes the conference room's maximum members limit configuration.
pincode *meetme_pincode*	Sets the numeric password callers need to enter to join the conference room.
no pincode	Removes the conference room's password configuration.
exit	Leaves the sub-command mode.
show pbx meetme	Displays the meet-me conference configuration.

18.19.1 Meet-me Conference Command Examples

Here are some examples of displaying and configuring call recording settings.

18.19.1.1 Configure a Meet-me Conference Room

This example creates conference room number 1234 for up to 5 members and uses PIN code 1234 and a description of 'conference1'.

```
Router> configure terminal
Router(config)#pbx meetme 1234
Router(config)# description conference1
Router(config)# max-members 5
Router(config)# pincode 1234
Router(config)# exit
Router#
```

18.19.1.2 Display Meet-me Conference Room Settings

This example displays the meet-me conference room configuration.

```
Router> show pbx meetme
index: 0
  number: 1234
  pincode: 1234
  max members: 5
  description: conference1
Router#
```

18.20 Paging Group Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 111 Input Values for Paging Group Commands

LABEL	DESCRIPTION
pg_num	The 3-10 digit paging group number.
description2	The description for a conference room. Use 1-61 of the following characters [a-zA-Z0-9 '()+,/:=?;!*#@$_%-].
pg_time	The maximum number of seconds that a person can page a group of extensions. 10-3600 or 0 for unlimited.
pg_pincode	The 3-10 digit numeric password callers need to dial to call the extensions in this page group.
exten_num	An extension number already configured in the ISG50.

The following table describes the commands for configuring paging groups. Use the `enable` or `configure terminal` command to be able to use the show commands. You must use the `configure terminal` command to enter the configuration mode before you can use the configuration commands.

Table 112 Paging Group Commands Summary

COMMAND	DESCRIPTION
`[no] pbx paging-group` *pg_num*	Creates the specified paging group and enters the sub-command mode for configuring it. The `no` command deletes the specified paging group.
`description` *description2*	Adds a description for the paging group.
`no description`	Removes the paging group's description.
`max-paging-time` *pg_time*	Sets the maximum number of seconds that a person can page a group of extensions.
`no max-paging-time`	Removes the conference room's maximum paging time limit configuration.
`pincode` *pg_pincode*	Sets the numeric password callers need to dial to call the extensions in this page group.
`no pincode`	Removes the paging group's password configuration.
`[no] exten` *exten_num*	Adds or removes an extension.
`show available-exten`	Lists all of the extensions that you can add to the paging group.

Table 112 Paging Group Commands Summary (continued)

COMMAND	DESCRIPTION
`exit`	Leaves the sub-command mode.
`show pbx paging-group`	Displays the paging group configuration.
`show pbx paging-group` *pg_num* `exten`	Displays the specified paging group's extensions.

18.20.1 Paging Group Command Examples

Here are some examples of configuring and displaying paging groups.

18.20.1.1 Configure a Paging Group

This example creates paging group 9999 with a description of "Marketing" and adds extensions 1001 and 1002 as members.

```
Router> configure terminal
Router(config)#pbx paging-group 9999
Router(config)# description Marketing
Router(config)# exten 10001
Router(config)# exten 10002
Router(config)# exit
Router#
```

18.20.1.2 Display Paging Group Configuration

This example displays the paging groups and their settings.

```
Router> show pbx paging-group
index: 0
  number: 9999
  pincode:
  max_paging_time: 0
  description: Marketing
```

This example displays the Marketing paging group's extensions.

```
Router> show pbx paging-group 9999 exten

exten
==========================================================================
10001
10002
```

18.21 ACD Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 113 Input Values for ACD Commands

LABEL	DESCRIPTION
wrapup_time	The number of seconds that the ISG50 waits before re-queuing the agent to receive new incoming calls. You can enter a number from 1 to 86400.
agent_id	The 3-20 digit identification number of an agent.
agent_name	The name of an agent. You can use 1-32 alphanumeric characters and the underscore.
agent_pwd	An agent's 1-32 digit numeric password.
acd_description	A brief description. You can use 0-64 alphanumeric characters, the underscore (_) and the hyphen (-).
skill_num	The 3-20 digit phone number callers dial to reach the agents associated with this particular skill.
skill_name	The name of the skill. You can use 1-32 alphanumeric characters and the underscore.
skill_member	The ID number of an ACD agent member assigned to this skill.
music_name	The name of a music or ring tone file the ISG50 plays. You can use 2-19 alphanumeric characters, the underscore (_), the hyphen (-) and periods (.). The first character must be a letter.
menuname	The name of a skill menu to associate this skill with. You can use 2-19 alphanumeric characters and the underscore. The first character must be a letter.
ext_num	A 3-10 digit extension number.
aa_name	The name of an auto attendant system configured on the ISG50. You can use 0-29 alphanumeric characters and the underscore. The first character must be a letter.

The following table describes the commands for configuring Automatic Call Distribution (ACD) settings. Use the `enable` or `configure terminal` command to be able to use the show commands. You must use the `configure terminal` command to enter the configuration mode before you can use the configuration commands.

Table 114 ACD Commands Summary

COMMAND	DESCRIPTION
`pbx acd wrap-up-time {`*`wrapup_time`*`|default}`	Sets the number of seconds that the ISG50 waits before re-queuing the agent to receive new incoming calls. You can enter a number between 1 and 86400.
`show pbx acd wrap-up-time`	Displays the ACD wrap up time.
`no pbx acd agent {all |` *`agent_id`*`}`	Deletes the specified ACD agent or all of them.
`pbx acd agent [`*`agent_id`*`]`	Creates the specified ACD agent ID and enters the sub-command mode for configuring it.
`description` *`acd_description`*	Adds a description for the ACD agent.
`no description`	Removes the ACD agent's description.
`name` *`agent_name`*	Adds a name for the ACD agent.

Table 114 ACD Commands Summary (continued)

COMMAND	DESCRIPTION
password *agent_pwd*	Configures the numeric password the ACD agent uses to log into the ACD system.
show	Displays the ACD agent's settings.
exit	Leaves the sub-command mode.
no pbx acd skill {all | *skill_num*}	Deletes the specified ACD skill or all of them.
pbx acd skill [*skill_num*]	Creates the specified ACD skill and enters the sub-command mode for configuring it.
name *skill_name*	Adds a name for the ACD skill.
description *acd_description*	Adds a description for the ACD skill.
no description	Removes the ACD skill's description.
strategy {least-recent|round-robin|fewest-call|random|ring-all}	Sets how the ISG50 decides the ring order of extensions associated with this skill. least-recent: Rings the the least recently called agent associated with this skill. round-robin: Takes turns ringing each available agent associated with this skill. fewest-call: Rings the agents who have received the fewest number of calls, in order, from lowest to highest. random: Rings a random extension. ring-all: Rings all extensions at the same time until one answers.
wait-music *music_name*	Specifies the music or ring tone to play while a caller waits for an agent to pick up.
max-wait-call {<1..99999>|default}	Sets the maximum number of calls to be put on hold while calling the agents associated with this skill.
timeout {<1..99999>|default}	Sets the duration in seconds that the call to the agents associated with the skill can ring before timing out. Once a call times out, the defined timeout action applies. This timeout only applies to calls in the queue that have not yet been routed to a particular agent.
ring-member-timeout {<1..99999>|default}	Sets the duration in seconds that a call to a specific agent associated with this skill can ring before timing out. Once a call times out, it is routed to a different agent.
announce-freq {<0..99999>|default}	Sets the duration in seconds that the ISG50 waits before informing the caller on hold what their current position in the queue is. This report occurs periodically and continues until either the caller hangs up or the agent answers. "0" disables this option. For example, if a caller is second in the queue then the ISG50 may say, "You are currently call number 2" every 60 seconds.
no announce-freq	Removes the position report frequency setting.
periodic-freq {<0..99999>|default}	Sets the duration in seconds that the ISG50 waits before playing a previously uploaded audio file. This announcement occurs periodically and continues until either the caller hangs up or the agent answers. "0" disables this option. For example, a caller to the Acme Mail Order Company may hear, "Thank you for calling us. A service representative will be with you momentarily" every 240 seconds.
no periodic-freq	Removes the periodic announce frequency setting.

Table 114 ACD Commands Summary (continued)

COMMAND	DESCRIPTION
member *skill_member* priority <1..5>	Adds an ACD agent as a member of this skill. The ISG50 uses the priority to determine to which agent to route incoming calls first (1 highest to 5 lowest). If multiple agents share the same priority, then the ring strategy applies first to the highest priority group, then if all those agents are engaged it applies to the next group, and so on.
no member {*skill_member*|all}	Removes the specified member ACD agent or all of them from this skill.
_announce *music_name*	Specifies the audio file the ISG50 plays when the agent answers the phone, before connecting his phone to the call. It can be used to announce which skill the incoming caller requires, which is especially useful when one agent is associated with multiple skills. For example, if an agent is associated with the skills “English” and “Spanish”, then the announce audio file played before receiving a call sent to him by way of the English skill may say “This caller speaks English.”
no announce	Removes the announce file setting.
_periodic *music_name*	Specifies the periodic announce audio file the ISG50 plays to a caller on hold every X number of seconds and can be used to keep the caller apprised of their status. For example, a caller may hear the following every 30 seconds: “Thank you for your patience. Please continue holding.”
no periodic	Removes the periodic announce file setting.
show	Displays the ACD skill’s settings.
exit	Leaves the sub-command mode.
show pbx acd skill {all | *skill_num*}	Displays the settings of the specified ACD skill or lists all of the ACD skills.
show pbx acd skill *skill_num* member	Lists the specified ACD skill’s member ACD agents.
pbx acd skill [*skill_num*] advanced	Enters the sub-command mode for configuring advanced settings for the specified ACD skill.
no-login-action {[hangup]|[backup *skill_name*]|[page *ext_num*]|[hunt *ext_num*]|[aa *aa_name*]|[extension *ext_num*]|[voicemail *ext_num*]}	Sets how the ISG50 handles calls sent to this skill when none of the skill’s agents are logged in. Possible actions are: hangup: Disconnect the call. backup: Send the call to the specified skill. page: Forward the call to the specified page group. hunt: Forward the call to the specified hunt group. aa: Route the call back to the specified auto attendant system. extension: Route the call to the specified extension. voicemail: Forward the call to the specified extension’s voice mail.

Table 114 ACD Commands Summary (continued)

COMMAND	DESCRIPTION
no-available-action {[join]|[hangup]|[backup *skill_name*]|[page *ext_num*]|[hunt *ext_num*]|[aa *aa_name*]|[extension *ext_num*]|[voicemail *ext_num*]}	Sets how the ISG50 handles calls sent to this skill when none of the skill's agents are available to take a call. Possible actions are: join: Put the call back in the queue for other extensions within this skill. hangup: Disconnect the call. backup: Send the call to the specified skill. page: Forward the call to the specified page group. hunt: Forward the call to the specified hunt group. aa: Route the call back to the specified auto attendant system. extension: Route the call to the specified extension. voicemail: Forward the call to the specified extension's voice mail.
timeout-action {[no-timeout]|[hangup]|[backup *skill_name*]|[page *ext_num*]|[hunt *ext_num*]|[aa *aa_name*]|[extension *ext_num*]|[voicemail *ext_num*]}	Sets how the ISG50 handles calls sent to this skill that time out. Possible actions are: no-timeout: Keep the caller on the line indefinitely while the extension is rung. hangup: Disconnect the call. backup: Send the call to the specified skill. page: Forward the call to the specified page group. hunt: Forward the call to the specified hunt group. aa: Route the call back to the specified auto attendant system. extension: Route the call to the specified extension. voicemail: Forward the call to the specified extension's voice mail.
menu *menuname*	Associate this skill with the specified skill menu.
no menu	Removes any association from this skill to a skill menu.
exit	Leaves the sub-command mode.
show pbx acd realtime agent status	Displays the current ACD agent status.
show pbx acd realtime waiting calls	Displays the current ACD skill waiting calls.
no pbx acd hunt {all | *skill_num*}	Deletes the specified ACD hunt group or all of them.
pbx acd hunt [*skill_num*]	Creates the specified ACD hunt group and enters the sub-command mode for configuring it.
name *skill_name*	Adds a name for the ACD hunt group.
description *acd_description*	Adds a description for the ACD hunt group.
no description	Removes the ACD hunt group's description.

Table 114 ACD Commands Summary (continued)

COMMAND	DESCRIPTION
strategy {least-recent|round-robin|fewest-call|random|ring-all}	Sets how the ISG50 decides the ring order of extensions associated with this hunt group. least-recent: Rings the the least recently called agent associated with this skill. round-robin: Takes turns ringing each available agent associated with this skill. fewest-call: Rings the agents who have received the fewest number of calls, in order, from lowest to highest. random: Rings a random extension. ring-all: Rings all extensions at the same time until one answers.
wait-music *music_name*	Specifies the music or ring tone to play while a caller waits for an agent to pick up.
max-wait-call {<1..99999>|default}	Sets the maximum number of calls to be put on hold while calling the agents associated with this hunt group.
timeout {<1..99999>|default}	Sets the duration in seconds that the call to the agents associated with the hunt group can ring before timing out. Once a call times out, the defined timeout action applies. This timeout only applies to calls in the queue that have not yet been routed to a particular agent.
ring-member-timeout {<1..99999>|default}	Sets the duration in seconds that a call to a specific agent associated with this hunt group can ring before timing out. Once a call times out, it is routed to a different agent.
member *skill_member* priority <1..5>;	Adds an ACD agent as a member of this hunt group. The ISG50 uses the priority to determine to which agent to route incoming calls first (1 highest to 5 lowest). If multiple agents share the same priority, then the ring strategy applies first to the highest priority group, then if all those agents are engaged it applies to the next group, and so on.
no member {*skill_member*|all};	Removes the specified member ACD agent or all of them from this hunt group.
exit	Leaves the sub-command mode.
show pbx acd hunt {all | *skill_num*}	Displays the settings of the specified ACD hunt group or lists all of them.
show pbx acd hunt *skill_num* member	Lists the specified ACD hunt group's member ACD agents.
pbx acd hunt [*skill_num*] advanced	Enters the sub-command mode for configuring advanced settings for the specified ACD hunt group.
timeout-action {[no-timeout]|[hangup]|[backup *skill_name*]|[hunt *ext_num*]|[aa *aa_name*]|[extension *ext_num*]|[voicemail *ext_num*]}	Sets how to handle calls sent to this hunt group that time out. Possible actions are: no-timeout: Keep the caller on the line indefinitely while the extension is rung. hangup: Disconnect the call. backup: Send the call to the specified skill. hunt: Forward the call to the specified hunt group. aa: Route the call back to the specified auto attendant system. extension: Route the call to the specified extension. voicemail: Forward the call to the specified extension's voice mail.
exit	Leaves the sub-command mode.
no pbx acd skill-menu {all | *menuname*}	Deletes the specified ACD skill menu or all of them.

Table 114 ACD Commands Summary (continued)

COMMAND	DESCRIPTION
pbx acd skill-menu [*menuname*]	Creates the specified ACD skill menu and enters the sub-command mode for configuring it.
description *acd_description*	Adds a description for the ACD skill menu.
no description	Removes the ACD skill menu's description.
action-id <0..9> {*skill_num*|exit}	Sets the number a caller presses to engage the associated action. A number can only be used once within a skill menu. Set the action to go to the specified skill number or exit the skill menu.
no action-id {<0..9>|all}	Deletes the specified ACD skill menu action or all of the ACD skill menu's actions.
show	Displays the ACD skill menu's settings.
exit	Leaves the sub-command mode.
show pbx acd skill-menu {all | *menuname*}	Displays the settings of the specified ACD skill menu or all of them.
show pbx acd skill-menu *menuname* code	Lists the specified ACD skill menu's configured action codes.

18.21.1 ACD Command Examples

Here are some examples of configuring and displaying ACD settings.

18.21.1.1 Configure Global ACD Settings

This example configures the global wrap-up time limit to 300 seconds and then displays the setting.

```
Router# configure terminal
Router(config)# pbx acd wrap-up-time 300
Router(config)#
Router(config)# show pbx acd wrap-up-time
wrap-up-time: 300
Router(config)# exit
Router#
```

18.21.1.2 Configure an ACD Agent

This example configures ACD agent number 1111, sets the name and password to 1111, and adds a description.

```
Router# configure terminal
Router(config)# pbx acd agent 1111
Router(pbx-acd-agent)# name 1111
Router(pbx-acd-agent)# password 1111
Router(pbx-acd-agent)# description it is agent1
Router(pbx-acd-agent)# exit
Router(config)#
```

18.21.1.3 Display the ACD Agents

This example displays the configured ACD agents.

```
Router# configure terminal
Router(config)# show pbx acd agent all
agent id: 1111
  name: 1111
  password: 1111
  description:  it is agent1
  create-time: Mon May  2 08:34:57 2011
Router(config)#
```

18.21.1.4 Remove an ACD Agent

This example deletes ACD agent number 1111.

```
Router# configure terminal
Router(config)# no pbx acd agent 1111
Router(config)#
```

18.21.1.5 Configure an ACD Skill

This example configures ACD skill number 4411, sets the name to 4411, and adds a description.

```
Router# configure terminal
Router(config)# pbx acd skill 4411
Router(pbx-acd-skill)# name 4411
Router(pbx-acd-skill)# member 1111 priority 1
Router(pbx-acd-skill)# description It is skill 4411
Router(pbx-acd-skill)# exit
Router(config)#
```

18.21.1.6 Display the ACD Skills

This example displays the configured ACD skills.

```
Router# configure terminal
Router(config)# show pbx acd skill all
skill number: 4411
  name: 4411
  description:  It is skill 4411
  skill-menu:
  ring-strategy: least-recent
  no-login-action: page
  nl-param: 5511
  no-available-action: extension
  na-param: 6702
  timeout-action: voicemail
  to-param: 6703
  waiting-music: default
  max-waiting-call: 64
  timeout: 180
  ring-member-timeout: 15
  announce-freq: 60
  periodic-freq: 60
  announce: false
  periodic: false
  create-time: Mon May  2 08:51:43 2011
  member: 1111 priority 1
Router(config)#
```

18.21.1.7 Remove an ACD Skill

This example deletes ACD skill number 4411.

```
Router# configure terminal
Router(config)# no pbx acd skill 4411
Router(config)#
```

18.21.1.8 Configure an ACD Skill's Advanced Settings

This example configures ACD skill number 4411 to forward calls to page group 5511 when there are no member agents logged in; forward calls to extension 6702 when none of the skill's agents are available to take a call, and forward calls that time out to extension 6703's voice mail.

```
Router# configure terminal
Router(config)# pbx acd skill 4411 advanced
Router(pbx-acd-skill-advanced)# no-login-action page 5511
Router(pbx-acd-skill-advanced)# no-available-action extension 6702
Router(pbx-acd-skill-advanced)# timeout-action voicemail 6703
Router(pbx-acd-skill-advanced)# exit
Router(config)#
```

18.21.1.9 Display the Real-time Status of the ACD Agents

This example displays the current status for the ACD agents.

```
Router# configure terminal
Router(config)# show pbx acd realtime agent status
agentID: 1111
  skillNum: 4411
  agentName: 1111
  priority: 1
  extension:
  status: Logoff
Router(config)#
```

18.21.1.10 Display the Waiting Calls for all the ACD Skills

This example displays the current list of waiting calls for all the ACD skills.

```
Router# configure terminal
Router(config)# show pbx acd realtime waiting calls
SkillNum             Caller               WaitTime        EnteredTime
================================================================================
4411
Router(config)#
```

18.21.1.11 Configure an ACD Hunt Group

This example configures ACD hunt group 6611, sets the name to 6611, adds extension 6702 as a priority 1 member, and sets the maximum number of calls that can be waiting for the hunt group to 90.

```
Router# configure terminal
Router(config)# pbx acd hunt 6611
Router(pbx-acd-hunt)# name 661
Router(pbx-acd-hunt)# member 6702 priority 1
Router(pbx-acd-hunt)# max-wait-call 90
Router(pbx-acd-hunt)# exit
Router(config)#
```

18.21.1.12 Display the ACD Hunt Groups

This example displays the configured ACD hunt groups.

```
Router# configure terminal
Router(config)# show pbx acd hunt all
hunt number: 6611
  name: 6611
  description:
  skill-menu:
  ring-strategy: least-recent
  no-login-action: aa
  nl-param: default
  no-available-action: aa
  na-param: default
  timeout-action: hangup
  to-param: default
  waiting-music: default
  max-waiting-call: 90
  timeout: 180
  ring-member-timeout: 15
  announce-freq: 0
  periodic-freq: 0
  create-time: Mon May  2 09:44:22 2011
  member: 6702 priority 1
Router(config)#
```

18.21.1.13 Remove an ACD Hunt Group

This example deletes the 6611 ACD hunt group.

```
Router# configure terminal
Router(config)# no pbx acd hunt 6611
Router(config)#
```

18.21.1.14 Configure an ACD Hunt Group's Advanced Settings

This example configures ACD hunt group 6611 to hang up calls that time out.

```
Router# configure terminal
Router(config)# pbx acd hunt 6611 advanced
Router(pbx-acd-hunt-advanced)# timeout-action hangup
Router(pbx-acd-hunt-advanced)# exit
Router(config)#
```

18.21.1.15 Configure an ACD Skill Menu

This example configures ACD skill menu jason and sets the action ID 1 to forward th call to extension 4411.

```
Router# configure terminal
Router(config)# pbx acd skill-menu jason
Router(pbx-acd-skill-menu)# action-id 1 4411
Router(pbx-acd-skill-menu)# exit
Router(config)#
```

18.22 Sound File Commands

The following table describes the commands for setting the default PBX language, working with the PBX language sound files, and setting the extension number the ISG50 records from for creating audio files for PBX functions. Use the `enable` or `configure terminal` command to be able to use the show commands. You must use the `configure terminal` command to enter the configuration mode before you can use the configuration commands.

Table 115 Sound File PBX Commands Summary

COMMAND	DESCRIPTION
`show pbx system-sound default`	Displays the default language set for the PBX.
`show pbx system-sound all`	Displays the PBX language names.
`pbx system-sound default` *`sound_language`*	Sets the default language for the PBX functions.
`[no] pbx system-sound language` *`sound_language`*	Adds or removes the specified language for PBX functions. Use the Web Configurator to upload language files.
`show pbx record-exten`	Displays which extension the ISG50 is set to record from for creating audio files to use for PBX functions.
`pbx record-exten` *`pbx_exten_num`*	Sets the 3-10 digit extension number the ISG50 records from for creating audio files to use for the PBX functions.
`no pbx record-exten`	Removes the setting of which extension number the ISG50 records from for creating audio files to use for the PBX functions.

18.22.1 Sound File Command Examples

Here are some examples of configuring and displaying sound file settings.

18.22.1.1 Show the Default PBX Language

This example shows how to display the language the PBX uses as its default.

```
Router> show pbx system-sound default
default: factory
```

18.22.1.2 Add a PBX Language

This example shows how to add German for the PBX system sounds. Use the Web Configurator to upload language files.

```
Router> configure terminal
Router(config)# pbx system-sound language German
Router(config)#exit
Router#
```

18.22.1.3 Show the PBX Extension for Recordings

Here is how to display which extension the ISG50 uses for recording audio files for PBX functions.

```
Router> show pbx record-exten
extension: 1003
```

18.22.1.4 Set the PBX Extension for Recordings

This example sets the ISG50 to use extension 1003 for recording audio files for PBX functions.

```
Router> configure terminal
Router(config)# pbx record-exten 1003
Router(config)# exit
Router#
```

18.23 Auto Provision Commands

The following table identifies values used in these commands. Other input values are discussed with the corresponding commands.

Table 116 Input Values for Auto Provision Commands

LABEL	DESCRIPTION
autoprov_extension	The 1-30 digit extension number of a supported SIP client for which you want to use auto provisioning.
autoprov_mac	The hexadecimal (`aa:bb:cc:dd:ee:ff` for example) MAC address of an extension upon which to use auto provisioning.
autoprov_phone_name	A type of phone that supports the ISG50's auto provisioning. `{snom_300|snom_320|snom_360|snom_370|snom_820|snom_870|snom_m3|ZyXEL_V310|ZyXEL_V311|ZyXEL_V510|NotSpecified}`
autoprov_url	The firmware upgrade URL for auto provision.
autoprov_xml	Uploaded XML 0-32 character file name.

Table 116 Input Values for Auto Provision Commands (continued)

LABEL	DESCRIPTION
autoprov_policy	Sets how to apply auto provisioning to an extension. {auto_update | ask_for_update | settings_only | never_update} auto_update: Automatically update this extension's firmware and/or configuration whenever an update of is available. ask_for_update: Update this extension's firmware and/or configuration whenever it checks for an update. settings_only: Do not update this extension's firmware, only update its configuration. never_update: Do not update this extension's firmware, and do not update its configuration.
autoprov_fkey_index	The feature key code for auto provision (0|1|2|3|4|5|6|7|8|9|10|11). This corresponds to the special feature keys on a snom VoIP phone.
autoprov_feature_type	The feature key type for auto provision (one|line|group-pickup|direct-pickup|call-transfer|voicemail|followme-on|followme-off|agent-login|agent-pause|mobile-extension-on|mobile-extension-off|mobile-extension-auto|call-recording-on-demand).

The following table describes the commands for using auto provision to configure supported SIP clients. Use the enable or configure terminal command to be able to use the show commands. You must use the configure terminal command to enter the configuration mode before you can use the configuration commands.

Table 117 Auto Provision Commands Summary

COMMAND	DESCRIPTION
show pbx auto-provision *autoprov_extension*	Displays the auto provision settings for the specified extension.
show pbx auto-provision extension-list	Lists the auto provision settings for the PBX extensions.
show pbx auto-provision feature-key	Lists the settings of the special feature keys on the auto provision extensions' VoIP phones.
show pbx auto-provision firmware	Shows the configured firmware upgrade file locations.
show pbx auto-provision config	Shows the configuration files for the auto provision extensions.
pbx auto-provision *autoprov_extension*	Enters the sub-command mode for configuring the specified auto provisioning extension.
phone-mac *autoprov_mac*	Specify the hexadecimal (aa:bb:cc:dd:ee:ff for example) MAC address of the SIP client that receives configuration settings from the ISG50 for this extension.
update-policy *autoprov_policy*	Sets how to apply auto provisioning to this extension.
phone-name *autoprov_phone_name*	Sets the phone type for auto provisioning to this extension.
exit	Leaves the sub-command mode.
no pbx auto-provision *autoprov_extension* {system|customize}	Removes the specified extension's system configuration profile or custom configuration file.
pbx auto-provision feature-key	Enters the sub-command mode for configuring the feature key settings for the auto provisioned SIP clients.

Table 117 Auto Provision Commands Summary (continued)

COMMAND	DESCRIPTION
pbx auto-provision feature-key *autoprov_fkey_index autoprov_feature_type* {on|off}	Enables or disables the specified key code index for the specified feature key.
exit	Leaves the sub-command mode.
pbx auto-provision firmware	Enters the sub-command mode for configuring the locations of firmware upgrade files for the auto provisioned SIP clients.
autoprov_phone_name autoprov_url	Specifies the firmware upgrade URL auto provisioning uses for the specified type of device. You can find this URL and any other upgrade information at the product page on the official snom website.
exit	Leaves the sub-command mode.
no pbx auto-provision firmware *autoprov_phone_name*	Turns off auto provisioning firmware upgrade for the specified type of device.
pbx auto-provision autoprov-status {enable|disable}	Tuns auto provisioning on or off.

18.23.1 Auto Provision Command Examples

Here are some examples of configuring PBX auto provision.

18.23.1.1 Configure an Extension for Auto Provision

This example shows how to configure extension 8801 for auto provision.

```
Router> configure terminal
Router(config)#pbx auto-provision 8801
Router(pbx auto-provision-8801)# phone-mac 112233445566
Router(pbx auto-provision-8801)# phone-name snom_300
Router(pbx auto-provision-8801)# update-policy auto_update
Router(pbx auto-provision-8801)#exit
Router(config)#exit
Router#
```

18.24 Voice Mail Configuration Commands

The following table describes the commands that configure global voice mail settings. Use the `enable` or `configure terminal` command to be able to use the show commands. You must use the `configure terminal` command to enter the configuration mode before you can use the configuration commands.

Table 118 Voice Mail Configuration Commands Summary

COMMAND	DESCRIPTION
pbx voicemail	Enters the sub-command mode for configuring voice mail.
maxlength {<1..90>|default}	Specify the maximum number of seconds for each voice mail message.

Table 118 Voice Mail Configuration Commands Summary (continued)

COMMAND	DESCRIPTION
quota {<1..600>|default}	Specify the maximum number of seconds for all voice mail messages for each extension. When a user hits this limit the ISG50 will no longer save voice mail messages.
body *body_string*	Enter up to 350 alphanumeric characters (a-z, A-Z, 1-0, all punctuation included) as the body text for e-mails sent out by the ISG50 to notify users of pending voice mails. You can also use the following ISG50-specific variables to include custom information about the voice mail: • DUR: This is the duration of the voice mail in hh:mm:ss format (hours, minutes, and seconds). • MSGNUM: This is the queue number of the voice mail in the mailbox. The more voice mails you have received, the higher this number. • MAILBOX: This is the telephone extension number of the mailbox owner. • CALLERID: This is the telephone extension of the person who left the voice mail. • DATE: This is the timestamp of when the voice mail was received.
subject *subject_string*	Enter up to 150 alphanumeric characters (a-z, A-Z, 1-0, all punctuation included) as the subject line for e-mails sent out by the ISG50 to notify users of pending voice mails.
show	Displays the voice mail configuration.
exit	Leaves the sub-command mode.

18.24.1 Voice Mail Configuration Command Examples

Here are some examples of configuring global voice mail settings.

18.24.1.1 Configure Voice Mail Settings

This example sets the maximum length of individual voice mail messages to 90 seconds, the maximum number of voice mail messages per extension to 300, and sets a subject line and body text for voice mails.

```
Router# configure terminal
Router(config)# pbx voicemail
Router(pbx-voicemail)# maxlength 90
Router(pbx-voicemail)# quota 300
Router(pbx-voicemail)# subject This is a test.
Router(pbx-voicemail)# body send for your information.
Router(pbx-voicemail)# exit
Router(config)#
```

18.24.1.2 Show Voice Mail Settings

This example displays the current voice mail configuration.

```
Router> configure terminal
Router(config)# show pbx voicemail
maxlength: 90
quota: 300
maxlength: 90
quota: 300
subject: This is a test.
body: send for your information.
```

18.25 Phonebook Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 119 Input Values for Phonebook Commands

LABEL	DESCRIPTION
phbook_name	The name of the phonebook entry. You can use 0-50 alphanumeric characters, the underscore (_), the hyphen (-) and periods (.).
phbook_num	The 0-20 digit, numeric telephone number for the phonebook entry.
e_mail	An e-mail address for the phonebook entry. You can use 1-80 alphanumeric characters, underscores (_), or hyphens (-), and you must use the @ character.
phbook_logon_name	The logon name value for the phonebook entry. An e-mail address. You can use 0-64 alphanumeric characters, underscores (_), periods (.), hyphens (-), and the @ character.
phbook_val	The country or department for the phonebook entry. You can use 0-60 alphanumeric characters, underscores (_), periods (.), and hyphens (-).
password	The password for the LDAP server. You can use 1-32 alphanumeric and ;‘~!@#$%^&()_+[]{}’,.=-characters.
string_128	A string less than 128 characters.

The following table describes the commands for configuring phonebook settings and entries. Use the `enable` or `configure terminal` command to be able to use the show commands. You must use the `configure terminal` command to enter the configuration mode before you can use the configuration commands.

Table 120 Phonebook Commands Summary

COMMAND	DESCRIPTION
`[no] pbx phonebook local <1..200>`	Creates the specified local phonebook entry and enters the sub-command mode for configuring it. The `no` command deletes the local phonebook entry.
`name` *phbook_name*	Specify the name of the local phonebook entry.
`no name`	Removes the local phonebook entry’s name configuration.
`ext` *phbook_num*	Specify the extension value of the local phonebook entry.

Table 120 Phonebook Commands Summary (continued)

COMMAND	DESCRIPTION
no ext	Removes the local phonebook entry's extension value configuration.
home *phbook_num*	Specify the home telephone number of the local phonebook entry.
no home	Removes the local phonebook entry's home telephone number configuration.
mobile *phbook_num*	Specify the mobile telephone number of the local phonebook entry.
no mobile	Removes the local phonebook entry's mobile telephone number configuration.
mail *e_mail*	Specify the e-mail address of the local phonebook entry.
no mail	Removes the local phonebook entry's e-mail address configuration.
logon-name *phbook_logon_name*	Specify the logon name of the local phonebook entry.
no logon-name	Removes the local phonebook entry's logon name configuration.
country *phbook_val*	Specify the country of the local phonebook entry.
no country	Removes the local phonebook entry's country configuration.
department *phbook_val*	Specify the department of the local phonebook entry.
no department	Removes the local phonebook entry's department configuration.
exit	Leaves the sub-command mode.
show pbx phonebook local	Displays the details of the local phonebook entries.
pbx phonebook ldap server	Enters the sub-command mode for configuring the LDAP server settings.
[no] activate	Enable or disable the LDAP phonebook feature.
host {*hostname*|IPv4}	Specify the address of the LDAP server.
no host	Removes the LDAP phonebook's LDAP server address configuration.
port <1..65535>	Specify the port number the LDAP server uses for sending the phonebook to the ISG50.
no port	Removes the LDAP phonebook's port number configuration.
[no] ssl	Set whether or not the ISG50 uses SSL when connecting to the LDAP server.
password *password*	Specify the password for using the LDAP server.
no password	Removes the LDAP phonebook's password configuration.
basedn *string_128*	Specify the string identifying the location on the LDAP server where the information you need for your phonebook is stored.
no basedn	Removes the LDAP phonebook's Base DN configuration.
binddn *string_128*	Specify the login name of the LDAP server.

Table 120 Phonebook Commands Summary (continued)

COMMAND	DESCRIPTION
no binddn	Removes the LDAP phonebook's LDAP server login name configuration.
search-time-limit <1..300>	Specify the longest that the ISG50 can attempt to connect to the LDAP server. If there is no response after this time, the ISG50 stops trying to connect and waits until the next day's update time.
no search-time-limit	Removes the time limit configuration for connecting to the LDAP server.
[no] auto-update	Has the ISG50 automatically update the LDAP phonebook with the LDAP database.
update-time hour <0..23> minute <0..59>	Specify the time in hour and minute format at which the ISG50 updates the LDAP phonebook with the LDAP database.
no update-time	Removes the configuration for regularly updating the LDAP phonebook with the LDAP database.
exit	Leaves the sub-command mode.
pbx phonebook ldap attr name *phbook_val*	Specify the attribute name in the LDAP database to map to the Name field of the LDAP phonebook.
no pbx phonebook ldap attr name	Removes the Name mapping configuration of the LDAP phonebook.
pbx phonebook ldap attr ext *phbook_val*	Specify the attribute name in the LDAP database to map to the Ext. field of the LDAP phonebook.
no pbx phonebook ldap attr ext	Removes the Ext. mapping configuration of the LDAP phonebook.
pbx phonebook ldap attr home *phbook_val*	Specify the attribute name in the LDAP database to map to the Home field of the LDAP phonebook.
no pbx phonebook ldap attr home	Removes the Home mapping configuration of the LDAP phonebook.
pbx phonebook ldap attr mobile *phbook_val*	Specify the attribute name in the LDAP database to map to the Mobile field of the LDAP phonebook.
no pbx phonebook ldap attr mobile	Removes the Mobile mapping configuration of the LDAP phonebook.
pbx phonebook ldap attr mail *phbook_val*	Specify the attribute name in the LDAP database to map to the E-mail field of the LDAP phonebook.
no pbx phonebook ldap attr mail	Removes the E-mail mapping configuration of the LDAP phonebook.
pbx phonebook ldap attr logon-name *phbook_val*	Specify the attribute name in the LDAP database to map to the Logon Name field of the LDAP phonebook.
no pbx phonebook ldap attr logon-name	Removes the Logon Name mapping configuration of the LDAP phonebook.
pbx phonebook ldap attr country *phbook_val*	Specify the attribute name in the LDAP database to map to the Country field of the LDAP phonebook.
no pbx phonebook ldap attr country	Removes the Country mapping configuration of the LDAP phonebook.
pbx phonebook ldap attr department *phbook_val*	Specify the attribute name in the LDAP database to map to the Department field of the LDAP phonebook.
no pbx phonebook ldap attr department	Removes the Department mapping configuration of the LDAP phonebook.
pbx phonebook ldap update	Update the LDAP phonebook from the LDAP database.

Table 120 Phonebook Commands Summary (continued)

COMMAND	DESCRIPTION
show pbx phonebook ldap last-update	Shows when the LDAP phonebook was last updated from the LDAP server.
show pbx phonebook ldap server	Displays the LDAP server settings.
show pbx phonebook ldap attr	Displays the LDAP phonebook field to server attribute mapping.
pbx phonebook selection	Enters the sub-command mode for specifying which phonebooks to transfer to the ZyXEL or snom VoIP phones.
[no] ldap	Sets whether or not to transfer the LDAP phonebook.
[no] local	Sets whether or not to transfer the local phonebook.
[no] extensions	Sets whether or not to transfer the ISG50's extensions.
exit	Leaves the sub-command mode.
show pbx phonebook selection	Displays which phonebooks the ISG50 transfers to the ZyXEL or snom VoIP phones.

18.25.1 Phonebook Command Examples

Here are some examples of configuring phonebook settings.

18.25.1.1 Configure a Local Phonebook Entry

This example adds a local phonebook entry named AAA with a home telephone number of 555-5555.

```
Router> configure terminal
Router(config)#pbx phonebook local 1
Router(config)# name AAA
Router(config)# home 5555555
Router(config)#exit
Router#
```

18.25.1.2 Display the Local Phonebook Entries

This example displays the details of the local phonebook entries.

```
Router> show pbx phonebook local
Phonebook: 1
  Name: AAA
  Ext:
  Home: 5555555
  Mobile:
  Mail:
  Logon Name:
  Country:
  Department
```

18.25.1.3 Configure LDAP Phonebook Server Settings

This example specifies the address of the LDAP server and the login name and password to use with it.

```
configure IPPBX LDAP server setting
Router> configure terminal
Router(config)#pbx phonebook ldap server
Router(config)# host ldap.zyxel.com
Router(config)# binddn 1234
Router(config)# password 1234
Router(config)#exit
Router#
```

18.25.1.4 Configure LDAP Phonebook Search Filter Settings

This example specifies the LDAP database attribute to map the Name field of the LDAP phonebook.

```
configure IPPBX LDAP name attribute setting
Router> configure terminal
Router(config)#pbx phonebook ldap attr name displayName
Router#
```

18.25.1.5 Update LDAP Phonebook from LDAP Server

This example updates the LDAP phonebook from the LDAP server's database.

```
Router> configure terminal
Router(config)#pbx phonebook ldap update
Router#
```

18.25.1.6 Display the Last LDAP Phonebook Update Time

This example shows when the LDAP phonebook was last updated from the LDAP server.

```
Router> show pbx phonebook ldap last-update
time: 2011/04/20 06:10:14
```

18.25.1.7 Display the LDAP Server Settings

This example displays the LDAP server settings.

```
Router> show pbx phonebook ldap server
activate: off
host: ldap.zyxel.com
port: 389
ssl: off
password: 1234
basedn:
binddn: 1234
search-time-limit: 5
auto-update: off
update-time-hour: 0
update-time-minute: 0
```

18.25.1.8 Display the LDAP Attribute Mapping

This example displays the LDAP phonebook field to server attribute mapping.

```
Router> show pbx phonebook ldap attr
name: displayName
ext: telephoneNumber
home: homePhone
mobile: mobile
mail: mail
logon-name: userPrincipalName
country: c
department: department
```

18.25.1.9 Select the Phonebooks to Share

This example puts the local phonebook and all the ISG50's extensions into the phonebook for VoIP phone extensions.

```
Router> configure terminal
Router(config)#pbx phonebook selection
Router(config)# local
Router(config)# extensions
Router(config)#exit
Router#
```

18.25.1.10 Display the Phonebook Selection

This example displays which phonebooks the ISG50 transfers to the ZyXEL or snom VoIP phones.

```
To show the detail of configuration status
Router> show pbx phonebook selection
ldap: no
local: yes
extensions: yes
```

18.26 Office Hour Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 121 Input Values for Office Hour Commands

LABEL	DESCRIPTION
dow	A day of the week. {sun|mon|tue|wed|thu|fri|sat}
time	Time range. HH:MM-HH:MM (HH: 01-23, MM: 00-59)
date	A date. MM/DD (MM: 01-12, DD: 01-31
pbx_description	A description using 0-62 alphanumeric characters (A-Z, a-z, 0-9) and spaces.

The following table describes the commands for configuring office hour settings. Use the `enable` or `configure terminal` command to be able to use the show commands. You must use the `configure terminal` command to enter the configuration mode before you can use the configuration commands.

Table 122 Office Hour Commands Summary

COMMAND	DESCRIPTION
`pbx system`	Enters the sub-command mode for specifying the office hour days of the week.
`[no] office-hour dow` *dow*	Sets a day of the week to be in the office hours. The `no` command removes it.
`[no] office-hour dow` *dow* `time` *time*	Configures the office hour time range for the specified day of the week. The `no` command removes it.
`no office-hour dow` *dow* `time all`	Removes all of the office hour time configuration for the specified day of the week.
`[no] office-hour holiday` *date*	Adds a date to the office hour holiday list or removes it.
`no office-hour holiday all`	Removes all dates from the office hour holiday list.
`office-hour holiday` *date* `description` *pbx_description*	Adds a description for the specified office hour holiday.
`no office-hour holiday` *date* `description`	Removes the description for the specified office hour holiday.
`show office-hour [dow|dow-time|holiday]`	Displays the office hour configuration. You can optionally show just the days of the week, days of the week with time ranges, and holidays.
`office-hour apply {default|to-authority|to-extension}`	Specifies the policy for applying the office hour configuration. `default`: set the system office hour configuration to the factory default (enable all days of the week settings, erase all time ranges and holidays). `to-authority`: apply the system office hour configuration to all authority groups. `to-extension`: apply the system office hour configuration to all authority groups and all extensions.

Table 122 Office Hour Commands Summary (continued)

COMMAND	DESCRIPTION
exit	Leaves the sub-command mode.
show pbx system office-hour [dow|dow-time|holiday]	Displays the office hour configuration. You can optionally show just the days of the week, days of the week with time ranges, and holidays.

18.26.1 Office Hour Command Examples

Here are some examples of configuring office hour settings.

18.26.1.1 Enable Office Hour for a Day of the Week

This example sets Mondays to be part of the office hours.

```
Router# configure terminal
Router(config)# pbx system
Router(sys-officehour)# office-hour dow mon
Router(sys-officehour)# exit
Router(config)# exit
Router#
```

18.26.1.2 Disable Office Hour for a Day of the Week

This example sets Monday to not be part of the office hours.

```
To disable the DOW—mon
Router# configure terminal
Router(config)# pbx system
Router(sys-officehour)# no office-hour dow mon
Router(sys-officehour)# exit
Router(config)# exit
Router#
```

18.26.1.3 Set Office Hour Time for a Day of the Week

This example sets 08:00-17:30 on Mondays to be part of the office hours.

```
Router# configure terminal
Router(config)# pbx system
Router(sys-officehour)# office-hour dow mon time 08:00-17:30
Router(sys-officehour)# exit
Router(config)# exit
Router#
```

18.26.1.4 Remove an Office Hour Time for a Day of the Week

This example removes 08:00-17:30 on Mondays from the office hours.

```
Router# configure terminal
Router(config)# pbx system
Router(sys-officehour)# no office-hour dow mon time 08:00-17:30
Router(sys-officehour)# exit
Router(config)# exit
Router#
```

18.26.1.5 Remove All Office Hour Time for a Day of the Week

This example removes all time on Mondays from the office hours.

```
Router# configure terminal
Router(config)# pbx system
Router(sys-officehour)# no office-hour dow mon time all
Router(sys-officehour)# exit
Router(config)# exit
Router#
```

18.26.1.6 Set an Office Hour Holiday

This example sets 01/01 to be a holiday in the office hour configuration.

```
Router# configure terminal
Router(config)# pbx system
Router(sys-officehour)# office-hour holiday 01/01
Router(sys-officehour)# exit
Router(config)# exit
Router#
```

18.26.1.7 Remove an Office Hour Holiday

This example removes 01/01 from the office hour holiday list.

```
Router(config)# pbx system
Router(sys-officehour)# no office-hour holiday 01/01
Router(sys-officehour)# exit
Router(config)# exit
Router#
```

18.26.1.8 Remove All Office Hour Holidays

This example removes all of the holidays from the office hour configuration.

```
Router# configure terminal
Router(config)# pbx system
Router(sys-officehour)# no office-hour holiday all
Router(sys-officehour)# exit
Router(config)# exit
Router#
```

18.26.1.9 Set an Office Hour Holiday with a Description

This example sets 01/01 with the description “1st holiday” to be a holiday in the office hour configuration.

```
Router# configure terminal
Router(config)# pbx system
Router(sys-officehour)# office-hour holiday 01/01 description 1st holiday
Router(sys-officehour)# exit
Router(config)# exit
Router#
```

18.26.1.10 Remove an Office Hour Holiday Description

This example removes the description from the 01/01 office hour holiday.

```
Router# configure terminal
Router(config)# pbx system
Router(sys-officehour)# no office-hour holiday 01/01 description
Router(sys-officehour)# exit
Router(config)# exit
Router#
```

18.26.1.11 Display the Office Hour Configuration

This example shows all the days of the week, time ranges, and holiday office hour configuration.

```
Router(config)# show pbx system office-hour
Sun: disable
Mon: enable
Tue: enable
Wed: enable
Thu: enable
Fri: enable
Sat: disable
Sequence Sun Time
================================================================================
Sequence Mon Time
================================================================================
1       08:00-17:30
Sequence Tue Time
================================================================================
1       08:00-17:30
Sequence Wed Time
================================================================================
1       08:00-17:00
Sequence Thu Time
================================================================================
1       08:00-17:30
Sequence Fri Time
================================================================================
1       08:00-17:30
Sequence Sat Time
================================================================================
Date   Description
================================================================================
01/01  1st holiday
```

18.26.1.12 Apply the Office Hour Configuration

This example applies the current system office hour configuration to all created authority groups and all created extensions.

```
Router# configure terminal
Router(config)# pbx system
Router(sys-officehour)# office-hour apply to-extension
Router(sys-officehour)# exit
Router(config)# exit
Router#
```

18.27 PBX Diagnostics Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 123 Input Values for PBX Diagnostics Commands

LABEL	DESCRIPTION
pbx_debug_level	The debug level. <1-3>
port	The location of the PSTN port. <1-5>

The following table describes the commands for debugging PBX functions. Use the enable command to be able to use the show commands.

Table 124 PBX Diagnostics Commands Summary

COMMAND	DESCRIPTION
debug pbx call progress start level *pbx_debug_level*	Sets the debug level and capture PBX diagnostic information.
debug pbx call progress stop	Stop capturing PBX diagnostic information and display it.
debug pbx call progress with-sip start level *pbx_debug_level*	Sets the debug level and capture PBX diagnostic information with SIP information.
debug pbx call progress with-sip stop	Stop capturing PBX diagnostic information with SIP information and display it.
debug pbx show calls	Displays the status of calls on the PBX system.
debug pbx show uptime	Displays how long the PBX system has been running.
debug pbx show channels	Displays the status of channels on the PBX system.
debug pbx show database status	Displays the status of the PBX database system.
debug pbx show sip-setting	Displays the PBX system configuration.
show ip pbx server status	Displays the status of the PBX-related server.
debug voice-sniffer *port* <start | stop>	Captures voice packets to help you debug voice quality.

18.27.1 PBX Diagnostics Command Examples

Here are some examples of capturing PBX diagnostic information.

18.27.1.1 Capture PBX Diagnostic Information

This example sets debug level 1 and captures and displays PBX diagnostic information. First you set the debug level and start capturing. Then you make a call and finally you use the stop command.

```
Router# debug pbx call progress start level 1
Maximum debug interval is 180 seconds.
Router# debug pbx call progress stop
[May  4 09:13:37] VERBOSE[4692] logger.c:  Asterisk Queue Logger restarted
[May  4 09:13:37] VERBOSE[4692] asterisk.c:     -- Remote UNIX connection
disconnected
[May  4 09:16:37] VERBOSE[4728] asterisk.c:     -- Remote UNIX connection
disconnected
Router#
```

18.27.1.2 Capture PBX SIP Diagnostic Information

This example sets SIP debug level 1 and captures and displays PBX SIP diagnostic information.

```
Router# debug pbx call progress with-sip start level 1
Maximum debug interval is 180 seconds.
Router# debug pbx call progress with-sip stop
[May  4 09:39:31] VERBOSE[2711] asterisk.c:     -- Remote UNIX connection
[May  4 09:39:31] VERBOSE[4886] config.c:   == Parsing '/etc/asterisk-cs/
logger.conf': [May  4 09:39:31] VERBOSE[4886] config.c:   == Found
[May  4 09:39:31] VERBOSE[4886] logger.c:  Asterisk Queue Logger restarted
[May  4 09:39:31] VERBOSE[4886] asterisk.c:     -- Remote UNIX connection
disconnected
Router#
```

18.27.1.3 Display Call Status

This example displays the status of calls on the PBX system.

```
Router# debug pbx show calls
1 of 75 max active call ( 1.33% of capacity)
3 calls processed
Router#
```

18.27.1.4 Display Uptime

This example displays how long the PBX system has been running.

```
Router# debug pbx show uptime
System uptime: 2 hours, 20 minutes, 25 seconds
Last reload: 2 hours, 20 minutes, 25 seconds
Router#
```

18.27.1.5 Display Channel Status

This example displays the status of channels on the PBX system.

```
Router# debug pbx show channels
Channel              Location             State   Application(Data)
SIP/1000-00000003    unavail@paa_vm_diale Up      BackGround(paa/paa-dial-exten-
1 active channel
1 of 75 max active call ( 1.33% of capacity)
4 calls processed
Router#
```

18.27.1.6 Display Database Status

This example displays the status of the PBX database system.

```
Router# debug pbx show database status
database is alive
Router#
```

18.27.1.7 Display PBX Configuration

This example displays the PBX system configuration.

```
Router# debug pbx show sip-setting
Global Settings:
----------------
  UDP Bindaddress:        0.0.0.0:5060
  TCP SIP Bindaddress:    Disabled
  TLS SIP Bindaddress:    Disabled
  Videosupport:           Yes
  Textsupport:            No
  Ignore SDP sess. ver.:  No
  AutoCreate Peer:        No
  Match Auth Username:    No
  Allow unknown access:   Yes
  Allow subscriptions:    Yes
  Allow overlap dialing:  Yes
  Allow promsic. redir:   No
  Enable call counters:   No
  SIP domain support:     No
  Realm. auth:            No
  Our auth realm          default
  Use domains as realms:  No
  Call to non-local dom.: Yes
  URI user is phone no:   No
  Always auth rejects:    Yes
  Direct RTP setup:       No
  User Agent:             ZyXEL IPPBX
  SDP Session Name:       ISG
  SDP Owner Name:         root
  Reg. context:           (not set)
  Regexten on Qualify:    No
  Caller ID:              ISG
  From: Domain:
  Record SIP history:     Off
  Call Events:            Off
  Auth. Failure Events:   Off
  T.38 support:           Yes
  T.38 EC mode:           Redundancy
  T.38 MaxDtgrm:          400
  SIP realtime:           Enabled
  Qualify Freq :          60000 ms
  Q.850 Reason header:    No
Network QoS Settings:
--------------------------
  IP ToS SIP:             CS0
  IP ToS RTP audio:       CS0
  IP ToS RTP video:       CS0
  IP ToS RTP text:        CS0
  802.1p CoS SIP:         4
  802.1p CoS RTP audio:   5
  802.1p CoS RTP video:   6
  802.1p CoS RTP text:    5
  Jitterbuffer enabled:   No
  Jitterbuffer forced:    No
  Jitterbuffer max size:  -1
  Jitterbuffer resync:    -1
  Jitterbuffer impl:
  Jitterbuffer log:       No
```

(continued)

```
Network Settings:
-------------------------
  SIP address remapping:  Disabled, no localnet list
  Externhost:             <none>
  externaddr:               (null)
  Externrefresh:          10

Global Signalling Settings:
-------------------------
  Codecs:                 0x2c194d
(g723|ulaw|alaw|g726|slin|g729|g722|h261|h263|h264)
  Codec Order:            ulaw:20,alaw:20,g722:20,g723:30,g726:20,g729:20,slin:20
  Relax DTMF:             No
  RFC2833 Compensation:   No
  Symmetric RTP:          No
  Compact SIP headers:    No
  RTP Keepalive:          0 (Disabled)
  RTP Timeout:            0 (Disabled)
  RTP Hold Timeout:       0 (Disabled)
  MWI NOTIFY mime type:   application/simple-message-summary
  DNS SRV lookup:         No
  Pedantic SIP support:   Yes
  Reg. min duration       60 secs
  Reg. max duration:      3600 secs
  Reg. default duration:  120 secs
  Outbound reg. timeout:  20 secs
  Outbound reg. attempts: 0
  Notify ringing state:   Yes
    Include CID:          No
  Notify hold state:      No
  SIP Transfer mode:      open
  Max Call Bitrate:       384 kbps
  Auto-Framing:           No
  Outb. proxy:            <not set>
  Session Timers:         Refuse
  Session Refresher:      pbx
  Session Expires:        1800 secs
  Session Min-SE:         90 secs
  Timer T1:               500
  Timer T1 minimum:       100
  Timer B:                32000
  No premature media:     Yes
  Max forwards:           70

Default Settings:
-----------------
  Allowed transports:     UDP
  Outbound transport:     UDP
  Context:                default
  Force rport:            No
  DTMF:                   rfc2833
  Qualify:                0
  Use ClientCode:         No
  Progress inband:        Never
  Language:
  MOH Interpret:          default
  MOH Suggest:
  Voice Mail Extension:   ISG
```

(continued)

```
Realtime SIP Settings:
----------------------
  Realtime Peers:         Yes
  Realtime Regs:          No
  Cache Friends:          Yes
  Update:                 Yes
  Ignore Reg. Expire:     No
  Save sys. name:         No
  Auto Clear:             120 (Disabled)

----
Router#
```

18.27.1.8 Display PBX Server Status

This example displays the status of the PBX-related server.

```
Router# show ip pbx server status
sip_active    : yes
sip_port      : 5060

database_active    : yes
database_port      : 5432

Router#
```

18.27.1.9 Capture Voice Packets

This example captures voice packets to help you debug voice quality. After capturing voice packets you need to use FTP to get the voice packet files. Use the admin account to log into your ISG50 and get “/voice-sniffer/voice-sniffer.zip”.

```
Router# debug voice-sniffer 1 start
Router# debug voice-sniffer 1 stop
```

19

User/Group

This chapter describes how to set up user accounts, user groups, and user settings for the ISG50. You can also set up rules that control when users have to log in to the ISG50 before the ISG50 routes traffic for them.

19.1 User Account Overview

A user account defines the privileges of a user logged into the ISG50. User accounts are used in firewall rules, in addition to controlling access to configuration and services in the ISG50.

19.1.1 User Types

There are the types of user accounts the ISG50 uses.

Table 125 Types of User Accounts

TYPE	ABILITIES	LOGIN METHOD(S)
Admin Users		
Admin	Change ISG50 configuration (web, CLI)	WWW, TELNET, SSH, FTP
Limited-Admin	Look at ISG50 configuration (web, CLI) Perform basic diagnostics (CLI)	WWW, TELNET, SSH
Access Users		
User	Access network services Browse user-mode commands (CLI)	WWW, TELNET, SSH
Guest	Access network services	WWW
Ext-User	See Section 19.2 on page 270.	WWW

Note: The default **admin** account is always authenticated locally, regardless of the authentication method setting. (See Chapter 24 on page 294 for more information about authentication methods.)

19.2 User/Group Commands Summary

The following table identify the values required for many username/groupname commands. Other input values are discussed with the corresponding commands.

Table 126 username/groupname Command Input Values

LABEL	DESCRIPTION
username	The name of the user (account). You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
groupname	The name of the user group. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. It cannot be the same as the user name.

The following sections list the username/groupname commands.

19.2.1 User Commands

The first table lists the commands for users.

Table 127 username/groupname Commands Summary: Users

COMMAND	DESCRIPTION
show username [*username*]	Displays information about the specified user or about all users set up in the ISG50.
username *username* nopassword user-type {admin | guest | limited-admin | user}	Creates the specified user (if necessary), disables the password, and sets the user type for the specified user.
username *username* password *password* user-type {admin | guest | limited-admin | user}	Creates the specified user (if necessary); enables and sets the password; and sets the user type for the specified user. *password*: You can use 1-63 printable ASCII characters, except double quotation marks (“) and question marks (?).
username *username* user-type ext-user	Creates the specified user (if necessary) and sets the user type to **Ext-User**.
no username *username*	Deletes the specified user.
username rename *username username*	Renames the specified user (first *username*) to the specified username (second *username*).
username *username* [no] description *description*	Sets the description for the specified user. The no command clears the description. *description*: You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 60 characters long.
username *username* [no] logon-time-setting <default | manual>	Sets the account to use the factory default lease and reauthentication times or custom ones.

Table 127 username/groupname Commands Summary: Users (continued)

COMMAND	DESCRIPTION
username *username* [no] logon-lease-time <0..1440>	Sets the lease time for the specified user. Set it to zero to set unlimited lease time. The no command sets the lease time to five minutes (regardless of the current default setting for new users).
username *username* [no] logon-re-auth-time <0..1440>	Sets the reauthorization time for the specified user. Set it to zero to set unlimited reauthorization time. The no command sets the reauthorization time to thirty minutes (regardless of the current default setting for new users).

19.2.2 User Group Commands

This table lists the commands for groups.

Table 128 username/groupname Commands Summary: Groups

COMMAND	DESCRIPTION
show groupname [*groupname*]	Displays information about the specified user group or about all user groups set up in the ISG50.
[no] groupname *groupname*	Creates the specified user group if necessary and enters sub-command mode. The no command deletes the specified user group.
[no] description *description*	Sets the description for the specified user group. The no command clears the description for the specified user group.
[no] groupname *groupname*	Adds the specified user group (second *groupname*) to the specified user group (first *groupname*).
[no] user *username*	Adds the specified user to the specified user group.
show	Displays information about the specified user group.
groupname rename *groupname groupname*	Renames the specified user group (first *groupname*) to the specified group-name (second *groupname*).

19.2.3 User Setting Commands

This table lists the commands for user settings, except for forcing user authentication.

Table 129 username/groupname Commands Summary: Settings

COMMAND	DESCRIPTION
show users default-setting {all | user-type {admin|user|guest|limited-admin|ext-user}}	Displays the default lease and reauthentication times for the specified type of user accounts.
users default-setting [no] logon-lease-time <0..1440>	Sets the default lease time (in minutes) for each new user. Set it to zero to set unlimited lease time. The no command sets the default lease time to five.

Table 129 username/groupname Commands Summary: Settings (continued)

COMMAND	DESCRIPTION
`users default-setting [no] logon-re-auth-time <0..1440>`	Sets the default reauthorization time (in minutes) for each new user. Set it to zero to set unlimited reauthorization time. The no command sets the default reauthorization time to thirty.
`users default-setting [no] user-type <admin |ext-user|guest|limited-admin|user>`	Sets the default user type for each new user. The no command sets the default user type to user.
`show users retry-settings`	Displays the current retry limit settings for users.
`[no] users retry-limit`	Enables the retry limit for users. The no command disables the retry limit.
`[no] users retry-count <1..99>`	Sets the number of failed login attempts a user can have before the account or IP address is locked out for lockout-period minutes. The no command sets the retry-count to five.
`[no] users lockout-period <1..65535>`	Sets the amount of time, in minutes, a user or IP address is locked out after retry-count number of failed login attempts. The no command sets the lockout period to thirty minutes.
`show users simultaneous-logon-settings`	Displays the current settings for simultaneous logins by users.
`[no] users simultaneous-logon {administration | access} enforce`	Enables the limit on the number of simultaneous logins by users of the specified account-type. The no command disables the limit, or allows an unlimited number of simultaneous logins.
`[no] users simultaneous-logon {administration | access} limit <1..1024>`	Sets the limit for the number of simultaneous logins by users of the specified account-type. The no command sets the limit to one.
`show users update-lease-settings`	Displays whether or not access users can automatically renew their lease time.
`[no] users update-lease automation`	Lets users automatically renew their lease time. The no command prevents them from automatically renewing it.
`show users idle-detection-settings`	Displays whether or not users are automatically logged out, and, if so, how many minutes of idle time must pass before they are logged out.
`[no] users idle-detection`	Enables logging users out after a specified number of minutes of idle time. The no command disables logging them out.
`[no] users idle-detection timeout <1..60>`	Sets the number of minutes of idle time before users are automatically logged out. The no command sets the idle-detection timeout to three minutes.

19.2.3.1 User Setting Command Examples

The following commands show the current settings for the number of simultaneous logins.

```
Router# configure terminal
Router(config)# show users simultaneous-logon-settings
enable simultaneous logon limitation for administration account: yes
maximum simultaneous logon per administration account          : 1
enable simultaneous logon limitation for access account        : yes
maximum simultaneous logon per access account                  : 3
```

19.2.4 Force User Authentication Commands

This table lists the commands for forcing user authentication.

Table 130 username/groupname Commands Summary: Forcing User Authentication

COMMAND	DESCRIPTION
`[no] force-auth activate`	Enables force user authentication that force users to log in to the ISG50 before the ISG50 routes traffic for them. The no command means the user authentication is not required.
`force-auth default-rule authentication {required | unnecessary} {no log | log [alert]}`	Sets the default authentication policy that the ISG50 uses on traffic that does not match any exceptional service or other authentication policy. `required`: Users need to be authenticated. They must manually go to the ISG50's login screen. The ISG50 will not redirect them to the login screen. `unnecessary`: Users do not need to be authenticated. `no log | log [alert]`: Select whether to have the ISG50 generate a log (`log`), log and alert (`log alert`) or not (`no log`) for packets that match this default policy.
`force-auth [no] exceptional-service` *`service_name`*	Sets a service which you want users to be able to access without user authentication. The `no` command removes the specified service from the exceptional list.
`force-auth policy <1..1024>`	Creates the specified condition for forcing user authentication, if necessary, and enters sub-command mode. The conditions are checked in sequence, starting at 1. See Table 131 on page 274 for the sub-commands.
`force-auth policy append`	Creates a new condition for forcing user authentication at the end of the current list and enters sub-command mode. See Table 131 on page 274 for the sub-commands.
`force-auth policy insert <1..1024>`	Creates a new condition for forcing user authentication at the specified location, renumbers the other conditions accordingly, and enters sub-command mode. See Table 131 on page 274 for the sub-commands.

Table 130 username/groupname Commands Summary: Forcing User Authentication (continued)

COMMAND	DESCRIPTION
`force-auth policy delete <1..1024>`	Deletes the specified condition. To modify a condition, you can insert a new condition (N) and then delete the one (N+1) that you want to modify.
`force-auth policy flush`	Deletes every condition.
`force-auth policy move <1..1024> to <1..1024>`	Moves the specified condition to the specified location and renumbers the other conditions accordingly.
`show force-auth activation`	Displays whether forcing user authentication is enabled or not.
`show force-auth exceptional-service`	Displays services that users can access without user authentication.
`show force-auth policy {<1..1024> | all}`	Displays details about the policies for forcing user authentication.

19.2.4.1 force-auth Sub-commands

The following table describes the sub-commands for several force-auth policy commands. Note that not all rule commands use all the sub-commands listed here.

Table 131 force-auth policy Sub-commands

COMMAND	DESCRIPTION
`[no] activate`	Activates the specified condition. The `no` command deactivates the specified condition.
`[no] authentication {force | required}`	Select the authentication requirement for users when their traffic matches this policy. The `no` command means user authentication is not required. `force`: Users need to be authenticated and the ISG50 automatically display the login screen when users who have not logged in yet try to send HTTP traffic. `required`: Users need to be authenticated. They must manually go to the login screen. The ISG50 will not redirect them to the login screen.
`[no] description` *`description`*	Sets the description for the specified condition. The `no` command clears the description. *`description`*: You can use alphanumeric and `()+/:=?!*#@$_%-` characters, and it can be up to 60 characters long.
`[no] destination {`*`address_object`* `|` *`group_name`*`}`	Sets the destination criteria for the specified condition. The `no` command removes the destination criteria, making the condition effective for all destinations.
`[no] force`	Forces users to log in to the ISG50 if the specified condition is satisfied. The `no` command means that users do not log in to the ISG50.
`[no] schedule` *`schedule_name`*	Sets the time criteria for the specified condition. The `no` command removes the time criteria, making the condition effective all the time.

Table 131 force-auth policy Sub-commands (continued)

COMMAND	DESCRIPTION
[no] source {*address_object* | *group_name*}	Sets the source criteria for the specified condition. The no command removes the source criteria, making the condition effective for all sources.
show	Displays information about the specified condition.

19.2.4.2 Force Authentication Policy Insert Command Example

The following commands show how to insert a force authentication policy at position 1 of the checking order. This policy applies endpoint secruity policies and uses the following settings:

- Activate: yes
- Description: EPS-on-LAN
- Source: use address object “LAN1_SUBNET”
- Destination: use address object “DMZ_Servers”
- User Authentication: required
- Schedule: no specified
-

```
Router# configure terminal
Router(config)# force-auth policy insert 1
Router(config-force-auth-1)# activate
Router(config-force-auth-1)# description EPS-on-LAN
Router(config-force-auth-1)# source LAN1_SUBNET
Router(config-force-auth-1)# destination DMZ_Servers
Router(config-force-auth-1)# authentication force
Router(config-force-auth-1)# no schedule
Router(config-force-auth-1)# exit
```

19.2.5 Additional User Commands

This table lists additional commands for users.

Table 132 username/groupname Commands Summary: Additional

COMMAND	DESCRIPTION
show users {*username* | all | current}	Displays information about the users logged onto the system.
show lockout-users	Displays users who are currently locked out.
unlock lockout-users *ip* | console	Unlocks the specified IP address.
users force-logout *ip* | *username*	Logs out the specified logins.

19.2.5.1 Additional User Command Examples

The following commands display the users that are currently logged in to the ISG50 and forces the logout of all logins from a specific IP address.

```
Router# configure terminal
Router(config)# show users all
No.  Name                           Type            From            Service
     Session Time    Idle Time       Lease Timeout   Re-Auth. Timeout
=============================================================================
1    admin                          admin          192.168.1.34    http/https
     00:33:27        unlimited       23:45:18        23:26:33
2    admin                          admin          192.168.1.34    http/https
     00:14:31        unlimited       23:48:38        23:45:29
3    admin                          admin          172.23.23.83    http/https
     00:04:07        unlimited       23:58:32        23:55:53
4    admin                           admin           172.23.23.83    telnet
     00:03:30        unlimited       23:59:59        23:56:30
Router(config)# users force-logout 192.168.1.34
Logout user 'admin'(from 192.168.1.34): OK
Logout user 'admin'(from 192.168.1.34): OK
Total 2 users have been forced logout
Router(config)# show users all
No.  Name                           Type            From            Service
     Session Time    Idle Time       Lease Timeout   Re-Auth. Timeout
=============================================================================
1    admin                          admin          172.23.23.83    http/https
     00:04:31        unlimited       23:58:08        23:55:29
2    admin                           admin           172.23.23.83    telnet
     00:03:54        unlimited       24:00:00        23:56:06
```

The following commands display the users that are currently locked out and then unlocks the user who is displayed.

```
Router# configure terminal
Router(config)# show lockout-users
No.  Username Tried                  From            Lockout Time Remaining
=============================================================================
No.  From            Failed Login Attempt    Record Expired Timer
=============================================================================
1    172.23.23.60    2                       46

Router(config)# unlock lockout-users 172.23.23.60
User from 172.23.23.60 is unlocked
Router(config)# show lockout-users
No.  Username Tried                  From            Lockout Time Remaining
=============================================================================
No.  From            Failed Login Attempt    Record Expired Timer
=============================================================================
```

20

Addresses

This chapter describes how to set up addresses and address groups for the ISG50.

20.1 Address Overview

Address objects can represent a single IP address or a range of IP addresses. Address groups are composed of address objects and other address groups.

You can create IP address objects based on an interface's IP address, subnet, or gateway. The ISG50 automatically updates these objects whenever the interface's IP address settings change. This way every rule or setting that uses the object uses the updated IP address settings. For example, if you change the LAN1 interface's IP address, the ISG50 automatically updates the corresponding interface-based, LAN1 subnet address object. So any configuration that uses the LAN1 subnet address object is also updated.

Address objects and address groups are used in dynamic routes, firewall rules, and VPN connection policies. Please see the respective sections for more information about how address objects and address groups are used in each one.

Address groups are composed of address objects and address groups. The sequence of members in the address group is not important.

20.2 Address Commands Summary

The following table describes the values required for many address object and address group commands. Other values are discussed with the corresponding commands.

Table 133 Input Values for Address Commands

LABEL	DESCRIPTION
object_name	The name of the address. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
group_name	The name of the address group. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
interface_name	The name of the interface. Use ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your ISG50 model.

The following sections list the address object and address group commands.

20.2.1 Address Object Commands

This table lists the commands for address objects.

Table 134 address-object Commands: Address Objects

COMMAND	DESCRIPTION
`show address-object [object_name]`	Displays information about the specified address or all the addresses.
`address-object object_name {ip | ip_range | ip_subnet | interface-ip | interface-subnet | interface-gateway} {interface_name}`	Creates the specified address object using the specified parameters. *ip_range*: <1..255>.<0..255>.<0..255>.<1..255>-<1..255>.<0..255>.<0..255>.<1..255> *ip_subnet*: <1..255>.<0..255>.<0..255>.<0..255>/<1..32> *interface*: You only need to specify an interface with you create an object based on an interface.
`no address-object object_name`	Deletes the specified address.
`address-object rename object_name object_name`	Renames the specified address (first *object_name*) to the second *object_name*.

20.2.1.1 Address Object Command Examples

The following example creates three address objects and then deletes one.

```
Router# configure terminal
Router(config)# address-object A0 192.168.1.1
Router(config)# address-object A1 192.168.1.1-192.168.1.20
Router(config)# address-object A2 192.168.1.0/24
Router(config)# show address-object
Object name                    Type    Address                          Ref.
=============================================================================
A0                             HOST    192.168.1.1                        0
A1                             RANGE   192.168.1.1-192.168.1.20      0
A2                             SUBNET 192.168.1.0/24                   0
Router(config)# no address-object A2
Router(config)# show address-object
Object name                    Type    Address                          Ref.
=============================================================================
A0                             HOST    192.168.1.1                        0
A1                             RANGE   192.168.1.1-192.168.1.20      0
```

20.2.2 Address Group Commands

This table lists the commands for address groups.

Table 135 object-group Commands: Address Groups

COMMAND	DESCRIPTION
`show object-group address [group_name]`	Displays information about the specified address group or about all address groups.
`[no] object-group address group_name`	Creates the specified address group if necessary and enters sub-command mode. The `no` command deletes the specified address group.
`[no] address-object object_name`	Adds the specified address to the specified address group. The `no` command removes the specified address from the specified group.
`[no] object-group group_name`	Adds the specified address group (second *group_name*) to the specified address group (first *group_name*). The `no` command removes the specified address group from the specified address group.
`[no] description description`	Sets the description to the specified value. The `no` command clears the description. *description*: You can use alphanumeric and `()+/:=?!*#@$_%-` characters, and it can be up to 60 characters long.
`object-group address rename group_name group_name`	Renames the specified address group from the first *group_name* to the second *group_name*.

20.2.2.1 Address Group Command Examples

The following commands create three address objects A0, A1, and A2 and add A1 and A2 to address group RD.

```
Router# configure terminal
Router(config)# address-object A0 192.168.1.1
Router(config)# address-object A1 192.168.1.2-192.168.2.20
Router(config)# address-object A2 192.168.3.0/24
Router(config)# object-group address RD
Router(group-address)# address-object A1
Router(group-address)# address-object A2
Router(group-address)# exit
Router(config)# show object-group address
Group name                      Reference
Description
================================================================================
TW_TEAM                         5

RD                              0

Router(config)# show object-group address RD
Object/Group name               Type   Reference
================================================================================
A1                              Object 1
A2                              Object 1
```

21

Services

Use service objects to define TCP applications, UDP applications, and ICMP messages. You can also create service groups to refer to multiple service objects in other features.

21.1 Services Overview

See the appendices in the web configurator's User Guide for a list of commonly-used services.

21.2 Services Commands Summary

The following table describes the values required for many service object and service group commands. Other values are discussed with the corresponding commands.

Table 136 Input Values for Service Commands

LABEL	DESCRIPTION
group_name	The name of the service group. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
object_name	The name of the service. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

The following sections list the service object and service group commands.

21.2.1 Service Object Commands

The first table lists the commands for service objects.

Table 137 service-object Commands: Service Objects

COMMAND	DESCRIPTION
`show service-object [`*`object_name`*`]`	Displays information about the specified service or about all the services.
`no service-object` *`object_name`*	Deletes the specified service.
`service-object` *`object_name`* `{tcp | udp} {eq <1..65535> | range <1..65535> <1..65535>}`	Creates the specified TCP service or UDP service using the specified parameters.

Table 137 service-object Commands: Service Objects (continued)

COMMAND	DESCRIPTION
service-object *object_name* icmp *icmp_value*	Creates the specified ICMP message using the specified parameters. *icmp_value*: <0..255> | alternate-address | conversion-error | echo | echo-reply | information-reply | information-request | mask-reply | mask-request | mobile-redirect | parameter-problem | redirect | router-advertisement | router-solicitation | source-quench | time-exceeded | timestamp-reply | timestamp-request | unreachable
service-object *object_name* protocol <1..255>	Creates the specified user-defined service using the specified parameters.
service-object rename *object_name object_name*	Renames the specified service from the first *object_name* to the second *object_name*.

21.2.1.1 Service Object Command Examples

The following commands create four services, displays them, and then removes one of them.

```
Router# configure terminal
Router(config)# service-object TELNET tcp eq 23
Router(config)# service-object FTP tcp range 20 21
Router(config)# service-object ICMP_ECHO icmp echo
Router(config)# service-object MULTICAST protocol 2
Router(config)# show service-object
Object name                 Protocol         Minmum port  Maxmum port  Ref.
=========================================================================TELNET
TCP               23            23             0
FTP                           TCP             20             21             0
ICMP_ECHO                    ICMP             0              0              0
MULTICAST                    2                 0              0              0
Router(config)# no service-object ICMP_ECHO
Router(config)# show service-object
Object name                 Protocol         Minmum port  Maxmum port  Ref.
=========================================================================TELNET
TCP               23            23             0
FTP                           TCP             20             21             0
MULTICAST                    2                 0              0              0
```

21.2.2 Service Group Commands

The first table lists the commands for service groups.

Table 138 object-group Commands: Service Groups

COMMAND	DESCRIPTION
show object-group service *group_name*	Displays information about the specified service group.
[no] object-group service *group_name*	Creates the specified service group if necessary and enters sub-command mode. The no command removes the specified service group.

Table 138 object-group Commands: Service Groups (continued)

COMMAND	DESCRIPTION
[no] service-object *object_name*	Adds the specified service to the specified service group. The no command removes the specified service from the specified group.
[no] object-group *group_name*	Adds the specified service group (second *group_name*) to the specified service group (first *group_name*). The no command removes the specified service group from the specified service group.
[no] description *description*	Sets the description to the specified value. The no command removes the description. *description*: You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 60 characters long.
object-group service rename *group_name group_name*	Renames the specified service group from the first *group_name* to the second *group_name*.

21.2.2.1 Service Group Command Examples

The following commands create service ICMP_ECHO, create service group SG1, and add ICMP_ECHO to SG1.

```
Router# configure terminal
Router(config)# service-object ICMP_ECHO icmp echo
Router(config)# object-group service SG1
Router(group-service)# service-object ICMP_ECHO
Router(group-service)# exit
Router(config)# show service-object ICMP_ECHO
Object name                    Protocol        Minmum port  Maxmum port  Ref.
================================================================================
ICMP_ECHO                        ICMP             8            8            1
Router(config)# show object-group service SG1
Object/Group name                Type   Reference
================================================================================
ICMP_ECHO                        Object 1
```

22

Schedules

Use schedules to set up one-time and recurring schedules for policy routes and firewall rules.

22.1 Schedule Overview

The ISG50 supports two types of schedules: one-time and recurring. One-time schedules are effective only once, while recurring schedules usually repeat. Both types of schedules are based on the current date and time in the ISG50.

Note: Schedules are based on the current date and time in the ISG50.

One-time schedules begin on a specific start date and time and end on a specific stop date and time. One-time schedules are useful for long holidays and vacation periods.

Recurring schedules begin at a specific start time and end at a specific stop time on selected days of the week (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday). Recurring schedules always begin and end in the same day. Recurring schedules are useful for defining the workday and off-work hours.

22.2 Schedule Commands Summary

The following table describes the values required for many schedule commands. Other values are discussed with the corresponding commands.

Table 139 Input Values for Schedule Commands

LABEL	DESCRIPTION
object_name	The name of the schedule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
time	24-hour time, hours and minutes; <0..23>:<0..59>.

The following table lists the schedule commands.

Table 140 schedule Commands

COMMAND	DESCRIPTION
show schedule-object	Displays information about the schedules in the ISG50.
no schedule-object *object_name*	Deletes the schedule object.

Table 140 schedule Commands (continued)

COMMAND	DESCRIPTION
schedule-object *object_name date time date time*	Creates or updates a one-time schedule. *date*: yyyy-mm-dd date format; yyyy-<01..12>-<01..31>
schedule-object *object_name time time* [*day*] [*day*] [*day*] [*day*] [*day*] [*day*] [*day*]	Creates or updates a recurring schedule. *day*: 3-character day of the week; sun | mon | tue | wed | thu | fri | sat

22.2.1 Schedule Command Examples

The following commands create recurring schedule SCHEDULE1 and one-time schedule SCHEDULE2 and then delete SCHEDULE1.

```
Router# configure terminal
Router(config)# schedule-object SCHEDULE1 11:00 12:00 mon tue wed thu fri
Router(config)# schedule-object SCHEDULE2 2006-07-29 11:00 2006-07-31 12:00
Router(config)# show schedule-object
Object name                    Type      Start/End                        Ref.
=============================================================================
SCHEDULE1                       Recurring 11:00/12:00 ===MonTueWedThuFri=== 0
SCHEDULE2                       Once      2006-07-29 11:00/2006-07-31 12:00 0

Router(config)# no schedule-object SCHEDULE1
Router(config)# show schedule-object
Object name                    Type      Start/End                        Ref.
=============================================================================
SCHEDULE2                       Once      2006-07-29 11:00/2006-07-31 12:00 0
```

23

AAA Server

This chapter introduces and shows you how to configure the ISG50 to use external authentication servers.

23.1 AAA Server Overview

You can use an AAA (Authentication, Authorization, Accounting) server to provide access control to your network.

The following lists the types of authentication server the ISG50 supports.

- Local user database

  The ISG50 uses the built-in local user database to authenticate administrative users logging into the ISG50's web configurator or network access users logging into the network through the ISG50. You can also use the local user database to authenticate VPN users.
- Directory Service (LDAP/AD)

  LDAP (Lightweight Directory Access Protocol)/AD (Active Directory) is a directory service that is both a directory and a protocol for controlling access to a network. The directory consists of a database specialized for fast information retrieval and filtering activities. You create and store user profile and login information on the external server.
- RADIUS

  RADIUS (Remote Authentication Dial-In User Service) authentication is a popular protocol used to authenticate users by means of an external or built-in RADIUS server. RADIUS authentication allows you to validate a large number of users from a central location.

23.2 Authentication Server Command Summary

This section describes the commands for authentication server settings.

23.2.1 ad-server Commands

The following table lists the `ad-server` commands you use to set the default AD server.

Table 141 ad-server Commands

COMMAND	DESCRIPTION
`show ad-server`	Displays the default AD server settings.
`[no] ad-server basedn` *basedn*	Sets a base distinguished name (DN) for the default AD server. A base DN identifies an AD directory. The `no` command clears this setting.

Table 141 ad-server Commands (continued)

COMMAND	DESCRIPTION
[no] ad-server binddn *binddn*	Sets the user name the ISG50 uses to log into the default AD server. The no command clears this setting.
[no] ad-server cn-identifier *uid*	Sets the unique common name (cn) to identify a record. The no command clears this setting.
[no] ad-server host *ad_server*	Sets the AD server address. Enter the IP address (in dotted decimal notation) or the domain name. The no command clears this setting.
[no] ad-server password *password*	Sets the bind password. This password will be encrypted when you use the show ad-server command to display. The no command clears this setting.
ad-server password-encrypted *password*	Sets the encrypted password (less than 32 alphanumerical characters) in order to hide the real password from people behind you when you are configuring AD server password. This password is displayed as what you typed when you use the show ad-server command.
[no] ad-server port *port_no*	Sets the AD port number. Enter a number between 1 and 65535. The default is 389. The no command clears this setting.
[no] ad-server search-time-limit *time*	Sets the search timeout period (in seconds). Enter a number between 1 and 300. The no command clears this setting.
[no] ad-server ssl	Enables the ISG50 to establish a secure connection to the AD server. The no command disables this feature.

23.2.2 ldap-server Commands

The following table lists the ldap-server commands you use to set the default LDAP server.

Table 142 ldap-server Commands

COMMAND	DESCRIPTION
show ldap-server	Displays current LDAP server settings.
[no] ldap-server basedn *basedn*	Sets a base distinguished name (DN) for the default LDAP server. A base DN identifies an LDAP directory. The no command clears this setting.
[no] ldap-server binddn *binddn*	Sets the user name the ISG50 uses to log into the default LDAP server. The no command clears this setting.
[no] ldap-server cn-identifier *uid*	Sets the unique common name (cn) to identify a record. The no command clears this setting.
[no] ldap-server host *ldap_server*	Sets the LDAP server address. Enter the IP address (in dotted decimal notation) or the domain name. The no command clears this setting.
[no] ldap-server password *password*	Sets the bind password. The no command clears this setting.
[no] ldap-server port *port_no*	Sets the LDAP port number. Enter a number between 1 and 65535. The default is 389. The no command clears this setting.
[no] ldap-server search-time-limit *time*	Sets the search timeout period (in seconds). Enter a number between 1 and 300. The no command clears this setting.
[no] ldap-server ssl	Enables the ISG50 to establish a secure connection to the LDAP server. The no command disables this feature.

23.2.3 radius-server Commands

The following table lists the `radius-server` commands you use to set the default RADIUS server.

Table 143 radius-server Commands

COMMAND	DESCRIPTION
`show radius-server`	Displays the default RADIUS server settings.
`[no] radius-server host` *`radius_server`* `auth-port` *`auth_port`*	Sets the RADIUS server address and service port number. Enter the IP address (in dotted decimal notation) or the domain name of a RADIUS server. The `no` command clears the settings.
`[no] radius-server key` *`secret`*	Sets a password (up to 15 alphanumeric characters) as the key to be shared between the RADIUS server and the ISG50. The `no` command clears this setting.
`[no] radius-server timeout` *`time`*	Sets the search timeout period (in seconds). Enter a number between 1 and 300. The `no` command clears this setting.

23.2.4 radius-server Command Example

The following example sets the secret key and timeout period of the default RADIUS server (172.23.10.100) to “87643210” and 80 seconds.

```
Router# configure terminal
Router(config)# radius-server host 172.23.10.100 auth-port 1812
Router(config)# radius-server key 876543210
Router(config)# radius-server timeout 80
Router(config)# show radius-server
host               : 172.23.10.100
authentication port: 1812
key                : 876543210
timeout            : 80
Router(config)#
```

23.2.5 aaa group server ad Commands

The following table lists the `aaa group server ad` commands you use to configure a group of AD servers.

Table 144 aaa group server ad Commands

COMMAND	DESCRIPTION
`clear aaa group server ad [`*`group-name`*`]`	Deletes all AD server groups or the specified AD server group. Note: You can NOT delete a server group that is currently in use.
`show aaa group server ad` *`group-name`*	Displays the specified AD server group settings.
`[no] aaa group server ad` *`group-name`*	Sets a descriptive name for an AD server group. Use this command to enter the sub-command mode. The `no` command deletes the specified server group.
`aaa group server ad rename` *`group-name group-name`*	Changes the descriptive name for an AD server group.

Table 144 aaa group server ad Commands (continued)

COMMAND	DESCRIPTION
aaa group server ad *group-name*	Enter the sub-command mode to configure an AD server group.
[no] server alternative-cn-identifier *uid*	Sets the second type of identifier that the users can use to log in if any. For example “name” or “e-mail address”. The no command clears this setting.
[no] server basedn *basedn*	Sets the base DN to point to the AD directory on the AD server group. The no command clears this setting.
[no] server binddn *binddn*	Sets the user name the ISG50 uses to log into the AD server group. The no command clears this setting.
[no] server cn-identifier *uid*	Sets the user name the ISG50 uses to log into the AD server group. The no command clears this setting.
[no] server description *description*	Sets the descriptive information for the AD server group. You can use up to 60 printable ASCII characters. The no command clears the setting.
[no] server group-attribute *group-attribute*	Sets the name of the attribute that the ISG50 is to check to determine to which group a user belongs. The value for this attribute is called a group identifier; it determines to which group a user belongs. You can add ext-group-user user objects to identify groups based on these group identifier values. For example you could have an attribute named “memberOf” with values like “sales”, “RD”, and “management”. Then you could also create an ext-group-user user object for each group. One with “sales” as the group identifier, another for “RD” and a third for “management”. The no command clears the setting.
[no] server host *ad_server*	Enter the IP address (in dotted decimal notation) or the domain name of an AD server to add to this group. The no command clears this setting.
[no] server password *password*	Sets the bind password (up to 15 alphanumerical characters). The no command clears this setting.
[no] server port *port_no*	Sets the AD port number. Enter a number between 1 and 65535. The default is 389. The no command clears this setting.
[no] server search-time-limit *time*	Sets the search timeout period (in seconds). Enter a number between 1 and 300. The no command clears this setting and set this to the default setting of 5 seconds.
[no] server ssl	Enables the ISG50 to establish a secure connection to the AD server. The no command disables this feature.

23.2.6 aaa group server ldap Commands

The following table lists the `aaa group server ldap` commands you use to configure a group of LDAP servers.

Table 145 aaa group server ldap Commands

COMMAND	DESCRIPTION
`clear aaa group server ldap [group-name]`	Deletes all LDAP server groups or the specified LDAP server group. Note: You can NOT delete a server group that is currently in use.
`show aaa group server ldap group-name`	Displays the specified LDAP server group settings.
`[no] aaa group server ldap group-name`	Sets a descriptive name for an LDAP server group. Use this command to enter the sub-command mode. The no command deletes the specified server group.
`aaa group server ldap rename group-name group-name`	Changes the descriptive name for an LDAP server group.
`aaa group server ldap group-name`	Enter the sub-command mode.
`[no] server alternative-cn-identifier uid`	Sets the second type of identifier that the users can use to log in if any. For example “name” or “e-mail address”. The no command clears this setting.
`[no] server basedn basedn`	Sets the base DN to point to the LDAP directory on the LDAP server group. The no command clears this setting.
`[no] server binddn binddn`	Sets the user name the ISG50 uses to log into the LDAP server group. The no command clears this setting.
`[no] server cn-identifier uid`	Sets the user name the ISG50 uses to log into the LDAP server group. The no command clears this setting.
`[no] server description description`	Sets the descriptive information for the LDAP server group. You can use up to 60 printable ASCII characters. The no command clears this setting.
`[no] server group-attribute group-attribute`	Sets the name of the attribute that the ISG50 is to check to determine to which group a user belongs. The value for this attribute is called a group identifier; it determines to which group a user belongs. You can add ext-group-user user objects to identify groups based on these group identifier values. For example you could have an attribute named “memberOf” with values like “sales”, “RD”, and “management”. Then you could also create an ext-group-user user object for each group. One with “sales” as the group identifier, another for “RD” and a third for “management”. The no command clears the setting.
`[no] server host ldap_server`	Enter the IP address (in dotted decimal notation) or the domain name of an LDAP server to add to this group. The no command clears this setting.
`[no] server password password`	Sets the bind password (up to 15 characters). The no command clears this setting.
`[no] server port port_no`	Sets the LDAP port number. Enter a number between 1 and 65535. The default is 389. The no command clears this setting.

Table 145 aaa group server ldap Commands (continued)

COMMAND	DESCRIPTION
[no] server search-time-limit *time*	Sets the search timeout period (in seconds). Enter a number between 1 and 300. The no command clears this setting and set this to the default setting of 5 seconds.
[no] server ssl	Enables the ISG50 to establish a secure connection to the LDAP server. The no command disables this feature.

23.2.7 aaa group server radius Commands

The following table lists the aaa group server radius commands you use to configure a group of RADIUS servers.

Table 146 aaa group server radius Commands

COMMAND	DESCRIPTION
clear aaa group server radius *group-name*	Deletes all RADIUS server groups or the specified RADIUS server group. Note: You can NOT delete a server group that is currently in use.
show aaa group server radius *group-name*	Displays the specified RADIUS server group settings.
[no] aaa group server radius *group-name*	Sets a descriptive name for the RADIUS server group. The no command deletes the specified server group.
aaa group server radius rename {*group-name-old*} *group-name-new*	Sets the server group name.
aaa group server radius *group-name*	Enter the sub-command mode.
[no] server description *description*	Sets the descriptive information for the RADIUS server group. You can use up to 60 printable ASCII characters. The no command clears the setting.
[no] server group-attribute <1-255>	Sets the value of an attribute that the ISG50 is used to determine to which group a user belongs. This attribute's value is called a group identifier. You can add **ext-group-user** user objects to identify groups based on different group identifier values. For example, you could configure attributes 1,10 and 100 and create a **ext-group-user** user object for each of them. The no command clears the setting.
[no] server host *radius_server*	Enter the IP address (in dotted decimal notation) or the domain name of a RADIUS server to add to this server group. The no command clears this setting.
[no] server key *secret*	Sets a password (up to 15 alphanumeric characters) as the key to be shared between the RADIUS server(s) and the ISG50. The no command clears this setting.
[no] server timeout *time*	Sets the search timeout period (in seconds). Enter a number between 1 and 300. The no command clears this setting and set this to the default setting of 5 seconds.

23.2.8 aaa group server Command Example

The following example creates a RADIUS server group with two members and sets the secret key to “12345678” and the timeout to 100 seconds. Then this example also shows how to view the RADIUS group settings.

```
Router# configure terminal
Router(config)# aaa group server radius RADIUSGroup1
Router(group-server-radius)# server host 192.168.1.100 auth-port 1812
Router(group-server-radius)# server host 172.23.22.100 auth-port 1812
Router(group-server-radius)# server key 12345678
Router(group-server-radius)# server timeout 100
Router(group-server-radius)# exit
Router(config)# show aaa group server radius RADIUSGroup1
key                : 12345678
timeout            : 100
description        :
group attribute    : 11

No.  Host Member                                                  Auth. Port

==========================================================================
1    192.168.1.100                                                 1812

2    172.23.22.100                                                 1812
```

24

Authentication Objects

This chapter shows you how to select different authentication methods for user authentication using the AAA servers or the internal user database.

24.1 Authentication Objects Overview

After you have created the AAA server objects, you can specify the authentication objects (containing the AAA server information) that the ISG50 uses to authenticate users (using VPN or managing through HTTP/HTTPS).

24.2 aaa authentication Commands

The following table lists the `aaa authentication` commands you use to configure an authentication profile.

Table 147 aaa authentication Commands

COMMAND	DESCRIPTION
`aaa authentication rename` *`profile-name-old profile-name-new`*	Changes the profile name. *`profile-name:`* You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
`clear aaa authentication` *`profile-name`*	Deletes all authentication profiles or the specified authentication profile. Note: You can NOT delete a profile that is currently in use.
`show aaa authentication {`*`group-name`*`|default}`	Displays the specified authentication server profile settings.
`[no] aaa authentication` *`profile-name`*	Sets a descriptive name for the authentication profile. The `no` command deletes a profile.

Table 147 aaa authentication Commands (continued)

COMMAND	DESCRIPTION
[no] aaa authentication default *member1* [*member2*] [*member3*] [*member4*]	Sets the default profile to use the authentication method(s) in the order specified. *member* = group ad, group ldap, group radius, or local. Note: You must specify at least one member for each profile. Each type of member can only be used once in a profile. The no command clears the specified authentication method(s) for the profile.
[no] aaa authentication *profile-name member1* [*member2*] [*member3*] [*member4*]	Sets the profile to use the authentication method(s) in the order specified. *member* = group ad, group ldap, group radius, or local. Note: You must specify at least one member for each profile. Each type of member can only be used once in a profile. The no command clears the specified authentication method(s) for the profile.

24.2.1 aaa authentication Command Example

The following example creates an authentication profile to authentication users using the LDAP server group and then the local user database.

```
Router# configure terminal
Router(config)# aaa authentication LDAPuser group ldap local
Router(config)# show aaa authentication LDAPuser
No.  Method
================================================================================
0    ldap
1    local
Router(config)#
```

24.3 test aaa Command

The following table lists the `test aaa` command you use to teat a user account on an authentication server.

Table 148 test aaa Command

COMMAND	DESCRIPTION
`test aaa {server|secure-server} {ad|ldap} host {`*`hostname`*`|`*`ipv4-address`*`} [host {`*`hostname`*`|`*`ipv4-address`*`}] port <1..65535> base-dn `*`base-dn-string`*` [bind-dn `*`bind-dn-string`*` password `*`password`*`] login-name-attribute `*`attribute`*` [alternative-login-name-attribute `*`attribute`*`] account `*`account-name`*	Tests whether a user account exists on the specified authentication server.

24.3.1 Test a User Account Command Example

The following example shows how to test whether a user account named userABC exists on the AD authentication server which uses the following settings:

- IP address: 172.16.50.1
- Port: 389
- Base-dn: DC=ZyXEL,DC=com
- Bind-dn: zyxel\engineerABC
- Password: abcdefg
- Login-name-attribute: sAMAccountName

The result shows the account exists on the AD server. Otherwise, the ISG50 responds an error.

```
Router> test aaa server ad host 172.16.50.1 port 389 base-dn DC=ZyXEL,DC=com
bind-dn zyxel\engineerABC password abcdefg login-name-attribute
sAMAccountName account userABC

dn:: Q049MTIzNzco546L5aOr56uRKSxPVT1XaXRoTWFpbCxEQz1aeVhFTCxEQz1jb20=
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn:: MTIzNzco546L5aOr56uRKQ==
sn: User
l: 2341100
-------------------------SNIP!-----------------------------------------
```

25

Certificates

This chapter explains how to use the **Certificates**.

25.1 Certificates Overview

The ISG50 can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities. You can use the ISG50 to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

25.2 Certificate Commands

This section describes the commands for configuring certificates.

25.3 Certificates Commands Input Values

The following table explains the values you can input with the `certificate` commands.

Table 149 Certificates Commands Input Values

LABEL	DESCRIPTION
certificate_name	The name of a certificate. You can use up to 31 alphanumeric and ;'~!@#$%^&()_+[]{}',.=- characters.
cn_address	A common name IP address identifies the certificate's owner. Type the IP address in dotted decimal notation.
cn_domain_name	A common name domain name identifies the certificate's owner. The domain name is for identification purposes only and can be any string. The domain name can be up to 255 characters. You can use alphanumeric characters, the hyphen and periods.
cn_email	A common name e-mail address identifies the certificate's owner. The e-mail address is for identification purposes only and can be any string. The e-mail address can be up to 63 characters. You can use alphanumeric characters, the hyphen, the @ symbol, periods and the underscore.

Table 149 Certificates Commands Input Values (continued)

LABEL	DESCRIPTION
organizational_unit	Identify the organizational unit or department to which the certificate owner belongs. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
organization	Identify the company or group to which the certificate owner belongs. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
country	Identify the nation where the certificate owner is located. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
key_length	Type a number to determine how many bits the key should use (512 to 2048). The longer the key, the more secure it is. A longer key also uses more PKI storage space.
password	When you have the ISG50 enroll for a certificate immediately online, the certification authority may want you to include a key (password) to identify your certification request. Use up to 31 of the following characters. a-zA-Z0-9;|`~!@#$%^&*()_+\{}':,./<>=-
ca_name	When you have the ISG50 enroll for a certificate immediately online, you must have the certification authority's certificate already imported as a trusted certificate. Specify the name of the certification authority's certificate. It can be up to 31 alphanumeric and ;'~!@#$%^&()_+[]{}',.=- characters.
url	When you have the ISG50 enroll for a certificate immediately online, enter the IP address (or URL) of the certification authority server. You can use up to 511 of the following characters. a-zA-Z0-9'()+,/ :.=?;!*#@$_%-

25.4 Certificates Commands Summary

The following table lists the commands that you can use to display and manage the ISG50's summary list of certificates and certification requests. You can also create certificates or certification requests. Use the `configure terminal` command to enter the configuration mode to be able to use these commands.

Table 150 ca Commands Summary

COMMAND	DESCRIPTION
`ca enroll cmp name` *certificate_name* `cn-type {ip cn` *cn_address*`|fqdn cn` *cn_domain_name*`|mail cn` *cn_email*`} [ou` *organizational_unit*`] [o` *organization*`] [c` *country*`] key-type {rsa|dsa} key-len` *key_length* `num <0..99999999> password` *password* `ca` *ca_name* `url` *url*`;`	Enrolls a certificate with a CA using Certificate Management Protocol (CMP). The certification authority may want you to include a reference number and key (password) to identify your certification request.
`ca enroll scep name` *certificate_name* `cn-type {ip cn` *cn_address*`|fqdn cn` *cn_domain_name*`|mail cn` *cn_email*`} [ou` *organizational_unit*`] [o` *organization*`] [c` *country*`] key-type {rsa|dsa} key-len` *key_length* `password` *password* `ca` *ca_name* `url` *url*	Enrolls a certificate with a CA using Simple Certificate Enrollment Protocol (SCEP). The certification authority may want you to include a key (password) to identify your certification request.

Table 150 ca Commands Summary (continued)

COMMAND	DESCRIPTION
ca generate pkcs10 name *certificate_name* cn-type {ip cn *cn_address*|fqdn cn *cn_domain_name*|mail cn *cn_email*} [ou *organizational_unit*] [o *organization*] [c *country*] key-type {rsa|dsa} key-len *key_length*	Generates a PKCS#10 certification request.
ca generate pkcs12 name *name* password *password*	Generates a PKCS#12 certificate.
ca generate x509 name *certificate_name* cn-type {ip cn *cn_address*|fqdn cn *cn_domain_name*|mail cn *cn_email*} [ou *organizational_unit*] [o *organization*] [c *country*] key-type {rsa|dsa} key-len *key_length*	Generates a self-signed x509 certificate.
ca rename category {local|remote} *old_name new_name*	Renames a local (my certificates) or remote (trusted certificates) certificate.
ca validation *remote_certificate*	Enters the sub command mode for validation of certificates signed by the specified remote (trusted) certificates.
cdp {activate|deactivate}	Has the ISG50 check (or not check) incoming certificates that are signed by this certificate against a Certificate Revocation List (CRL) or an OCSP server. You also need to configure the OSCP or LDAP server details.
ldap {activate|deactivate}	Has the ISG50 check (or not check) incoming certificates that are signed by this certificate against a Certificate Revocation List (CRL) on a LDAP (Lightweight Directory Access Protocol) directory server.
ldap ip {*ip*|*fqdn*} port <1..65535> [id *name* password *password*] [deactivate]	Sets the validation configuration for the specified remote (trusted) certificate where the directory server uses LDAP. *ip*: Type the IP address (in dotted decimal notation) or the domain name of the directory server. The domain name can use alphanumeric characters, periods and hyphens. Up to 255 characters. port: Specify the LDAP server port number. You must use the same server port number that the directory server uses. 389 is the default server port number for LDAP. The ISG50 may need to authenticate itself in order to access the CRL directory server. Type the login name (up to 31 characters) from the entity maintaining the server (usually a certification authority). You can use alphanumeric characters, the underscore and the dash. Type the password (up to 31 characters) from the entity maintaining the CRL directory server (usually a certification authority). You can use the following characters: a-zA-Z0-9;|`~!@#$%^&*()_+\{}':,./<>=-
ocsp {activate|deactivate}	Has the ISG50 check (or not check) incoming certificates that are signed by this certificate against a directory server that uses OCSP (Online Certificate Status Protocol).

Table 150 ca Commands Summary (continued)

COMMAND	DESCRIPTION
ocsp url *url* [id *name* password *password*] [deactivate]	Sets the validation configuration for the specified remote (trusted) certificate where the directory server uses OCSP. *url*: Type the protocol, IP address and pathname of the OCSP server. name: The ISG50 may need to authenticate itself in order to access the OCSP server. Type the login name (up to 31 characters) from the entity maintaining the server (usually a certification authority). You can use alphanumeric characters, the underscore and the dash. password: Type the password (up to 31 characters) from the entity maintaining the OCSP server (usually a certification authority). You can use the following characters: a-zA-Z0-9;|`~!@#$%^&*()_+\{}':,./<>=-
no ca category {local|remote} *certificate_name*	Deletes the specified local (my certificates) or remote (trusted certificates) certificate.
no ca validation *name*	Removes the validation configuration for the specified remote (trusted) certificate.
show ca category {local|remote} name *certificate_name* certpath	Displays the certification path of the specified local (my certificates) or remote (trusted certificates) certificate.
show ca category {local|remote} [name *certificate_name* format {text|pem}]	Displays a summary of the certificates in the specified category (local for my certificates or remote for trusted certificates) or the details of a specified certificate.
show ca validation name *name*	Displays the validation configuration for the specified remote (trusted) certificate.
show ca spaceusage	Displays the storage space in use by certificates.

25.5 Certificates Commands Examples

The following example creates a self-signed X.509 certificate with IP address 10.0.0.58 as the common name. It uses the RSA key type with a 512 bit key. Then it displays the list of local certificates. Finally it deletes the pkcs12request certification request.

```
Router# configure terminal
Router(config)# ca generate x509 name test_x509 cn-type ip cn 10.0.0.58 key-
type rsa key-len 512
Router(config)# show ca category local
certificate: default
  type: SELF
  subject: CN=ISG50_Factory_Default_Certificate
  issuer: CN=ISG50_Factory_Default_Certificate
  status: VALID
  ID: ISG50_Factory_Default_Certificate
    type: EMAIL
  valid from: 2003-01-01 00:38:30
  valid to: 2022-12-27 00:38:30
certificate: test
  type: REQ
  subject: CN=1.1.1.1
  issuer: none
  status: VALID
  ID: 1.1.1.1
    type: IP
  valid from: none
  valid to: none
certificate: pkcs12request
  type: REQ
  subject: CN=1.1.1.2
  issuer: none
  status: VALID
  ID: 1.1.1.2
    type: IP
  valid from: none
  valid to: none
certificate: test_x509
  type: SELF
  subject: CN=10.0.0.58
  issuer: CN=10.0.0.58
  status: VALID
  ID: 10.0.0.58
    type: IP
  valid from: 2006-05-29 10:26:08
  valid to: 2009-05-28 10:26:08
Router(config)# no ca category local pkcs12request
```

26

ISP Accounts

Use ISP accounts to manage Internet Service Provider (ISP) account information for PPPoE/PPTP interfaces.

26.1 ISP Accounts Overview

An ISP account is a profile of settings for Internet access using PPPoE or PPTP.

26.1.1 PPPoE and PPTP Account Commands

The following table lists the PPPoE and PPTP ISP account commands.

Table 151 PPPoE and PPTP ISP Account Commands

COMMAND	DESCRIPTION
`show account [pppoe` *`profile_name`* `| pptp` *`profile_name`*`]`	Displays information about the specified account(s).
`[no] account {pppoe | pptp}` *`profile_name`*	Creates a new ISP account with name *`profile_name`* if necessary and enters sub-command mode. The `no` command deletes the specified ISP account. *`profile_name`*: use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
`[no] user` *`username`*	Sets the username for the specified ISP account. The `no` command clears the username. *`username`*: You can use alphanumeric, underscores (_), dashes (-), and `/@$` characters, and it can be up to 30 characters long.
`[no] password` *`password`*	Sets the password for the specified ISP account. The `no` command clears the password. *`password`*: You can use up to 63 printable ASCII characters. Spaces are not allowed.
`[no] authentication {chap-pap | chap | pap | mschap | mschap-v2}`	Sets the authentication for the specified ISP account. The `no` command sets the authentication to chap-pap.
`[no] compression {on | off}`	Turns compression on or off for the specified ISP account. The `no` command turns off compression.
`[no] idle <0..360>`	Sets the idle timeout for the specified ISP account. The `no` command sets the idle timeout to zero.

Table 151 PPPoE and PPTP ISP Account Commands (continued)

COMMAND	DESCRIPTION
[no] service-name {*ip* | *hostname* | *service_name*}	Sets the service name for the specified PPPoE ISP account. The no command clears the service name. *hostname*: You may up to 63 alphanumeric characters, dashes (-), or periods (.), but the first character cannot be a period. *service_name*: You can use 1-253 alphanumeric characters, underscores (_), dashes (-), and @$./ characters.
[no] server *ip*	Sets the PPTP server for the specified PPTP ISP account. The no command clears the server name.
[no] encryption {nomppe | mppe-40 | mppe-128}	Sets the encryption for the specified PPTP ISP account. The no command sets the encryption to nomppe.
[no] connection-id *connection_id*	Sets the connection ID for the specified PPTP ISP account. The no command clears the connection ID. *connection_id*: You can use up to 31 alphanumeric characters, underscores (_), dashes (-), and colons (:).

26.1.2 Cellular Account Commands

The following table lists the cellular ISP account commands.

Table 152 Cellular Account Commands

COMMAND	DESCRIPTION
show account cellular *profile_name*	Displays information about the specified account.
[no] account cellular *profile_name*	Creates a new cellular ISP account with name *profile_name* if necessary and enters sub-command mode. The no command deletes the specified ISP account. *profile_name*: use 0-30 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
[no] apn *access_point_name*	Sets the Access Point Name (APN) for the cellular ISP account. The no command clears the APN. *access_point_name*: Use up to 64 alphanumeric characters and underscores (_), dashes (-), periods (.), and /@\$#.
[no] phone *phone_number*	Sets the username for the specified ISP account. The no command clears the username. *username*: Use up to 64 alphanumeric characters and underscores (_), dashes (-), periods (.), and /@\$#.
[no] user *username*	Sets the username for the specified ISP account. The no command clears the username. *username*: Use up to 64 alphanumeric characters and underscores (_), dashes (-), periods (.), and /@\$#.
[no] password *password*	Sets the password for the specified ISP account. The no command clears the password. *password*: Use up to 63 printable ASCII characters. Spaces are not allowed.

Table 152 Cellular Account Commands (continued)

COMMAND	DESCRIPTION
`[no] authentication {none | pap | chap}`	Sets the authentication for the cellular account. The no command sets the authentication to none.
`[no] idle <0..360>`	Sets the idle timeout for the cellular account. Zero disables the idle timeout. The no command sets the idle timeout to zero.

27

System

This chapter provides information on the commands that correspond to what you can configure in the system screens.

27.1 System Overview

Use these commands to configure general ISG50 information, the system time and the console port connection speed for a terminal emulation program. They also allow you to configure DNS settings and determine which services/protocols can access which ISG50 zones (if any) from which computers.

27.2 Customizing the WWW Login Page

Use these commands to customize the Web Configurator login screen. You can also customize the page that displays after an access user logs into the Web Configurator to access network services like the Internet. See Chapter 19 on page 269 for more on access user accounts.

The following figures identify the parts you can customize in the login and access pages.

Figure 22 Login Page Customization

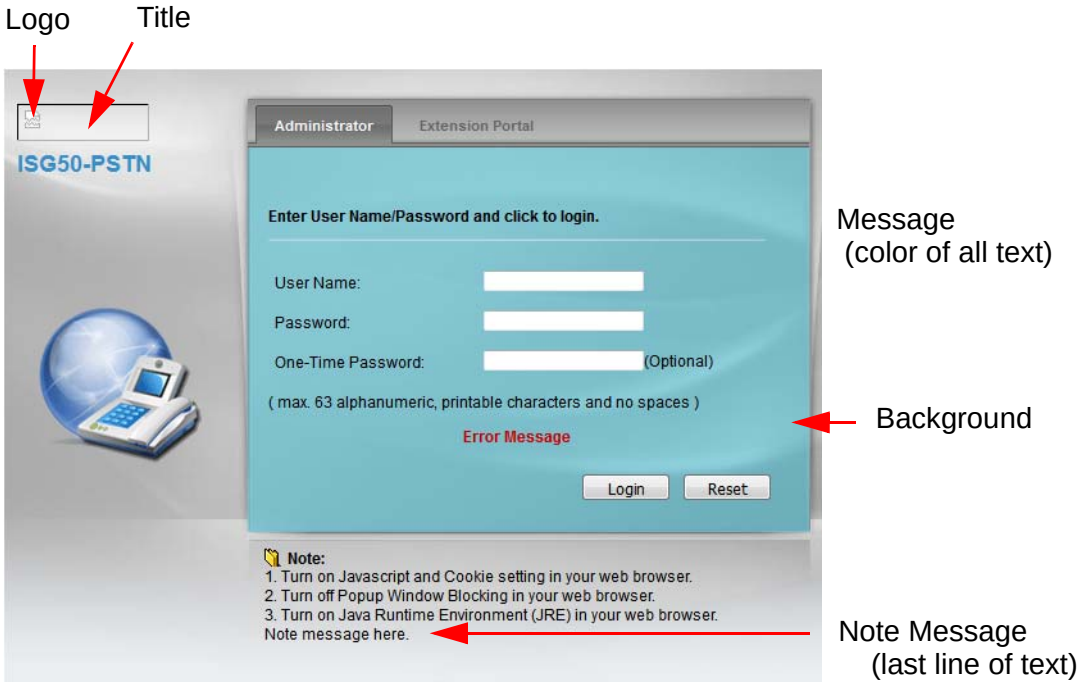
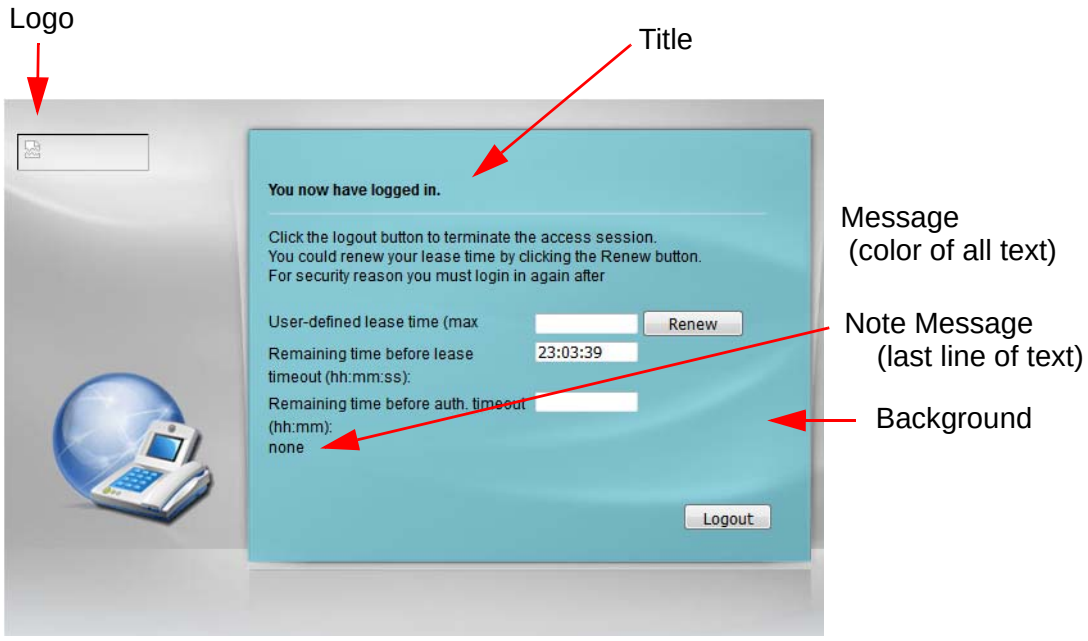


Figure 23 Access Page Customization



You can specify colors in one of the following ways:

- *color-rgb*: Enter red, green, and blue values in parenthesis and separate by commas. For example, use “rgb(0,0,0)” for black.
- *color-name*: Enter the name of the desired color.

- *color-number*: Enter a pound sign (#) followed by the six-digit hexadecimal number that represents the desired color. For example, use "#000000" for black.

The following table describes the commands available for customizing the Web Configurator login screen and the page that displays after an access user logs into the Web Configurator to access network services like the Internet. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 153 Command Summary: Customization

COMMAND	DESCRIPTION
`[no] access-page color-window-background`	Sets whether or not the access page uses a colored background.
`access-page message-color {`*`color-rgb`* `|` *`color-name`* `|` *`color-number`*`}`	Sets the color of the message text on the access page.
`[no] access-page message-text` *`message`*	Sets a note to display below the access page's title. Use up to 64 printable ASCII characters. Spaces are allowed.
`access-page title` *`title`*	Sets the title for the top of the access page. Use up to 64 printable ASCII characters. Spaces are allowed.
`access-page window-color {`*`color-rgb`* `|` *`color-name`* `|` *`color-number`*`}`	Sets the color of the access page's colored background.
`login-page background-color {`*`color-rgb`* `|` *`color-name`* `|` *`color-number`*`}`	Sets the color of the login page's background.
`[no] login-page color-background`	Sets the login page to use a solid colored background.
`[no] login-page color-window-background`	Sets the login page's window to use a solid colored background.
`login-page message-color {`*`color-rgb`* `|` *`color-name`* `|` *`color-number`*`}`	Sets the color of the message text on the login page.
`[no] login-page message-text %` *`message`*	Sets a note to display at the bottom of the login screen. Use up to 64 printable ASCII characters. Spaces are allowed.
`login-page title` *`title`*	Sets the title for the top of the login screen. Use up to 64 printable ASCII characters. Spaces are allowed.
`login-page title-color {`*`color-rgb`* `|` *`color-name`* `|` *`color-number`*`}`	Sets the title text color of the login page.
`login-page window-color {`*`color-rgb`* `|` *`color-name`* `|` *`color-number`*`}`	Sets the color of the login page's window border.
`logo background-color {`*`color-rgb`* `|` *`color-name`* `|` *`color-number`*`}`	Sets the color of the logo banner across the top of the login screen and access page.
`show access-page settings`	Lists the current access page settings.
`show login-page default-title`	Lists the factory default title for the login page.
`show login-page settings`	Lists the current login page settings.
`show logo settings`	Lists the current logo background (banner) and floor (line below the banner) settings.
`show page-customization`	Lists whether the ISG50 is set to use custom login and access pages or the default ones.

27.3 Host Name Commands

The following table describes the commands available for the hostname and domain name. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 154 Command Summary: Host Name

COMMAND	DESCRIPTION
`[no] domainname` *domain_name*	Sets the domain name. The no command removes the domain name. *domain_name*: This name can be up to 254 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
`[no] hostname` *hostname*	Sets a descriptive name to identify your ISG50. The no command removes the host name.
`show fqdn`	Displays the fully qualified domain name.

27.4 Time and Date

For effective scheduling and logging, the ISG50 system time must be accurate. The ISG50's Real Time Chip (RTC) keeps track of the time and date. There is also a software mechanism to set the time manually or get the current time and date from an external server.

27.4.1 Date/Time Commands

The following table describes the commands available for date and time setup. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 155 Command Summary: Date/Time

COMMAND	DESCRIPTION
`clock date` *yyyy-mm-dd* `time` *hh:mm:ss*	Sets the new date in year, month and day format manually and the new time in hour, minute and second format.
`[no] clock daylight-saving`	Enables daylight saving. The no command disables daylight saving.
`[no] clock saving-interval begin {apr|aug|dec|feb|jan|jul|jun|mar|may|nov|oct|sep} {1|2|3|4|last} {fri|mon|sat|sun|thu|tue|wed}` *hh:mm* `end {apr|aug|dec|feb|jan|jul|jun|mar|may|nov|oct|sep} {1|2|3|4|last} {fri|mon|sat|sun|thu|tue|wed}` *hh:mm* `offset`	Configures the day and time when Daylight Saving Time starts and ends. The no command removes the day and time when Daylight Saving Time starts and ends. offset: a number from 1 to 5.5 (by 0.5 increments)
`clock time` *hh:mm:ss*	Sets the new time in hour, minute and second format.
`[no] clock time-zone {-|+`*hh*`}`	Sets your time zone. The no command removes time zone settings.

Table 155 Command Summary: Date/Time (continued)

COMMAND	DESCRIPTION
[no] ntp	Saves your date and time and time zone settings and updates the data and time every 24 hours. The no command stops updating the data and time every 24 hours.
[no] ntp server {*fqdn*|*w.x.y.z*}	Sets the IP address or URL of your NTP time server. The no command removes time server information.
ntp sync	Gets the time and date from a NTP time server.
show clock date	Displays the current date of your ISG50.
show clock status	Displays your time zone and daylight saving settings.
show clock time	Displays the current time of your ISG50.
show ntp server	Displays time server settings.

27.5 Console Port Speed

This section shows you how to set the console port speed when you connect via the console port using a terminal emulation program. The following table describes the console port commands. You must use the configure terminal command to enter the configuration mode before you can use these commands.

Table 156 Command Summary: Console Port Speed

COMMAND	DESCRIPTION
[no] console baud *baud_rate*	Sets the speed of the console port. The no command resets the console port speed to the default (115200). *baud_rate*: 9600, 19200, 38400, 57600 or 115200.
show console	Displays console port speed.

27.6 DNS Overview

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it.

27.6.1 Domain Zone Forwarder

A domain zone forwarder contains a DNS server's IP address. The ISG50 can query the DNS server to resolve domain zones for features like VPN, DDNS and the time server. A domain zone is a fully qualified domain name without the host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name.

27.6.2 DNS Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 157 Input Values for General DNS Commands

LABEL	DESCRIPTION
address_object	The name of the IP address (group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
interface_name	The name of the interface. Ethernet interface: Use ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your ISG50 model. virtual interface on top of Ethernet interface: add a colon (:) and the number of the virtual interface. For example: ge*x*:*y*, *x* = 1 - N, *y* = 1 - 4 VLAN interface: vlan*x*, *x* = 0 - 4094 virtual interface on top of VLAN interface: vlan*x*:*y*, *x* = 0 - 4094, *y* = 1 - 12 bridge interface: br*x*, *x* = 0 - N, where N depends on the number of bridge interfaces your ISG50 model supports. virtual interface on top of bridge interface: br*x*:*y*, *x* = the number of the bridge interface, *y* = 1 - 4 PPPoE/PPTP interface: ppp*x*, *x* = 0 - N, where N depends on the number of PPPoE/PPTP interfaces your ISG50 model supports.

The following table describes the commands available for DNS. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 158 Command Summary: DNS

COMMAND	DESCRIPTION
`[no] ip dns server a-record` *`fqdn w.x.y.z`*	Sets an A record that specifies the mapping of a fully qualified domain name (FQDN) to an IP address. The `no` command deletes an A record.
`ip dns server -flush`	Clears the DNS .
`[no] ip dns server mx-record` *`domain_name`* {*`w.x.y.z`*|*`fqdn`*}	Sets a MX record that specifies a mail server that is responsible for handling the mail for a particular domain. The `no` command deletes a MX record.
`ip dns server rule {<1..32>|append|insert <1..32>} access-group {ALL|`*`address_object`*`} zone {ALL|`*`address_object`*`} action {accept|deny}`	Sets a service control rule for DNS requests.
`ip dns server rule move <1..32> to <1..32>`	Changes the number of a service control rule.

Table 158 Command Summary: DNS (continued)

COMMAND	DESCRIPTION
[no] ip dns server zone-forwarder {<1..32>|append|insert <1..32>} {*domain_zone_name*|*} interface *interface_name*	Sets a domain zone forwarder record that specifies a fully qualified domain name. You can also use a star (*) if all domain zones are served by the specified DNS server(s). *domain_zone_name*: This is a domain zone, not a host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name. For example, whenever the ISG50 receives needs to resolve a zyxel.com.tw domain name, it can send a query to the recorded name server IP address. *interface_name*: This is the interface through which the ISP provides a DNS server. The interface should be activated and set to be a DHCP client. The no command deletes a zone forwarder record.
ip dns server zone-forwarder {<1..32>|append|insert <1..32>} {*domain_zone_name*|*} user-defined *w.x.y.z* [private | interface {*interface_name* | auto}]	Sets a domain zone forwarder record that specifies a DNS server's IP address. private | interface: Use private if the ISG50 connects to the DNS server through a VPN tunnel. Otherwise, use the interface command to set the interface through which the ISG50 sends DNS queries to a DNS server. The auto means any interface that the ISG50 uses to send DNS queries to a DNS server according to the routing rule.
ip dns server zone-forwarder move <1..32> to <1..32>	Changes the index number of a zone forwarder record.
no ip dns server rule <1..32>	Deletes a service control rule.
show ip dns server	Displays all DNS entries.
show ip dns server database	Displays all configured records.
show ip dns server status	Displays whether this service is enabled or not.

27.6.3 DNS Command Example

This command sets an A record that specifies the mapping of a fully qualified domain name (www.abc.com) to an IP address (210.17.2.13).

```
Router# configure terminal
Router(config)# ip dns server a-record www.abc.com 210.17.2.13
```

27.7 SNAT Overview

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it.

28

System Remote Management

This chapter shows you how to determine which services/protocols can access which ISG50 zones (if any) from which computers.

Note: To allow the ISG50 to be accessed from a specified computer using a service, make sure you do not have a service control rule or to-ISG50 rule to block that traffic.

28.1 Remote Management Overview

You may manage your ISG50 from a remote location via:

- Internet (WAN only)
- LAN only
- ALL (LAN&WAN&DMZ)
- DMZ only

To disable remote management of a service, deselect **Enable** in the corresponding service screen.

28.1.1 Remote Management Limitations

Remote management will not work when:

1. You have disabled that service in the corresponding screen.
2. The accepted IP address in the **Service Control** table does not match the client IP address. If it does not match, the ISG50 will disconnect the session immediately.
3. There is a firewall rule that blocks it.

28.1.2 System Timeout

There is a lease timeout for administrators. The ISG50 automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling.

Each user is also forced to log in the ISG50 for authentication again when the reauthentication time expires.

28.2 Common System Command Input Values

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

Table 159 Input Values for General System Commands

LABEL	DESCRIPTION
address_object	The name of the IP address (group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
rule_number	The number of a service control rule. 1 - *X* where *X* is the highest number of rules the ISG50 model supports.
zone_object	The name of the zone. Use up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive.

28.3 HTTP/HTTPS Commands

The following table describes the commands available for HTTP/HTTPS. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 160 Command Summary: HTTP/HTTPS

COMMAND	DESCRIPTION
`[no] ip http authentication` *auth_method*	Sets an authentication method used by the HTTP/HTTPS server. The `no` command resets the authentication method used by the HTTP/HTTPS server to the factory default (`default`). *auth_method*: The name of the authentication method. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
`[no] ip http port <1..65535>`	Sets the HTTP service port number. The `no` command resets the HTTP service port number to the factory default (80).
`[no] ip http secure-port <1..65535>`	Sets the HTTPS service port number. The `no` command resets the HTTPS service port number to the factory default (443).
`[no] ip http secure-server`	Enables HTTPS access to the ISG50 web configurator. The `no` command disables HTTPS access to the ISG50 web configurator.
`[no] ip http secure-server auth-client`	Sets the client to authenticate itself to the HTTPS server. The `no` command sets the client not to authenticate itself to the HTTPS server.
`[no] ip http secure-server cert` *certificate_name*	Specifies a certificate used by the HTTPS server. The `no` command resets the certificate used by the HTTPS server to the factory default (`default`). *certificate_name*: The name of the certificate. You can use up to 31 alphanumeric and ;'~!@#$%^&()_+[]{}',.=- characters.

Table 160 Command Summary: HTTP/HTTPS (continued)

COMMAND	DESCRIPTION
[no] ip http secure-server force-redirect	Redirects all HTTP connection requests to a HTTPS URL. The no command disables forwarding HTTP connection requests to a HTTPS URL.
ip http secure-server table {admin|user} rule {*rule_number*|append|insert *rule_number*} access-group {ALL|*address_object*} zone {ALL|*zone_object*} action {accept|deny}	Sets a service control rule for HTTPS service.
ip http secure-server table {admin|user} rule move *rule_number* to *rule_number*	Changes the index number of a HTTPS service control rule.
ip http secure-server cipher-suite {*cipher_algorithm*} [*cipher_algorithm*] [*cipher_algorithm*] [*cipher_algorithm*]	Sets the encryption algorithms (up to four) that the ISG50 uses for the SSL in HTTPS connections and the sequence in which it uses them. The *cipher_algorithm* can be any of the following. rc4: RC4 (RC4 may impact the ISG50's CPU performance since the ISG50's encryption accelerator does not support it). aes: AES des: DES 3des: Triple DES.
no ip http secure-server cipher-suite {*cipher_algorithm*}	Has the ISG50 not use the specified encryption algorithm for the SSL in HTTPS connections.
[no] ip http server	Allows HTTP access to the ISG50 web configurator. The no command disables HTTP access to the ISG50 web configurator.
ip http server table {admin|user} rule {*rule_number*|append|insert *rule_number*} access-group {ALL|*address_object*} zone {ALL|*zone_object*} action {accept|deny}	Sets a service control rule for HTTP service.
ip http server table {admin|user} rule move *rule_number* to *rule_number*	Changes the number of a HTTP service control rule.
no ip http secure-server table {admin|user} rule *rule_number*	Deletes a service control rule for HTTPS service.
no ip http server table {admin|user} rule *rule_number*	Deletes a service control rule for HTTP service.
show ip http server status	Displays HTTP settings.
show ip http server secure status	Displays HTTPS settings.

28.3.1 HTTP/HTTPS Command Examples

This following example adds a service control rule that allowed an administrator from the computers with the IP addresses matching the Marketing address object to access the WAN zone using HTTP service.

```
Router# configure terminal
Router(config)# ip http server table admin rule append access-group
Marketing zone WAN action accept
```

This command sets an authentication method used by the HTTP/HTTPS server to authenticate the client(s).

```
Router# configure terminal
Router(config)# ip http authentication Example
```

This following example sets a certificate named MyCert used by the HTTPS server to authenticate itself to the SSL client.

```
Router# configure terminal
Router(config)# ip http secure-server cert MyCert
```

28.4 SSH

Unlike Telnet or FTP, which transmit data in clear text, SSH (Secure Shell) is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network.

28.4.1 SSH Implementation on the ISG50

Your ISG50 supports SSH versions 1 and 2 using RSA authentication and four encryption methods (AES, 3DES, Archfour, and Blowfish). The SSH server is implemented on the ISG50 for remote management on port 22 (by default).

28.4.2 Requirements for Using SSH

You must install an SSH client program on a client computer (Windows or Linux operating system) that is used to connect to the ISG50 over SSH.

28.4.3 SSH Commands

The following table describes the commands available for SSH. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 161 Command Summary: SSH

COMMAND	DESCRIPTION
`[no] ip ssh server`	Allows SSH access to the ISG50 CLI. The `no` command disables SSH access to the ISG50 CLI.
`[no] ip ssh server cert` *certificate_name*	Sets a certificate whose corresponding private key is to be used to identify the ISG50 for SSH connections. The `no` command resets the certificate used by the SSH server to the factory default (`default`). *certificate_name*: The name of the certificate. You can use up to 31 alphanumeric and ;'~!@#$%^&()_+[]{}',.=- characters.
`[no] ip ssh server port <1..65535>`	Sets the SSH service port number. The `no` command resets the SSH service port number to the factory default (22).
`ip ssh server rule {`*rule_number*`|append|insert` *rule_number*`} access-group {ALL|`*address_object*`} zone {ALL|`*zone_object*`} action {accept|deny}`	Sets a service control rule for SSH service. *address_object*: The name of the IP address (group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. *zone_object*: The name of the zone. Use up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive.
`ip ssh server rule move` *rule_number* `to` *rule_number*	Changes the index number of a SSH service control rule.
`[no] ip ssh server v1`	Enables remote management using SSH v1. The `no` command stops the ISG50 from using SSH v1.
`no ip ssh server rule` *rule_number*	Deletes a service control rule for SSH service.
`show ip ssh server status`	Displays SSH settings.

28.4.4 SSH Command Examples

This command sets a service control rule that allowed the computers with the IP addresses matching the specified address object to access the specified zone using SSH service.

```
Router# configure terminal
Router(config)# ip ssh server rule 2 access-group Marketing zone WAN action
accept
```

This command sets a certificate (Default) to be used to identify the ISG50.

```
Router# configure terminal
Router(config)# ip ssh server cert Default
```

28.5 Telnet

You can configure your ISG50 for remote Telnet access.

28.6 Telnet Commands

The following table describes the commands available for Telnet. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 162 Command Summary: Telnet

COMMAND	DESCRIPTION
`[no] ip telnet server`	Allows Telnet access to the ISG50 CLI. The `no` command disables Telnet access to the ISG50 CLI.
`[no] ip telnet server port <1..65535>`	Sets the Telnet service port number. The `no` command resets the Telnet service port number back to the factory default (23).
`ip telnet server rule {`*`rule_number`*`|append|insert` *`rule_number`*`} access-group {ALL|`*`address_object`*`} zone {ALL|`*`zone_object`*`} action {accept|deny}`	Sets a service control rule for Telnet service. *address_object*: The name of the IP address (group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. *zone_object*: The name of the zone. Use up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive.
`ip telnet server rule move` *`rule_number`* `to` *`rule_number`*	Changes the index number of a service control rule.
`no ip telnet server rule` *`rule_number`*	Deletes a service control rule for Telnet service.
`show ip telnet server status`	Displays Telnet settings.

28.6.1 Telnet Commands Examples

This command sets a service control rule that allowed the computers with the IP addresses matching the specified address object to access the specified zone using Telnet service.

```
Router# configure terminal
Router(config)# ip telnet server rule 11 access-group RD zone LAN action
-> accept
```

This command displays Telnet settings.

```
Router# configure terminal
Router(config)# show ip telnet server status
active     : yes
port       : 23
service control:
No.  Zone                        Address                      Action
==========================================================================
Router(config)#
```

28.7 Configuring FTP

You can upload and download the ISG50's firmware and configuration files using FTP. To use this feature, your computer must have an FTP client.

28.7.1 FTP Commands

The following table describes the commands available for FTP. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 163 Command Summary: FTP

COMMAND	DESCRIPTION
`[no] ip ftp server`	Allows FTP access to the ISG50. The `no` command disables FTP access to the ISG50.
`[no] ip ftp server cert` *`certificate_name`*	Sets a certificate to be used to identify the ISG50. The `no` command resets the certificate used by the FTP server to the factory default.
`[no] ip ftp server port <1..65535>`	Sets the FTP service port number. The `no` command resets the FTP service port number to the factory default (21).
`[no] ip ftp server tls-required`	Allows FTP access over TLS. The `no` command disables FTP access over TLS.
`ip ftp server rule {`*`rule_number`*`|append|insert` *`rule_number`*`} access-group {ALL|`*`address_object`*`} zone {ALL|`*`zone_object`*`} action {accept|deny}`	Sets a service control rule for FTP service. *`address_object`*: The name of the IP address (group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. *`zone_object`*: The name of the zone. Use up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive.
`ip ftp server rule move` *`rule_number`* `to` *`rule_number`*	Changes the index number of a service control rule.
`no ip ftp server rule` *`rule_number`*	Deletes a service control rule for FTP service.
`show ip ftp server status`	Displays FTP settings.

28.7.2 FTP Commands Examples

This command sets a service control rule that allowed the computers with the IP addresses matching the specified address object to access the specified zone using FTP service.

```
Router# configure terminal
Router(config)# ip ftp server rule 4 access-group Sales zone WAN action
accept
```

This command displays FTP settings.

```
Router# configure terminal
Router(config)# show ip ftp server status
active     : yes
port       : 21
certificate: default
TLS        : no
service control:
No.  Zone                      Address                       Action
================================================================================
```

28.8 SNMP

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. Your ISG50 supports SNMP agent functionality, which allows a manager station to manage and monitor the ISG50 through the network. The ISG50 supports SNMP version one (SNMPv1) and version two (SNMPv2c).

28.8.1 Supported MIBs

The ISG50 supports MIB II that is defined in RFC-1213 and RFC-1215. The ISG50 also supports private MIBs (ZYXEL-ES-SMI.mib and ZYXEL-ES_COMMON.mib) to collect information about CPU and memory usage and VPN total throughput. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance. You can download the ISG50's MIBs from www.zyxel.com.

28.8.2 SNMP Traps

The ISG50 will send traps to the SNMP manager when any one of the following events occurs:

Table 164 SNMP Traps

OBJECT LABEL	OBJECT ID	DESCRIPTION
Cold Start	1.3.6.1.6.3.1.1.5.1	This trap is sent when the ISG50 is turned on or an agent restarts.
linkDown	1.3.6.1.6.3.1.1.5.3	This trap is sent when the Ethernet link is down.

Table 164 SNMP Traps (continued)

OBJECT LABEL	OBJECT ID	DESCRIPTION
linkUp	1.3.6.1.6.3.1.1.5.4	This trap is sent when the Ethernet link is up.
authenticationFailure	1.3.6.1.6.3.1.1.5.5	This trap is sent when an SNMP request comes from non-authenticated hosts.

28.8.3 SNMP Commands

The following table describes the commands available for SNMP. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 165 Command Summary: SNMP

COMMAND	DESCRIPTION
`[no] snmp-server`	Allows SNMP access to the ISG50. The `no` command disables SNMP access to the ISG50.
`[no] snmp-server community` *community_string* `{ro|rw}`	Enters up to 64 characters to set the password for read-only (ro) or read-write (rw) access. The `no` command resets the password for read-only (`ro`) or read-write (`rw`) access to the default.
`[no] snmp-server contact` *description*	Sets the contact information (of up to 60 characters) for the person in charge of the ISG50. The `no` command removes the contact information for the person in charge of the ISG50.
`[no] snmp-server enable {informs|traps}`	Enables all SNMP notifications (informs or traps). The `no` command disables all SNMP notifications (informs or traps).
`[no] snmp-server host {`*w.x.y.z*`}` `[`*community_string*`]`	Sets the IP address of the host that receives the SNMP notifications. The `no` command removes the host that receives the SNMP notifications.
`[no] snmp-server location` *description*	Sets the geographic location (of up to 60 characters) for the ISG50. The `no` command removes the geographic location for the ISG50.
`[no] snmp-server port <1..65535>`	Sets the SNMP service port number. The `no` command resets the SNMP service port number to the factory default (`161`).
`snmp-server rule {`*rule_number*`|append|insert` *rule_number*`} access-group {ALL|`*address_object*`}` `zone {ALL|`*zone_object*`} action {accept|deny}`	Sets a service control rule for SNMP service. *address_object*: The name of the IP address (group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. *zone_object*: The name of the zone. Use up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive.
`snmp-server rule move` *rule_number* `to` *rule_number*	Changes the index number of a service control rule.
`no snmp-server rule` *rule_number*	Deletes a service control rule for SNMP service.
`show snmp status`	Displays SNMP Settings.

28.8.4 SNMP Commands Examples

The following command sets a service control rule that allowed the computers with the IP addresses matching the specified address object to access the specified zone using SNMP service.

```
Router# configure terminal
Router(config)# snmp-server rule 11 access-group Example zone WAN action
accept
```

The following command sets the password (secret) for read-write (rw) access.

```
Router# configure terminal
Router(config)# snmp-server community secret rw
```

The following command sets the IP address of the host that receives the SNMP notifications to 172.23.15.84 and the password (sent with each trap) to qwerty.

```
Router# configure terminal
Router(config)# snmp-server host 172.23.15.84 qwerty
```

28.9 ICMP Filter

The ip icmp-filter commands are obsolete. See Chapter 16 on page 117 to configure firewall rules for ICMP traffic going to the ISG50 to discard or reject ICMP packets destined for the ISG50.

Configure the ICMP filter to help keep the ISG50 hidden from probing attempts. You can specify whether or not the ISG50 is to respond to probing for unused ports.

You must use the configure terminal command to enter the configuration mode before you can use these commands.

Table 166 Command Summary: ICMP Filter

COMMAND	DESCRIPTION
[no] ip icmp-filter activate	Turns the ICMP filter on or off.
ip icmp-filter rule {<1..32>|append|insert <1..32>} access-group {ALL|ADDRESS_OBJECT} zone {ALL|ZONE_OBJECT} icmp-type {ALL |echo-reply |destination-unreachable |source-quench|redirect|echo-request| router-advertisement|router-solicitation |time-exceeded | parameter-problem| timestamp-request|timestamp-reply| address-mask-request| address-mask-reply} action {accept|deny}	Sets an ICMP filter rule. ADDRESS_OBJECT: The name of the IP address (group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. ZONE_OBJECT: The name of the zone. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
no ip icmp-filter rule <1..64>	Deletes an ICMP filter rule.

Table 166 Command Summary: ICMP Filter (continued)

COMMAND	DESCRIPTION
`ip icmp-filter rule move <1..64> to <1..64>`	Changes the index number of an ICMP filter rule.
`show ip icmp-filter status`	Displays ICMP filter settings.

28.10 Language Commands

Use the `language` commands to display what language the web configurator is using or change it. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 167 Command Summary: Language

COMMAND	DESCRIPTION
`language <English | Simplified_Chinese | Traditional_Chinese>`	Specifies the language used in the web configurator screens.
`show language {setting | all}`	`setting` displays the current display language in the web configurator screens. `all` displays the available languages.

29

File Manager

This chapter covers how to work with the ISG50's firmware, certificates, configuration files, packet trace results, shell scripts and temporary files.

29.1 File Directories

The ISG50 stores files in the following directories.

Table 168 FTP File Transfer Notes

DIRECTORY	FILE TYPE	FILE NAME EXTENSION
A	Firmware (upload only)	bin
cert	Non-PKCS#12 certificates	cer
conf	Configuration files	conf
packet_trace	Packet trace results (download only)	
script	Shell scripts	.zysh
tmp	Temporary system maintenance files and crash dumps for technical support use (download only)	

A. After you log in through FTP, you do not need to change directories in order to upload the firmware.

29.2 Configuration Files and Shell Scripts Overview

You can store multiple configuration files and shell script files on the ISG50.

When you apply a configuration file, the ISG50 uses the factory default settings for any features that the configuration file does not include. Shell scripts are files of commands that you can store on the ISG50 and run when you need them. When you run a shell script, the ISG50 only applies the commands that it contains. Other settings do not change.

You can edit configuration files or shell scripts in a text editor and upload them to the ISG50. Configuration files use a .conf extension and shell scripts use a .zysh extension.

These files have the same syntax, which is also identical to the way you run CLI commands manually. An example is shown below.

Figure 24 Configuration File / Shell Script: Example

```
# enter configuration mode
configure terminal
# change administrator password
username admin password 4321 user-type admin
# configure ge3
interface ge3
ip address 172.23.37.240 255.255.255.0
ip gateway 172.23.37.254 metric 1
exit
# create address objects for remote management / to-Device firewall rules
# use the address group in case we want to open up remote management later
address-object TW_SUBNET 172.23.37.0/24
object-group address TW_TEAM
address-object TW_SUBNET
exit
# enable Telnet access (not enabled by default, unlike other services)
ip telnet server
# open WAN-to-Device firewall for TW_TEAM for remote management
firewall WAN Device insert 4
sourceip TW_TEAM
service TELNET
action allow
exit
write
```

While configuration files and shell scripts have the same syntax, the ISG50 applies configuration files differently than it runs shell scripts. This is explained below.

Table 169 Configuration Files and Shell Scripts in the ISG50

Configuration Files (.conf)	Shell Scripts (.zysh)
• Resets to default configuration. • Goes into CLI **Configuration** mode. • Runs the commands in the configuration file.	• Goes into CLI **Privilege** mode. • Runs the commands in the shell script.

You have to run the example in Table 24 on page 326 as a shell script because the first command is run in **Privilege** mode. If you remove the first command, you have to run the example as a configuration file because the rest of the commands are executed in **Configuration** mode. (See Section 1.5 on page 25 for more information about CLI modes.)

29.2.1 Comments in Configuration Files or Shell Scripts

In a configuration file or shell script, use “#” or “!” as the first character of a command line to have the ISG50 treat the line as a comment.

Your configuration files or shell scripts can use “exit” or a command line consisting of a single “!” to have the ISG50 exit sub command mode.

Note: “exit” or “!'” must follow sub commands if it is to make the ISG50 exit sub command mode.

Line 3 in the following example exits sub command mode.

```
interface ge1
ip address dhcp
!
```

Lines 1 and 3 in the following example are comments and line 4 exits sub command mode.

```
!
interface ge1
# this interface is a DHCP client
!
```

Lines 1 and 2 are comments. Line 5 exits sub command mode.

```
! this is from Joe
# on 2006/06/05
interface ge1
ip address dhcp
!
```

29.2.2 Errors in Configuration Files or Shell Scripts

When you apply a configuration file or run a shell script, the ISG50 processes the file line-by-line. The ISG50 checks the first line and applies the line if no errors are detected. Then it continues with the next line. If the ISG50 finds an error, it stops applying the configuration file or shell script and generates a log.

You can change the way a configuration file or shell script is applied. Include `setenv stop-on-error off` in the configuration file or shell script. The ISG50 ignores any errors in the configuration file or shell script and applies all of the valid commands. The ISG50 still generates a log for any errors.

29.2.3 ISG50 Configuration File Details

You can store multiple configuration files on the ISG50. You can also have the ISG50 use a different configuration file without the ISG50 restarting.

- When you first receive the ISG50, it uses the **system-default.conf** configuration file of default settings.
- When you change the configuration, the ISG50 creates a **startup-config.conf** file of the current configuration.
- The ISG50 checks the **startup-config.conf** file for errors when it restarts. If there is an error in the **startup-config.conf** file, the ISG50 copies the **startup-config.conf** configuration file to the **startup-config-bad.conf** configuration file and tries the existing **lastgood.conf** configuration file.

- When the ISG50 reboots, if the **startup-config.conf** file passes the error check, the ISG50 keeps a copy of the **startup-config.conf** file as the **lastgood.conf** configuration file for you as a back up file. If you upload and apply a configuration file with an error, you can apply **lastgood.conf** to return to a valid configuration.

29.2.4 Configuration File Flow at Restart

If there is not a **startup-config.conf** when you restart the ISG50 (whether through a management interface or by physically turning the power off and back on), the ISG50 uses the **system-default.conf** configuration file with the ISG50's default settings.

If there is a **startup-config.conf**, the ISG50 checks it for errors and applies it. If there are no errors, the ISG50 uses it and copies it to the **lastgood.conf** configuration file. If there is an error, the ISG50 generates a log and copies the **startup-config.conf** configuration file to the **startup-config-bad.conf** configuration file and tries the existing **lastgood.conf** configuration file. If there isn't a **lastgood.conf** configuration file or it also has an error, the ISG50 applies the **system-default.conf** configuration file.

You can change the way the **startup-config.conf** file is applied. Include the `setenv-startup stop-on-error off` command. The ISG50 ignores any errors in the **startup-config.conf** file and applies all of the valid commands. The ISG50 still generates a log for any errors.

29.3 File Manager Commands Input Values

The following table explains the values you can input with the file manager commands.

Table 170 File Manager Command Input Values

LABEL	DESCRIPTION
file_name	The name of a file. Use up to 25 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{},.=-).

29.4 File Manager Commands Summary

The following table lists the commands that you can use for file management.

Table 171 File Manager Commands Summary

COMMAND	DESCRIPTION
`apply /conf/`*`file_name.conf`* `[ignore-error] [rollback]`	Has the ISG50 use a specific configuration file. You must still use the `write` command to save your configuration changes to the flash (“non-volatile” or “long term”) memory. Use this command without specify both `ignore-error` and `rollback`: this is not recommended because it would leave the rest of the configuration blank. If the interfaces were not configured before the first error, the console port may be the only way to access the device. Use `ignore-error` without `rollback`: this applies the valid parts of the configuration file and generates error logs for all of the configuration file’s errors. This lets the ISG50 apply most of your configuration and you can refer to the logs for what to fix. Use both `ignore-error` and `rollback`: this applies the valid parts of the configuration file, generates error logs for all of the configuration file’s errors, and starts the ISG50 with a fully valid configuration file. Use `rollback` without `ignore-error`: this gets the ISG50 started with a fully valid configuration file as quickly as possible. You can use the “`apply /conf/system-default.conf`” command to reset the ISG50 to go back to its system defaults.
`copy {/cert | /conf | /packet_trace | /script | /tmp}`*`file_name-a.conf`* `{/cert | /conf | /packet_trace | /script | /tmp}/`*`file_name-b.conf`*	Saves a duplicate of a file on the ISG50 from the source file name to the target file name. Specify the directory and file name of the file that you want to copy and the directory and file name to use for the duplicate. Always copy the file into the same directory.
`copy running-config startup-config`	Saves your configuration changes to the flash (“non-volatile” or “long term”) memory. The ISG50 immediately uses configuration changes made via commands, but if you do not use this command or the write command, the changes will be lost when the ISG50 restarts.
`copy running-config /conf/`*`file_name.conf`*	Saves a duplicate of the configuration file that the ISG50 is currently using. You specify the file name to which to copy.
`delete {/cert | /conf | /packet_trace | /script | /tmp}/`*`file_name`*	Removes a file. Specify the directory and file name of the file that you want to delete.
`dir {/cert | /conf | /packet_trace | /script | /tmp}`	Displays the list of files saved in the specified directory.

Table 171 File Manager Commands Summary (continued)

COMMAND	DESCRIPTION
rename {/cert | /conf | /packet_trace | /script | /tmp}/*old-file_name* {/cert | /conf | /packet_trace | /script | /tmp}/*new-file_name*	Changes the name of a file. Specify the directory and file name of the file that you want to rename. Then specify the directory again followed by the new file name.
rename /script/*old-file_name* /script/*new-file_name*	Changes the name of a shell script.
run /script/*file_name.zysh*	Has the ISG50 execute a specific shell script file. You must still use the write command to save your configuration changes to the flash (“non-volatile” or “long term”) memory.
show running-config	Displays the settings of the configuration file that the system is using.
setenv-startup stop-on-error off	Has the ISG50 ignore any errors in the startup-config.conf file and apply all of the valid commands.
show setenv-startup	Displays whether or not the ISG50 is set to ignore any errors in the startup-config.conf file and apply all of the valid commands.
write	Saves your configuration changes to the flash (“non-volatile” or “long term”) memory. The ISG50 immediately uses configuration changes made via commands, but if you do not use the write command, the changes will be lost when the ISG50 restarts.

29.5 File Manager Command Example

This example saves a back up of the current configuration before applying a shell script file.

```
Router(config)# copy running-config /conf/backup.conf
Router(config)# run /script/vpn_setup.zysh
```

29.6 FTP File Transfer

You can use FTP to transfer files to and from the ISG50 for advanced maintenance and support.

29.6.1 Command Line FTP File Upload

1. Connect to the ISG50.
2. Enter “bin” to set the transfer mode to binary.
3. You can upload the firmware after you log in through FTP. To upload other files, use “cd” to change to the corresponding directory.

4 Use “put” to transfer files from the computer to the ISG50.[1] For example:

In the conf directory, use "put config.conf today.conf” to upload the configuration file (config.conf) to the ISG50 and rename it “today.conf”.

"put 1.00(XL.0).bin” transfers the firmware (1.00(XL.0).bin) to the ISG50.

The firmware update can take up to five minutes. Do not turn off or reset the ISG50 while the firmware update is in progress! If you lose power during the firmware upload, you may need to refer to Section 29.8 on page 333 to recover the firmware.

29.6.2 Command Line FTP Configuration File Upload Example

The following example transfers a configuration file named tomorrow.conf from the computer and saves it on the ISG50 as next.conf.

Note: Uploading a custom signature file named "custom.rules”, overwrites all custom signatures on the ISG50.

Figure 25 FTP Configuration File Upload Example

```
C:\>ftp 192.168.1.1
Connected to 192.168.1.1.
220 FTP Server (ISG50) [192.168.1.1]
User (192.168.1.1:(none)): admin
331 Password required for admin.
Password:
230 User admin logged in.
ftp> cd conf
250 CWD command successful
ftp> bin
200 Type set to I
ftp> put tomorrow.conf next.conf
200 PORT command successful
150 Opening BINARY mode data connection for next.conf
226-Post action ok!!
226 Transfer complete.
ftp: 20231 bytes sent in 0.00Seconds 20231000.00Kbytes/sec.
```

29.6.3 Command Line FTP File Download

1 Connect to the ISG50.

2 Enter “bin” to set the transfer mode to binary.

3 Use “cd” to change to the directory that contains the files you want to download.

4 Use “dir” or “ls” if you need to display a list of the files in the directory.

1. When you upload a custom signature, the ISG50 appends it to the existing custom signatures stored in the "custom.rules” file.

5 Use "get" to download files. For example:

"get vpn_setup.zysh vpn.zysh" transfers the vpn_setup.zysh configuration file on the ISG50 to your computer and renames it "vpn.zysh."

29.6.4 Command Line FTP Configuration File Download Example

The following example gets a configuration file named today.conf from the ISG50 and saves it on the computer as current.conf.

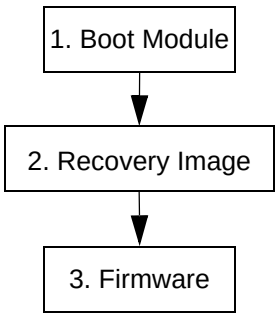
Figure 26 FTP Configuration File Download Example

```
C:\>ftp 192.168.1.1
Connected to 192.168.1.1.
220 FTP Server (ISG50) [192.168.1.1]
User (192.168.1.1:(none)): admin
331 Password required for admin.
Password:
230 User admin logged in.
ftp> bin
200 Type set to I
ftp> cd conf
250 CWD command successful
ftp> get today.conf current.conf
200 PORT command successful
150 Opening BINARY mode data connection for conf/today.conf
(20220 bytes)
226 Transfer complete.
ftp: 20220 bytes received in 0.03Seconds 652.26Kbytes/sec.
```

29.7 ISG50 File Usage at Startup

The ISG50 uses the following files at system startup.

Figure 27 ISG50 File Usage at Startup



1 The boot module performs a basic hardware test. You cannot restore the boot module if it is damaged. The boot module also checks and loads the recovery image. The ISG50 notifies you if the recovery image is damaged.

2 The recovery image checks and loads the firmware. The ISG50 notifies you if the firmware is damaged.

29.8 Notification of a Damaged Recovery Image or Firmware

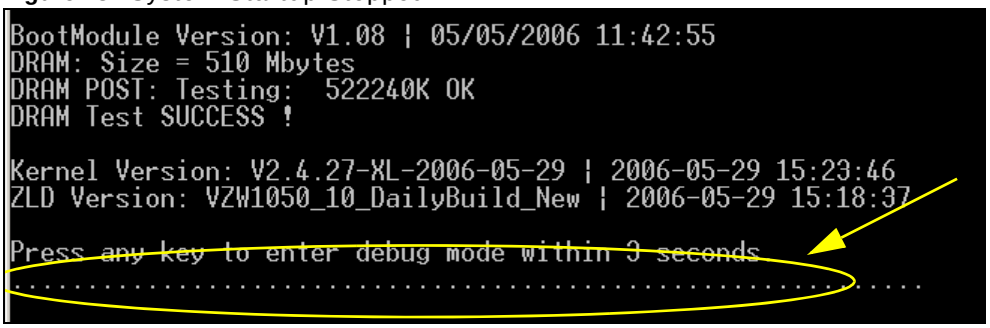
The ISG50's recovery image and/or firmware could be damaged, for example by the power going off during a firmware upgrade. This section describes how the ISG50 notifies you of a damaged recovery image or firmware file. Use this section if your device has stopped responding for an extended period of time and you cannot access or ping it. Note that the ISG50 does not respond while starting up. It takes less than five minutes to start up with the default configuration, but the start up time increases with the complexity of your configuration.

1 Use a console cable and connect to the ISG50 via a terminal emulation program (such as HyperTerminal). Your console session displays the ISG50's startup messages. If you cannot see any messages, check the terminal emulation program's settings (see Section 1.2.1 on page 20) and restart the ISG50.

2 The system startup messages display followed by "Press any key to enter debug mode within 3 seconds."

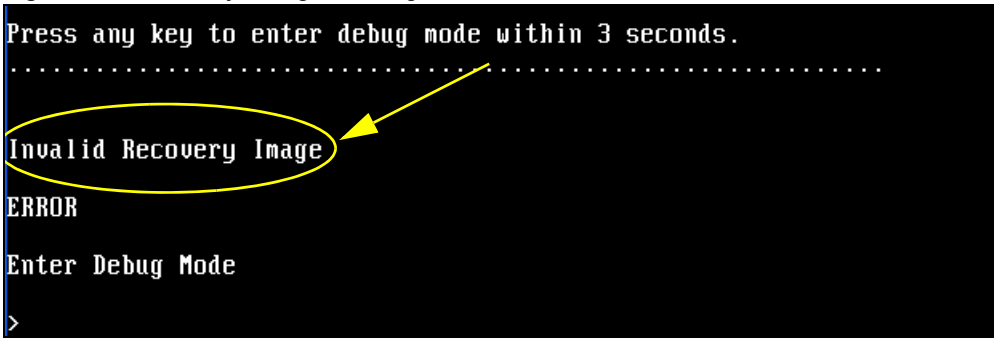
Note: Do not press any keys at this point. Wait to see what displays next.

Figure 28 System Startup Stopped



3 If the console session displays "Invalid Firmware", or "Invalid Recovery Image", or the console freezes at "Press any key to enter debug mode within 3 seconds" for more than one minute, go to Section 29.9 on page 334 to restore the recovery image.

Figure 29 Recovery Image Damaged



4 If “Connect a computer to port 1 and FTP to 192.168.1.1 to upload the new file” displays on the screen, the firmware file is damaged. Use the procedure in Section 29.10 on page 336 to restore it. If the message does not display, the firmware is OK and you do not need to use the firmware recovery procedure.

Figure 30 Firmware Damaged

```
Building ...

Connect a computer to port 1 and FTP to 192.168.1.1 to upload the new file.
```

29.9 Restoring the Recovery Image

This procedure requires the ISG50’s recovery image. Download the firmware package from www.zyxel.com and unzip it. The recovery image uses a .ri extension, for example, "1.01(XL.0)C0.ri". Do the following after you have obtained the recovery image file.

Note: You only need to use this section if you need to restore the recovery image.

1 Restart the ISG50.

2 When “Press any key to enter debug mode within 3 seconds.” displays, press a key to enter debug mode.

Figure 31 Enter Debug Mode

```
BootModule Version: V1.011 | 2007-03-30 12:22:57
DRAM: Size = 510 Mbytes
DRAM POST: Testing:  522240K OK
DRAM Test SUCCESS !

Kernel Version: V2.4.27-kernel-2006-08-21 | 2006-08-21 19:54:00
ZLD Version: V1.01(XL.0) | 2006-09-11 17:41:56

Press any key to enter debug mode within 3 seconds.
.............................
Enter Debug Mode

> 
```

3 Enter `atuk` to initialize the recovery process.If the screen displays “ERROR”, enter `atur` to initialize the recovery process.

Note: You only need to use the atuk or atur command if the recovery image is damaged.

Figure 32 atuk Command for Restoring the Recovery Image

```
> atuk
This command is for restoring the "recovery image" (xxx.ri).
Use This command only when
1) the console displays "Invalid Recovery Image" or
2) the console freezes at "Press any key to enter debug mode within 3 seconds"
   for more than one minute.

Note:
Please exit this command immediately if you do not need to restore the
"recovery image".

Do you want to start the recovery process (Y/N)? (default N)
```

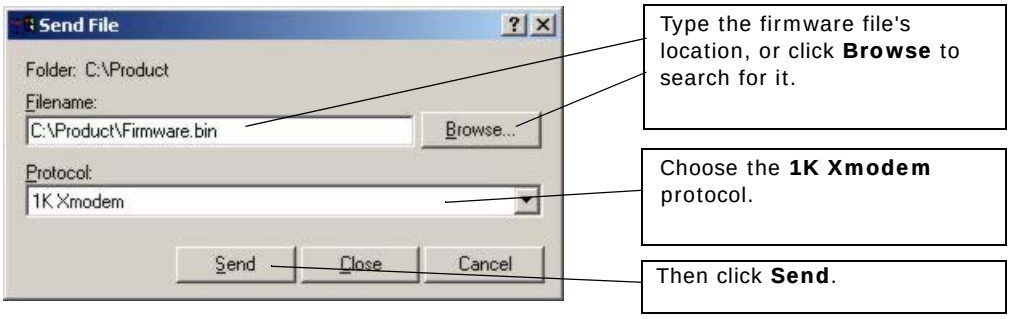
4 Enter Y and wait for the “Starting XMODEM upload” message before activating XMODEM upload on your terminal.

Figure 33 Starting Xmodem Upload

```
Do you want to start the recovery process (Y/N)? (default N)
Starting XMODEM upload (CRC mode)....
C
```

5 This is an example Xmodem configuration upload using HyperTerminal. Click **Transfer**, then **Send File** to display the following screen.

Figure 34 Example Xmodem Upload



6 Wait for about three and a half minutes for the Xmodem upload to finish.

Figure 35 Recovery Image Upload Complete

```
Total  1867264 bytes received.
programming ..................................................
..............................................................
..............................................................
..............................................................
..............................................................
..............................................................

OK

>
```

7 Enter `atgo`. The ISG50 starts up. If “Connect a computer to port 1 and FTP to 192.168.1.1 to upload the new file” displays on the screen, the firmware file is damaged and you need to use the procedure in Section 29.10 on page 336 to recover the firmware.

Figure 36 atgo Debug Command

```
> atgo
Booting...
```

29.10 Restoring the Firmware

This procedure requires the ISG50’s firmware. Download the firmware package from www.zyxel.com and unzip it. The firmware file uses a .bin extension, for example, "1.01(XL.0)C0.bin". Do the following after you have obtained the firmware file.

Note: This section is not for normal firmware uploads. You only need to use this section if you need to recover the firmware.

1 Connect your computer to the ISG50’s port **1** (only port **1** can be used).

2 The ISG50’s FTP server IP address for firmware recovery is 192.168.1.1, so set your computer to use a static IP address from 192.168.1.2 ~192.168.1.254.

3 Use an FTP client on your computer to connect to the ISG50. For example, in the Windows command prompt, type `ftp 192.168.1.1`. Keep the console session connected in order to see when the firmware recovery finishes.

4 Hit enter to log in anonymously.

5 Set the transfer mode to binary (type `bin`).

6 Transfer the firmware file from your computer to the ISG50. Type `put` followed by the path and name of the firmware file. This examples uses `put e:\ftproot\ZLD FW \1.01(XL.0)C0.bin`.

Figure 37 FTP Firmware Transfer Command

```
C:\>ftp 192.168.1.1
Connected to 192.168.1.1.
220-=(<*>)=-.:. (( Welcome to PureFTPd 1.0.11 )) .:.-=(<*>)=-
220-You are user number 1 of 50 allowed
220-Local time is now 21:33 and the load is 0.01. Server port: 21.
220-Only anonymous FTP is allowed here
220 You will be disconnected after 15 minutes of inactivity.
User (192.168.1.1:(none)):
230 Anonymous user logged in
ftp> bi
200 TYPE is now 8-bit binary
ftp> put E:\ftproot\ZLD_FW\100XL0c0\1.00(XL.0)C0.bin_
```

7 Wait for the file transfer to complete.

Figure 38 FTP Firmware Transfer Complete

```
200 PORT command successful
150 Connecting to port 1564
226-87.0 Mbytes free disk space
226-File successfully transferred
226 3.231 seconds (measured here), 10.83 Mbytes per second
ftp: 36708858 bytes sent in 3.23Seconds 11350.91Kbytes/sec.
ftp> _
```

8 After the transfer is complete, “Firmware received” or “ZLD-current received” displays. Wait (up to four minutes) while the ISG50 recovers the firmware.

Figure 39 Firmware Received and Recovery Started

```
Firmware received ...

[Update Filesystem]
       Updating Code
       ..
```

9 The console session displays “done” when the firmware recovery is complete. Then the ISG50 automatically restarts.

Figure 40 Firmware Recovery Complete and Restart

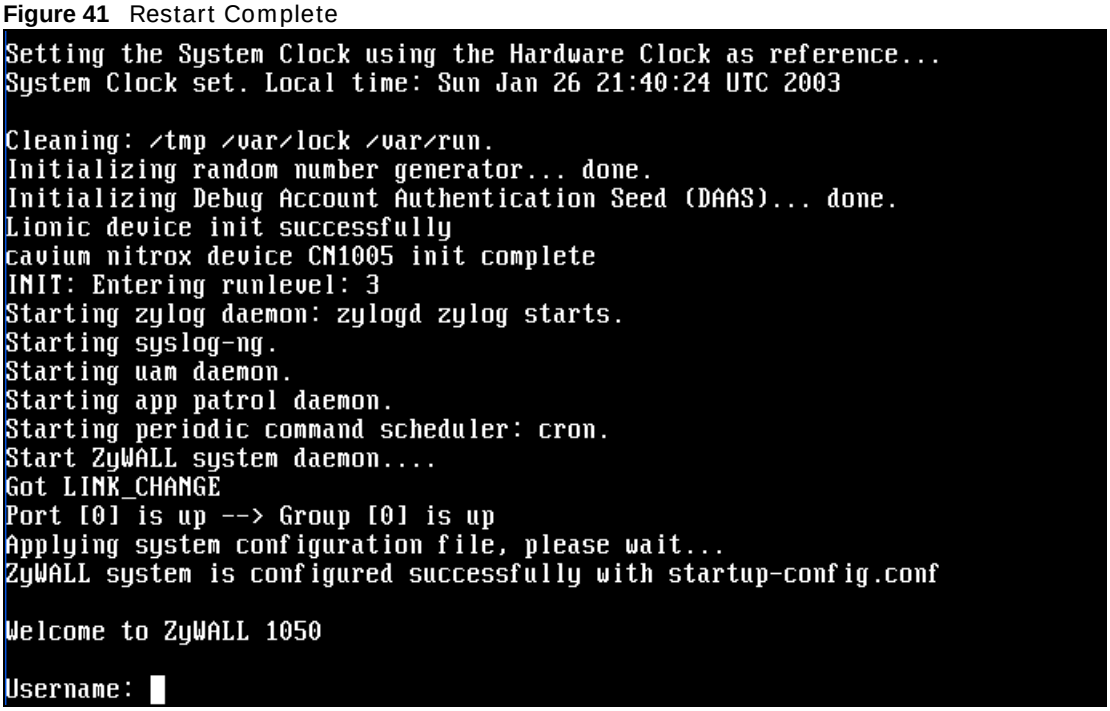
```
.....
.....
.....
.....
.....
.....
.....
       done

[Update Kernel]
       Extracting Kernel Image
       ..
       done
       Writing Kernel Image ... done

[Update BootModule]
       Extracting BootModule Image
       .
       done
       Writing BootModule
       .....
.....                                  done
Restarting system.
```

10 The username prompt displays after the ISG50 starts up successfully. The firmware recovery process is now complete and the ISG50 is ready to use.

Figure 41 Restart Complete



30

Logs

This chapter provides information about the ISG50's logs.

Note: When the system log reaches the maximum number of log messages, new log messages automatically overwrite existing log messages, starting with the oldest existing log message first.

See the User's Guide for the maximum number of system log messages in the ISG50.

30.1 Log Commands Summary

The following table describes the values required for many log commands. Other values are discussed with the corresponding commands.

Table 172 Input Values for Log Commands

LABEL	DESCRIPTION
module_name	The name of the category; `kernel`, `syslog`, ... The `default` category includes debugging messages generated by open source software. The `all` category includes all messages in all categories.

The following sections list the logging commands.

30.1.1 Log Entries Commands

This table lists the commands to look at log entries.

Table 173 logging Commands: Log Entries

COMMAND	DESCRIPTION
`show logging entries [priority` *`pri`*`] [category` *`module_name`*`] [srcip` *`ip`*`] [dstip` *`ip`*`] [service` *`service_name]`* `[begin <1..512> end <1..512>] [keyword` *`keyword`*`]`	Displays the selected entries in the system log. PRI: alert | crit | debug | emerg | error | info | notice | warn *keyword*: You can use alphanumeric and `()+/:=?!*#@$_%-` characters, and it can be up to 63 characters long.This searches the message, source, destination, and notes fields.
`show logging entries field` *`field`* `[begin <1..512> end <1..512>]`	Displays the selected fields in the system log. *field*: time | msg | src | dst | note | pri | cat | all

30.1.2 System Log Commands

This table lists the commands for the system log settings.

Table 174 logging Commands: System Log Settings

COMMAND	DESCRIPTION
`show logging status system-log`	Displays the current settings for the system log.
`logging system-log category` *`module_name`* `{disable | level normal | level all}`	Specifies what kind of information, if any, is logged in the system log and debugging log for the specified category.
`[no] logging system-log suppression interval <10..600>`	Sets the log consolidation interval for the system log. The `no` command sets the interval to ten.
`[no] logging system-log suppression`	Enables log consolidation in the system log. The `no` command disables log consolidation in the system log.
`[no] connectivity-check continuous-log activate`	Has the ISG50 generate a log for each connectivity check. The no command has the ISG50 only log the first connectivity check.
`show connectivity-check continuous-log status`	Displays whether or not the ISG50 generates a log for each connectivity check.
`clear logging system-log buffer`	Clears the system log.

30.1.2.1 System Log Command Examples

The following command displays the current status of the system log.

```
Router(config)# show logging status system-log
78 events logged
suppression active  : yes
suppression interval: 10
category settings   :
    user              : normal , myZyXEL.com       : normal ,
    zysh              : normal , bwm               : normal ,
    ike               : normal , ipsec             : normal ,
    firewall          : normal , sessions-limit    : normal ,
    policy-route      : normal , built-in-service  : normal ,
    system            : normal , system-monitoring : no     ,
    connectivity-check: normal , routing-protocol  : normal ,
    nat               : normal , pki               : normal ,
    interface         : normal , interface-statistics: no     ,
    account           : normal , port-grouping     : normal ,
    force-auth        : normal , traffic-log       : no     ,
    file-manage       : normal , adp               : normal ,
    cellular          : normal , usb-storage       : normal ,
    daily-report      : normal , ipmac-binding     : normal ,
    dhcp              : normal , auth-policy       : normal ,
    pbx-call-service  : normal , pbx-dialplan      : normal ,
    pbx-dsp           : normal , pbx-default       : normal ,
    pbx-sip           : normal , pbx-supp-service  : normal ,
    pbx-trunk         : normal , pbx-physical-port : normal ,
    default           : all    ,
```

30.1.3 Debug Log Commands

This table lists the commands for the debug log settings.

Table 175 logging Commands: Debug Log Settings

COMMAND	DESCRIPTION
show logging debug status	Displays the current settings for the debug log.
show logging debug entries [priority *pri]* [category *module_name*] [srcip *ip*] [dstip *ip*] [service *service_name*] [begin <1..512> end <1..512>] [keyword *keyword*]	Displays the selected entries in the debug log. *pri*: alert | crit | debug | emerg | error | info | notice | warn *keyword*: You can use alphanumeric and ()+/ :=?!*#@$_%- characters, and it can be up to 63 characters long.This searches the message, source, destination, and notes fields.
show logging debug entries field *field* [begin <1..1024> end <1..1024>]	Displays the selected fields in the debug log. *field*: time | msg | src | dst | note | pri | cat | all
[no] logging debug suppression	Enables log consolidation in the debug log. The no command disables log consolidation in the debug log.
[no] logging debug suppression interval <10..600>	Sets the log consolidation interval for the debug log. The no command sets the interval to ten.
clear logging debug buffer	Clears the debug log.

This table lists the commands for the remote syslog server settings.

Table 176 logging Commands: Remote Syslog Server Settings

COMMAND	DESCRIPTION
show logging status syslog	Displays the current settings for the remote servers.
[no] logging syslog <1..4>	Enables the specified remote server. The no command disables the specified remote server.
[no] logging syslog <1..4> address {*ip* | *hostname*}	Sets the URL or IP address of the specified remote server. The no command clears this field. *hostname*: You may up to 63 alphanumeric characters, dashes (-), or periods (.), but the first character cannot be a period.
[no] logging syslog <1..4> {disable | level normal | level all}	Specifies what kind of information, if any, is logged for the specified category.
[no] logging syslog <1..4> facility {local_1 | local_2 | local_3 | local_4 | local_5 | local_6 | local_7}	Sets the log facility for the specified remote server. The no command sets the facility to local_1.
[no] logging syslog <1..4> format {cef | vrpt}	Sets the format of the log information. cef: Common Event Format, syslog-compatible format. vrpt: ZyXEL's Vantage Report, syslog-compatible format.

This table lists the commands for setting how often to send information to the VRPT (ZyXEL's Vantage Report) server.

Table 177 logging Commands: VRPT Settings

COMMAND	DESCRIPTION
vrpt send device information interval <15..3600>	Sets the interval (in seconds) for how often the ISG50 sends a device information log to the VRPT server.
vrpt send interface statistics interval <15..3600>	Sets the interval (in seconds) for how often the ISG50 sends an interface statistics log to the VRPT server.
vrpt send system status interval <15..3600>	Sets the interval (in seconds) for how often the ISG50 sends a system status log to the VRPT server.
show vrpt send device information interval	Displays the interval (in seconds) for how often the ISG50 sends a device information log to the VRPT server.
show vrpt send interface statistics interval	Displays the interval (in seconds) for how often the ISG50 sends an interface statistics log to the VRPT server.
show vrpt send system status interval	Displays the interval (in seconds) for how often the ISG50 sends a system status log to the VRPT server.

30.1.4 E-mail Profile Commands

This table lists the commands for the e-mail profile settings.

Table 178 logging Commands: E-mail Profile Settings

COMMAND	DESCRIPTION
show logging status mail	Displays the current settings for the e-mail profiles.
[no] logging mail <1..2>	Enables the specified e-mail profile. The no command disables the specified e-mail profile.
[no] logging mail <1..2> address {*ip* | *hostname*}	Sets the URL or IP address of the mail server for the specified e-mail profile. The no command clears the mail server field. *hostname*: You may up to 63 alphanumeric characters, dashes (-), or periods (.), but the first character cannot be a period.
logging mail <1..2> sending_now	Sends mail for the specified e-mail profile immediately, according to the current settings.
[no] logging mail <1..2> authentication	Enables SMTP authentication. The no command disables SMTP authentication.
[no] logging mail <1..2> authentication username *username* password *password*	Sets the username and password required by the SMTP mail server. The no command clears the username and password fields. *username*: You can use alphanumeric characters, underscores (_), and dashes (-), and it can be up to 31 characters long. *password*: You can use most printable ASCII characters. You cannot use square brackets [ ], double quotation marks (“), question marks (?), tabs or spaces. It can be up to 31 characters long.

Table 178 logging Commands: E-mail Profile Settings (continued)

COMMAND	DESCRIPTION
[no] logging mail <1..2> {send-log-to | send-alerts-to} *e_mail*	Sets the e-mail address for logs or alerts. The no command clears the specified field. *e_mail*: You can use up to 63 alphanumeric characters, underscores (_), or dashes (-), and you must use the @ character.
[no] logging mail <1..2> subject *subject*	Sets the subject line when the ISG50 mails to the specified e-mail profile. The no command clears this field. *subject*: You can use up to 60 alphanumeric characters, underscores (_), dashes (-), or !@#$%*()+=;:',./ characters.
[no] logging mail <1..2> category *module_name* level {alert | all}	Specifies what kind of information is logged for the specified category. The no command disables logging for the specified category.
[no] logging mail <1..2> port <1..65535>	Sets the port number of the mail server for the specified e-mail profile.
[no] logging mail <1..2> schedule {full | hourly}	Sets the e-mail schedule for the specified e-mail profile. The no command clears the schedule field.
logging mail <1..2> schedule daily hour <0..23> minute <0..59>	Sets a daily e-mail schedule for the specified e-mail profile.
logging mail <1..2> schedule weekly day *day* hour <0..23> minute <0..59>	Sets a weekly e-mail schedule for the specified e-mail profile. *day*: sun | mon | tue | wed | thu | fri | sat

30.1.4.1 E-mail Profile Command Examples

The following commands set up e-mail log 1.

```
Router# configure terminal
Router(config)# logging mail 1 address mail.zyxel.com.tw
Router(config)# logging mail 1 subject AAA
Router(config)# logging mail 1 authentication username lachang.li password
XXXXXX
Router(config)# logging mail 1 send-log-to lachang.li@zyxel.com.tw
Router(config)# logging mail 1 send-alerts-to lachang.li@zyxel.com.tw
Router(config)# logging mail 1 from lachang.li@zyxel.com.tw
Router(config)# logging mail 1 schedule weekly day mon hour 3 minute 3
Router(config)# logging mail 1
```

30.1.5 Console Port Logging Commands

This table lists the commands for the console port settings.

Table 179 logging Commands: Console Port Settings

COMMAND	DESCRIPTION
show logging status console	Displays the current settings for the console log. (This log is not discussed above.)
[no] logging console	Enables the console log. The no command disables the console log.

Table 179 logging Commands: Console Port Settings (continued)

COMMAND	DESCRIPTION
`logging console category` *`module_name`* `level {alert | crit | debug | emerg | error | info | notice | warn}`	Controls whether or not debugging information for the specified priority is displayed in the console log, if logging for this category is enabled.
`[no] logging console category` *`module_name`*	Enables logging for the specified category in the console log. The `no` command disables logging.

31

Reports and Reboot

This chapter provides information about the report associated commands and how to restart the ISG50 using commands. It also covers the daily report e-mail feature.

31.1 Report Commands Summary

The following sections list the report and session commands.

31.1.1 Report Commands

This table lists the commands for reports.

Table 180 report Commands

COMMAND	DESCRIPTION
`[no] report`	Begins data collection. The `no` command stops data collection.
`show report status`	Displays whether or not the ISG50 is collecting data and how long it has collected data.
`clear report [`*`interface_name`*`]`	Clears the report for the specified interface or for all interfaces.
`show report [`*`interface_name`* `{ip | service | url}]`	Displays the traffic report for the specified interface and controls the format of the report. Formats are: `ip` - traffic by IP address and direction `service` - traffic by service and direction `url` - hits by URL

31.1.2 Report Command Examples

The following commands start collecting data, display the traffic reports, and stop collecting data.

```
Router# configure terminal
Router(config)# show report ge1 ip
No. IP Address      User                  Amount          Direction
=================================================================
1   192.168.1.4     admin                 1273(bytes)     Outgoing
2   192.168.1.4     admin                 711(bytes)      Incoming
Router(config)# show report ge1 service
No. Port  Service          Amount          Direction
=================================================================
1   21    ftp              1273(bytes)     Outgoing
2   21    ftp              711(bytes)      Incoming
Router(config)# show report ge1 url
No. Hit        URL
=================================================================
1   1          140.114.79.60
Router(config)# show report status
Report status: on
Collection period: 0 days 0 hours 0 minutes 18 seconds
```

31.1.3 Session Commands

This table lists the command to display the current sessions for debugging or statistical analysis.

Table 181 session Commands

COMMAND	DESCRIPTION
show conn [user {*username*|any|unknown}] [service {*service-name*|any|unknown}] [source {*ip*|any}] [destination {*ip*|any}] [begin <1..128000>] [end <1..128000>]	Displays information about the selected sessions or about all sessions. You can look at all the active sessions or filter the information by user name, service object, source IP, destination IP, or session number(s). any means all users, services and IP addresses resepectively. unknow means unknown users and services resepectively.
show conn ip-traffic destination	Displays information about traffic session sorted by the destination.
show conn ip-traffic source	Displays information about traffic session sorted by the source.
show conn status	Displays the number of active sessions.

31.2 Email Daily Report Commands

The following table identifies the values used in some of these commands. Other input values are discussed with the corresponding commands.

Table 182 Input Values for Email Daily Report Commands

LABEL	DESCRIPTION
e_mail	An e-mail address. You can use up to 80 alphanumeric characters, underscores (_), periods (.), or dashes (-), and you must use the @ character.

Use these commands to have the ISG50 e-mail you system statistics every day. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 183 Email Daily Report Commands

COMMAND	DESCRIPTION
`show daily-report status`	Displays the e-mail daily report settings.
`daily-report`	Enters the sub-command mode for configuring daily e-mail reports settings.
`[no] activate`	Turns daily e-mail reports on or off.
`smtp-address {`*`ip`*` | `*`hostname`*`}`	Sets the SMTP mail server IP address or domain name.
`[no] smtp-auth activate`	Enables or disables SMTP authentication.
`smtp-auth username `*`username`*` password `*`password`*	Sets the username and password for SMTP authentication.
`no smtp-address`	Resets the SMTP mail server configuration.
`no smtp-auth username`	Resets the authentication configuration.
`mail-subject set `*`subject`*	Configures the subject of the report e-mails.
`no mail-subject set`	Clears the configured subject for the report e-mails.
`[no] mail-subject append system-name`	Determines whether the system name will be appended to the subject of report mail.
`[no] mail-subject append date-time`	Determine whether the sending date-time will be appended at subject of the report e-mails.
`mail-from `*`e_mail`*	Sets the sender value of the report e-mails.
`mail-to-1 `*`e_mail`*	Sets to whom the ISG50 sends the report e-mails (up to five recipients).
`mail-to-2 `*`e_mail`*	See above.
`mail-to-3 `*`e_mail`*	See above.
`mail-to-4 `*`e_mail`*	See above.
`mail-to-5 `*`e_mail`*	See above.
`[no] item cpu-usage`	Determines whether or not CPU usage statistics are included in the report e-mails.
`[no] item mem-usage`	Determines whether or not memory usage statistics are included in the report e-mails.
`[no] item session-usage`	Determines whether or not session usage statistics are included in the report e-mails.
`[no] item port-usage`	Determines whether or not port usage statistics are included in the report e-mails.

Table 183 Email Daily Report Commands (continued)

COMMAND	DESCRIPTION
[no] item traffic-report	Determines whether or not network traffic statistics are included in the report e-mails.
schedule hour <0..23> minute <00..59>	Sets the time for sending out the report e-mails.
[no] reset-counter	Determines whether or not to clear the report statistics data after successfully sending out a report e-mail.
send-now	Sends the daily e-mail report immediately. let user actively send out the report e-mails.
reset-counter-now	Discards all report data and starts all of the counters over at zero.
exit	Leaves the sub-command mode.

31.2.1 Email Daily Report Example

This example sets the ISG50 to send a daily report e-mail.

```
Router(config)# daily-report
Router(config-daily-report)# no activate
Router(config-daily-report)# smtp-address example-SMTP-mail-server.com
Router(config-daily-report)# mail-subject set test subject
Router(config-daily-report)# no mail-subject append system-name
Router(config-daily-report)# mail-subject append date-time
Router(config-daily-report)# mail-from my-email@example.com
Router(config-daily-report)# example-administrator@example.com
Router(config-daily-report)# no mail-to-2
Router(config-daily-report)# no mail-to-3
Router(config-daily-report)# mail-to-4 my-email@example.com
Router(config-daily-report)# no mail-to-5
Router(config-daily-report)# smtp-auth activate
Router(config-daily-report)# smtp-auth username 12345 password pass12345
Router(config-daily-report)# schedule hour 13 minutes 57
Router(config-daily-report)# no schedule reset-counter
Router(config-daily-report)# item cpu-usage
Router(config-daily-report)# item mem-usage
Router(config-daily-report)# item port-usage
Router(config-daily-report)# item session-usage
Router(config-daily-report)# item traffic-report
Router(config-daily-report)# activate
Router(config-daily-report)# exit
Router(config)#
```

This displays the email daily report settings and has the ISG50 send the report.

```
Router(config)# show daily-report status
email daily report status
=========================
activate: yes
scheduled time: 13:57
reset counter: no
smtp address: example-SMTP-mail-server.com
smtp port: 25
smtp auth: yes
smtp username: 12345
smtp password: pass12345
mail subject:  test subject
append system name: no
append date time: yes
mail from: my-email@example.com
mail-to-1: example-administrator@example.com
mail-to-2:
mail-to-3:
mail-to-4: my-email@example.com
mail-to-5:
cpu-usage: yes
mem-usage: yes
session-usage: yes
port-usage: yes
traffic-report: yes

Router(config)# daily-report send-now
```

31.3 Reboot

Use this to restart the device (for example, if the device begins behaving erratically).

If you made changes in the CLI, you have to use the `write` command to save the configuration before you reboot. Otherwise, the changes are lost when you reboot.

Use the `reboot` command to restart the device.

32

Session Timeout

Use these commands to modify and display the session timeout values. You must use the `configure terminal` command before you can use these commands.

Table 184 Session Timeout Commands

COMMAND	DESCRIPTION
`session timeout {udp-connect <1..300> | udp-deliver <1..300> | icmp <1..300>}`	Sets the timeout for UDP sessions to connect or deliver and for ICMP sessions.
`session timeout session {tcp-established | tcp-synrecv | tcp-close | tcp-finwait | tcp-synsent | tcp-closewait | tcp-lastack | tcp-timewait} <1..300>`	Sets the timeout for TCP sessions in the ESTABLISHED, SYN_RECV, FIN_WAIT, SYN_SENT, CLOSE_WAIT, LAST_ACK, or TIME_WAIT state.
`show session timeout {icmp | tcp-timewait | udp}`	Displays ICMP, TCP, and UDP session timeouts.

The following example sets the UDP session connect timeout to 10 seconds, the UDP deliver session timeout to 15 seconds, and the ICMP timeout to 15 seconds.

```
Router(config)# session timeout udp-connect 10
Router(config)# session timeout udp-deliver 15
Router(config)# session timeout icmp 15
Router(config)# show session timeout udp
UDP session connect timeout: 10 seconds
UDP session deliver timeout: 15 seconds
Router(config)# show session timeout icmp
ICMP session timeout: 15 seconds
```

33

Diagnostics

This chapter covers how to use the diagnostics feature.

33.1 Diagnostics

The diagnostics feature provides an easy way for you to generate a file containing the ISG50's configuration and diagnostic information. You may need to generate this file and send it to customer support during troubleshooting.

33.2 Diagnosis Commands

The following table lists the commands that you can use to have the ISG50 collect diagnostics information. Use the `configure terminal` command to enter the configuration mode to be able to use these commands.

Table 185 diagnosis Commands

COMMAND	DESCRIPTION
`diag-info collect`	Has the ISG50 create a new diagnostic file.
`show diag-info`	Displays the name, size, and creation date (in yyyy-mm-dd hh:mm:ss format) of the diagnostic file.

33.3 Diagnosis Commands Example

The following example creates a diagnostic file and displays its name, size, and creation date.

```
Router# configure terminal
Router(config)# diag-info collect
Please wait, collecting information
Router(config)# show diag-info
Filename  : diaginfo-20070423.tar.bz2
File size : 1259 KB
Date      : 2007-04-23 09:55:09
```

34

Packet Flow Explore

This chapter covers how to use the packet flow explore feature.

34.1 Packet Flow Explore

Use this to get a clear picture on how the ISG50 determines where to forward a packet and how to change the source IP address of the packet according to your current settings. This function provides you a summary of all your routing and SNAT settings and helps troubleshoot the related problems.

34.2 Packet Flow Explore Commands

The following table lists the commands that you can use to have the ISG50 display routing and SNAT related settings.

Table 186 Packet Flow Explore Commands

COMMAND	DESCRIPTION
`show route order`	Displays the order of routing related functions the ISG50 checks for packets. Once a packet matches the criteria of a routing rule, the ISG50 takes the corresponding action and does not perform any further flow checking.
`show system snat order`	Displays the order of SNAT related functions the ISG50 checks for packets. Once a packet matches the criteria of an SNAT rule, the ISG50 uses the corresponding source IP address and does not perform any further flow checking.
`show system route policy-route`	Displays activated policy routes.
`show system route nat-1-1`	Displays activated 1-to-1 NAT rules.
`show system route site-to-site-vpn`	Displays activated site-to-site VPN rules.
`show system route dynamic-vpn`	Displays activated dynamic VPN rules.
`show system route default-wan-trunk`	Displays the default WAN trunk settings.
`show ip route static-dynamic`	Displays activated static-dynamic routes.
`show system snat policy-route`	Displays activated policy routes which use SNAT.
`show system snat nat-1-1`	Displays activated NAT rules which use SNAT.

Table 186 Packet Flow Explore Commands (continued)

COMMAND	DESCRIPTION
`show system snat nat-loopback`	Displays activated activated NAT rules which use SNAT with NAT loopback enabled.
`show system snat default-snat`	Displays the default WAN trunk settings.

34.3 Packet Flow Explore Commands Example

The following example shows all routing related functions and their order.

```
Router> show route order
route order: Policy Route, Direct Route, 1-1 SNAT, SiteToSite VPN, Dynamic
VPN, Static-Dynamic Route, Default WAN Trunk, Main Route
```

The following example shows all SNAT related functions and their order.

```
Router> show system snat order
snat order: Policy Route SNAT, 1-1 SNAT, Loopback SNAT, Default SNAT
```

The following example shows all SNAT related functions and their order.

```
Router> show system route policy-route
No.  PR NO. Source   Destination      Incoming     DSCP   Service   Nexthop
Type        Nexthop Info
================================================================================
```

The following example shows all activated 1-to-1 SNAT rules.

```
Router> show system route nat-1-1
No.  VS Name         Source     Destination   Outgoing        Gateway
================================================================================
```

The following example shows all activated site-to-site VPN rules.

```
Router> show system route site-to-site-vpn
No.  Source         Destination          VPN Tunnel
================================================================================
```

The following example shows all activated dynamic VPN rules.

```
Router> show system route dynamic-vpn
No.  Source         Destination             VPN Tunnel
================================================================================
```

The following example shows the default WAN trunk's settings.

```
Router> show system route default-wan-trunk
No.  Source          Destination     Trunk
================================================================================
1    any             any             trunk_ex
```

The following example shows all activated dynamic VPN rules.

```
Router> show system route dynamic-vpn
No.  Source         Destination             VPN Tunnel
================================================================================
```

The following example shows all activated static-dynamic VPN rules.

```
Router> show ip route static-dynamic
Flags: A - Activated route, S - Static route, C - directly Connected
       O - OSPF derived, R - RIP derived, G - selected Gateway
       ! - reject, B - Black hole, L - Loop

IP Address/Netmask    Gateway          IFace           Metric    Flags
Persis
t
================================================================================
0.0.0.0/0             10.1.1.254       wan1            0         ASG      -
```

The following example shows all activated policy routes which use SNAT.

```
Router> show system snat policy-route
No.  PR NO. Outgoing        SNAT
================================================================================
```

The following example shows all activated 1-to-1 NAT rules.

```
Router> show system snat nat-1-1
No.  VS Name     Source        Destination   Outgoing        SNAT
================================================================================
```

The following example shows all activated policy routes which use SNAT and enable NAT loopback..

```
Router> show system snat nat-loopback
Note: Loopback SNAT will be only applied only when the initiator is located
at the network which the server locates at

No.  VS Name        Source        Destination     SNAT
================================================================================
```

The following example shows all activated 1-to-1 NAT rules.

```
Router> show system snat nat-1-1
No.  VS Name     Source        Destination   Outgoing        SNAT
================================================================================
```

The following example shows the default WAN trunk settings.

```
Router> show system snat default-snat
Incoming                Outgoing                SNAT
================================================================================
Internal Interface      External Interface      Outgoing Interface IP


Internal Interfaces: lan1, hidden, lan2, dmz
External Interfaces: wan1, wan2, wan1_ppp, wan2_ppp
Router>
```

35

Maintenance Tools

Use the maintenance tool commands to check the conditions of other devices through the ISG50. The maintenance tools can help you to troubleshoot network problems.

Here are maintenance tool commands that you can use in privilege mode.

Table 187 Maintenance Tools Commands in Privilege Mode

COMMAND	DESCRIPTION
packet-trace [interface *interface_name*] [ip-proto {<0..255> | *protocol_name* | any}] [src-host {*ip* | *hostname* | any}] [dst-host {*ip* | *hostname* | any}] [port {<1..65535> | any}] [file] [duration <1..3600>] [extension-filter *filter_extension*] traceroute {*ip* | *hostname*}	Sends traffic through the specified interface with the specified protocol, source address, destination address, and/or port number. If you specify `file`, the ISG50 dumps the traffic to `/packet_trace/packet_trace_interface`. Use FTP to retrieve the files (see Section 29.6 on page 330). If you do not assign the duration, the ISG50 keeps dumping traffic until you use Ctrl-C. Use the extension filter to extend the use of this command. *protocol_name*: You can use the name, instead of the number, for some IP protocols, such as `tcp`, `udp`, `icmp`, and so on. The names consist of 1-16 alphanumeric characters, underscores (_), or dashes (-). The first character cannot be a number. *hostname*: You can use up to 252 alphanumeric characters, dashes (-), or periods (.). The first character cannot be a period. *filter_extension*: You can use 1-256 alphanumeric characters, spaces, or '()+,/:=?;!*#@$_%.- characters.
traceroute {*ip* | *hostname*}	Displays the route taken by packets to the specified destination. Use `Ctrl+c` when you want to return to the prompt.
[no] packet-capture activate	Performs a packet capture that captures network traffic going through the set interface(s). Studying these packet captures may help you identify network problems. The no command stops the running packet capture on the ISG50. Note: Use the `packet-capture configure` command to configure the packet-capture settings before using this command.
packet-capture configure	Enters the sub-command mode.

Table 187 Maintenance Tools Commands in Privilege Mode (continued)

COMMAND	DESCRIPTION
duration <0..300>	Sets a time limit in seconds for the capture. The ISG50 stops the capture and generates the capture file when either this period of time has passed or the file reaches the size specified using the files-size command below. 0 means there is no time limit.
file-suffix <*profile_name*>	Specifies text to add to the end of the file name (before the dot and filename extension) to help you identify the packet capture files. Modifying the file suffix also avoids making new capture files that overwrite existing files of the same name. The file name format is “interface name-file suffix.cap”, for example “vlan2-packet-capture.cap”.
files-size <1..10000>	Specify a maximum size limit in kilobytes for the total combined size of all the capture files on the ISG50, including any existing capture files and any new capture files you generate. The ISG50 stops the capture and generates the capture file when either the file reaches this size or the time period specified (using the duration command above) expires. Note: If you have existing capture files you may need to set this size larger or delete existing capture files.
host-ip {*ip-address* | *profile_name* | any>	Sets a host IP address or a host IP address object for which to capture packets. any means to capture packets for all hosts.
host-port <0..65535>	If you set the IP Type to any, tcp, or udp using the ip-type command below, you can specify the port number of traffic to capture.
iface {add | del} {*interface_name* | *virtual_interface_name*}	Adds or deletes an interface or a virtual interface for which to capture packets to the capture interfaces list.
ip-type {icmp | igmp | igrp | pim | ah | esp | vrrp | udp | tcp | any}	Sets the protocol of traffic for which to capture packets. any means to capture packets for all types of traffic.
snaplen <68..1512>	Specifies the maximum number of bytes to capture per packet. The ISG50 automatically truncates packets that exceed this size. As a result, when you view the packet capture files in a packet analyzer, the actual size of the packets may be larger than the size of captured packets.
storage <internal|usbstorage>	Sets to have the ISG50 only store packet capture entries on the ISG50 (internal) or on a USB storage connected to the ISG50.
ring-buffer <enable|disable>	Enables or disables the ring buffer used as a temporary storage.
split-size <1..2048>	Specify a maximum size limit in megabytes for individual packet capture files. After a packet capture file reaches this size, the ISG50 starts another packet capture file.
show packet-capture status	Displays whether a packet capture is ongoing.
show packet-capture config	Displays current packet capture settings.

35.0.1 Command Examples

Some packet-trace command examples are shown below.

```
Router# packet-trace duration 3
tcpdump: listening on eth0
19:24:43.239798 192.168.1.10 > 192.168.1.1: icmp: echo request
19:24:43.240199 192.168.1.1 > 192.168.1.10: icmp: echo reply
19:24:44.258823 192.168.1.10 > 192.168.1.1: icmp: echo request
19:24:44.259219 192.168.1.1 > 192.168.1.10: icmp: echo reply
19:24:45.268839 192.168.1.10 > 192.168.1.1: icmp: echo request
19:24:45.269238 192.168.1.1 > 192.168.1.10: icmp: echo reply

6 packets received by filter
0 packets dropped by kernel
```

```
Router# packet-trace interface ge2 ip-proto icmp file extension-filter -s
-> 500 -n
tcpdump: listening on eth1
07:24:07.898639 192.168.105.133 > 192.168.105.40: icmp: echo request (DF)
07:24:07.900450 192.168.105.40 > 192.168.105.133: icmp: echo reply
07:24:08.908749 192.168.105.133 > 192.168.105.40: icmp: echo request (DF)
07:24:08.910606 192.168.105.40 > 192.168.105.133: icmp: echo reply

8 packets received by filter
0 packets dropped by kernel
```

```
Router# packet-trace interface ge2 ip-proto icmp file extension-filter
-> and src host 192.168.105.133 and dst host 192.168.105.40 -s 500 -n
tcpdump: listening on eth1
07:26:51.731558 192.168.105.133 > 192.168.105.40: icmp: echo request (DF)
07:26:52.742666 192.168.105.133 > 192.168.105.40: icmp: echo request (DF)
07:26:53.752774 192.168.105.133 > 192.168.105.40: icmp: echo request (DF)
07:26:54.762887 192.168.105.133 > 192.168.105.40: icmp: echo request (DF)

8 packets received by filter
0 packets dropped by kernel
```

```
Router# traceroute www.zyxel.com
traceroute to www.zyxel.com (203.160.232.7), 30 hops max, 38 byte packets
 1  172.23.37.254  3.049 ms  1.947 ms  1.979 ms
 2  172.23.6.253  2.983 ms  2.961 ms  2.980 ms
 3  172.23.6.1  5.991 ms  5.968 ms  6.984 ms
 4  * * *
```

Here are maintenance tool commands that you can use in configure mode.

Table 188 Maintenance Tools Commands in Configuration Mode

COMMAND	DESCRIPTION
show arp-table	Displays the current Address Resolution Protocol table.
arp IP *mac_address*	Edits or creates an ARP table entry.
no arp *ip*	Removes an ARP table entry.

The following example creates an ARP table entry for IP address 192.168.1.10 and MAC address 01:02:03:04:05:06. Then it shows the ARP table and finally removes the new entry.

```
Router# arp 192.168.1.10 01:02:03:04:05:06
Router# show arp-table
Address                HWtype  HWaddress          Flags Mask            Iface
192.168.1.10            ether   01:02:03:04:05:06   CM                    ge1
172.23.19.254           ether   00:04:80:9B:78:00   C                     ge2
Router# no arp 192.168.1.10
Router# show arp-table
Address                HWtype  HWaddress          Flags Mask            Iface
192.168.1.10                    (incomplete)                             ge1
172.23.19.254           ether   00:04:80:9B:78:00   C                     ge2
```

35.0.1.1 Packet Capture Command Example

The following examples show how to configure packet capture settings and perform a packet capture. First you have to check whether a packet capture is running. This example shows no other packet capture is running. Then you can also check the current packet capture settings.

```
Router(config)# show packet-capture status
capture status: off
Router(config)#
Router(config)# show packet-capture config
iface: wan1,lan2,wan2
ip-type: any
host-port: 0
host-ip: any
file-suffix: Example
snaplen: 1500
duration: 150
file-size: 10000
split-size: 2
ring-buffer: 0
storage: 0
```

Then configure the following settings to capture packets going through the ISG50's WAN1 interface only (this means you have to remove LAN2 and WAN2 from the iface list).

- IP address: any
- Host IP: any
- Host port: any (then you do not need to configure this setting)
- File suffix: Example

- File size: 10000 byes
- Duration: 150 seconds
- Save the captured packets to: USB storage device
- Use the ring buffer: no
- The maximum size of a packet capture file: 100 MB

```
Router(config)# packet-capture configure
Router(packet-capture)# iface add wan1
Router(packet-capture)# iface del lan2
Router(packet-capture)# iface del wan2
Router(packet-capture)# ip-type any
Router(packet-capture)# host-ip any
Router(packet-capture)# file-suffix Example
Router(packet-capture)# files-size 10000
Router(packet-capture)# duration 150
Router(packet-capture)# storage usbstorage
Router(packet-capture)# ring-buffer disable
Router(packet-capture)# split-size 100
Router(packet-capture)#
```

Exit the sub-command mode and have the ISG50 capture packets according to the settings you just configured.

```
Router(packet-capture)# exit
Router(config)# packet-capture activate
Router(config)#
```

Manually stop the running packet capturing.

```
Router(config)# no packet-capture activate
Router(config)#
```

Check current packet capture status and list all stored packet captures.

```
Router(config)# show packet-capture status
capture status: off
Router(config)# dir /packet_trace
File Name                                          Size     Modified Time
=============================================================================
wan1-Example.cap                                 575160   2009-11-24 09:06:59
Router(config)#
```

You can use FTP to download a capture file. Open and study it using a packet analyzer tool (for example, Ethereal or Wireshark).

36

Watchdog Timer

This chapter provides information about the ISG50's watchdog timers.

36.1 Hardware Watchdog Timer

The hardware watchdog has the system restart if the hardware fails.

The `hardware-watchdog-timer` commands are for support engineers. It is recommended that you not modify the hardware watchdog timer settings.

Table 189 hardware-watchdog-timer Commands

COMMAND	DESCRIPTION
`[no] hardware-watchdog-timer <4..37>`	Sets how long the system's hardware can be unresponsive before resetting. The no command turns the timer off.
`show hardware-watchdog-timer status`	Displays the settings of the hardware watchdog timer.

36.2 Software Watchdog Timer

The software watchdog has the system restart if the core firmware fails.

The `software-watchdog-timer` commands are for support engineers. It is recommended that you not modify the software watchdog timer settings.

Table 190 software-watchdog-timer Commands

COMMAND	DESCRIPTION
`[no] software-watchdog-timer <10..600>`	Sets how long the system's core firmware can be unresponsive before resetting. The no command turns the timer off.
`show software-watchdog-timer status`	Displays the settings of the software watchdog timer.
`show software-watchdog-timer log`	Displays a log of when the software watchdog timer took effect.

36.3 Application Watchdog

The application watchdog has the system restart a process that fails. These are the `app-watchdog` commands.Use the `configure terminal` command to enter the configuration mode to be able to use these commands.

Table 191 app-watchdog Commands

COMMAND	DESCRIPTION
`[no] app-watch-dog activate`	Turns the application watchdog timer on or off.
`[no] app-watch-dog console-print {always|once}`	Display debug messages on the console (every time they occur or once). The no command changes the setting back to the default.
`[no] app-watch-dog interval <5..60>`	Sets how frequently (in seconds) the ISG50 checks the system processes. The no command changes the setting back to the default.
`[no] app-watch-dog retry-count <1..5>`	Set how many times the ISG50 is to re-check a process before considering it failed. The no command changes the setting back to the default.
`[no] app-watch-dog alert`	Has the ISG50 send an alert the user when the system is out of memory or disk space.
`[no] app-watch-dog disk-threshold min <1..100> max <1..100>`	Sets the percentage thresholds for sending a disk usage alert. The ISG50 starts sending alerts when disk usage exceeds the maximum (the second threshold you enter). The ISG50 stops sending alerts when the disk usage drops back below the minimum threshold (the first threshold you enter). The no command changes the setting back to the default.
`[no] app-watch-dog mem-threshold min` *`threshold_min`* `max` *`threshold_max`*	Sets the percentage thresholds for sending a memory usage alert. The ISG50 starts sending alerts when memory usage exceeds the maximum (the second threshold you enter). The ISG50 stops sending alerts when the memory usage drops back below the minimum threshold (the first threshold you enter). The no command changes the setting back to the default.
`show app-watch-dog config`	Displays the application watchdog timer settings.
`show app-watch-dog monitor-list`	Display the list of applications that the application watchdog is monitoring.

36.3.1 Application Watchdog Commands Example

The following example displays the application watchdog configuration and lists the processes that the application watchdog is monitoring.

```
Router(config)# show app-watch-dog config
Application Watch Dog Setting:
  activate: yes
  alert: yes
  console print: always
  retry count: 3
  interval: 300 seconds
  mem threshold: 80% ~ 90%
  cpu threshold: 80% ~ 90%
  disk threshold: 80% ~ 90%
  auto recover: yes
Router(config)# show app-watch-dog monitor-list
#app_name       min_process_count       max_process_count(negative integer
means unlimited)
uamd                    1                               -1
firewalld               1                               -1
policyd                 1                               -1
classify                1                               -1
ospfd                   1                               -1
ripd                    1                               -1
resd                    1                               -1
zyshd_wd                1                               -1
sshipsecpm              1                               -1
zylogd                  1                               -1
syslog-ng               1                               -1
zylogger                1                               -1
ddns_had                1                               -1
tpd                     1                               -1
wdtd                    1                               -1
zebra                   1                               -1
link_updown             1                               -1
fauthd                  1                               -1
signal_wrapper          1                               -1
ggsvca                  1                               -1
asterisk-mg             1                               -1
asterisk-cs             1                               -1
```

List of Commands (Alphabetical)

This section lists the commands and sub-commands in alphabetical order. Commands and subcommandsappear at the same level.

(no) p2p-localnet *ipv4_cidr* 141
[no] aaa authentication default *member1* [*member2*] [*member3*] [*member4*] 295
[no] aaa authentication *profile-name* 294
[no] aaa authentication *profile-name member1* [*member2*] [*member3*] [*member4*] 295
[no] aaa group server ad *group-name* 289
[no] aaa group server ldap *group-name* 291
[no] aaa group server radius *group-name* 292
[no] access-page color-window-background 309
[no] access-page message-text *message* 309
[no] account {pppoe | pptp} *profile_name* 303
[no] account cellular *profile_name* 304
[no] account *profile_name* 68
[no] account *profile_name* 70
[no] activate 120
[no] activate 123
[no] activate 219
[no] activate 221
[no] activate 249
[no] activate 274
[no] activate 347
[no] address *address_object* 123
[no] address-object *object_name* 279
[no] ad-server basedn *basedn* 287
[no] ad-server binddn *binddn* 288
[no] ad-server cn-identifier *uid* 288
[no] ad-server host *ad_server* 288
[no] ad-server password *password* 288
[no] ad-server port *port_no* 288
[no] ad-server search-time-limit *time* 288
[no] ad-server ssl 288
[no] apn *access_point_name* 304
[no] app-watch-dog activate 366
[no] app-watch-dog alert 366
[no] app-watch-dog console-print {always|once} 366
[no] app-watch-dog disk-threshold min <1..100> max <1..100> 366
[no] app-watch-dog interval <5..60> 366
[no] app-watch-dog mem-threshold min *threshold_min* max *threshold_max* 366
[no] app-watch-dog retry-count <1..5> 366
[no] area IP [{stub | nssa}] 95
[no] area IP authentication 95
[no] area IP authentication authentication-key *authkey* 95
[no] area IP authentication message-digest 95
[no] area IP authentication message-digest-key <1..255> md5 *authkey* 95
[no] area IP virtual-link IP 95
[no] area IP virtual-link IP authentication 95
[no] area IP virtual-link IP authentication authentication-key *authkey* 96
[no] area IP virtual-link IP authentication message-digest 96
[no] area IP virtual-link IP authentication message-digest-key <1..255> md5 *authkey* 96
[no] area IP virtual-link IP authentication same-as-area 96
[no] area IP virtual-link IP authentication-key *authkey* 96

[no] associate authority-group *pbx_grp_name* 216
[no] associate lcr *pbx_grp_name* 216
[no] authentication {chap-pap | chap | pap | mschap | mschap-v2} 303
[no] authentication {force | required} 274
[no] authentication {none | pap | chap} 305
[no] authentication mode {md5 | text} 94
[no] authentication string *authkey* 94
[no] auto-destination 86
[no] auto-disable 86
[no] auto-update 250
[no] backmx 103
[no] backup-custom *ip* 102
[no] backup-iface *interface_name* 103
[no] band {auto|wcdma|gsm} 70
[no] bandwidth <1..1048576> priority <1..1024> [maximize-bandwidth-usage] 86
[no] bind *interface_name* 68
[no] black-list 157
[no] black-list extension *phone_num* 157
[no] block 98
[no] block no-caller-id 157
[no] budget active 70
[no] budget data active {download-upload|download|upload} <1..100000> 71
[no] budget time active <1..672> 70
[no] busy-detect <1-10> 147
[no] bwm activate 86
[no] call-forward blind 156
[no] call-forward busy 156
[no] call-forward night-service 156
[no] call-forward noanswer 156
[no] calling-party-num-hide activate 192
[no] call-waiting 156
[no] client-identifier *mac_address* 58
[no] client-name *host_name* 58
[no] clock daylight-saving 310
[no] clock saving-interval begin {apr|aug|dec|feb|jan|jul|jun|mar|may|nov|oct|sep}
{1|2|3|4|last} {fri|mon|sat|sun|thu|tue|wed} *hh:mm* end
{apr|aug|dec|feb|jan|jul|jun|mar|may|nov|oct|sep} {1|2|3|4|last}
{fri|mon|sat|sun|thu|tue|wed} *hh:mm* offset 310
[no] clock time-zone {-|+*hh*} 310
[no] codec *pbx_codec* 157
[no] compression {on | off} 303
[no] connection-id *connection_id* 304
[no] connectivity {nail-up | dial-on-demand} 68
[no] connectivity-check continuous-log activate 340
[no] connectivity-check continuous-log activate 64
[no] connlimit max-per-host <1..8192> 118
[no] console baud *baud_rate* 311
[no] corefile copy usb-storage 76
[no] cptone *country_code* 147
[no] crypto ignore-df-bit 129
[no] crypto map *map_name* 129
[no] crypto *map_name* 132
[no] crypto *profile_name* 98
[no] ctmatch {dnat | snat} 120
[no] custom *ip* 102
[no] deactivate 86
[no] default-router *ip* 59
[no] description *description* 120
[no] description *description* 123

[no] description *description* 271
[no] description *description* 274
[no] description *description* 279
[no] description *description* 283
[no] description *description* 55
[no] description *description* 59
[no] description *description* 86
[no] descrption *description* 177
[no] destination {*address_object* | *group_name*} 274
[no] destination {*address_object*|any} 86
[no] destinationip *address_object* 120
[no] device <*device_model_name*> 72
[no] diag-info copy usb-storage 76
[no] dial-extension active 196
[no] dial-extension active 199
[no] dial-extension active 199
[no] dial-interval <1-10> 147
[no] dnd 157
[no] dnd white-list extension *phone_num* 157
[no] domainname *domain_name* 310
[no] domain-name *domain_name* 59
[no] downstream <0..1048576> 55
[no] dpd 127
[no] dscp {any | <0..63>} 86
[no] dscp class {default | *dscp_class*} 87
[no] duplex <full | half> 66
[no] encryption {nomppe | mppe-40 | mppe-128} 304
[no] exten EXTEN_NUM 231
[no] extension *exten_num* 220
[no] extension *ext_number* 228
[no] extensions 251
[no] fall-back 127
[no] fax-protocol <pass-through|t38> 148
[no] firewall activate 119
[no] first-dns-server {*ip* | *interface_name* {1st-dns | 2nd-dns | 3rd-dns}} 59
[no] first-wins-server *ip* 59
[no] force 274
[no] force-active 149
[no] force-auth activate 273
[no] from *zone_object* 120
[no] groupname *groupname* 271
[no] groupname *groupname* 271
[no] group-pickup 155
[no] ha-iface *interface_name* 103
[no] hardware-address *mac_address* 58
[no] hardware-watchdog-timer <4..37> 365
[no] host *hostname* 102
[no] host *ip* 58
[no] hostname *hostname* 310
[no] idle <0..360> 303
[no] idle <0..360> 305
[no] incoming-cgpn-abbreviated-prefix *number_prefix* 149
[no] incoming-cgpn-international-prefix *number_prefix* 149
[no] incoming-cgpn-national-prefix *number_prefix* 149
[no] incoming-cgpn-networkspecific-prefix *number_prefix* 149
[no] incoming-cgpn-subscriber-prefix *number_prefix* 149
[no] incoming-cgpn-unknown-prefix *number_prefix* 149
[no] in-dnat activate 130
[no] in-snat activate 130

[no] interface {*num*|*interface-name*} 81
[no] interface *interface_name* 54
[no] interface *interface_name* 70
[no] interface *interface_name* 87
[no] interface *interface_name* 98
[no] interface-group *group-name* 80
[no] ip address dhcp 55
[no] ip address *ip subnet_mask* 55
[no] ip ddns profile *profile_name* 102
[no] ip dhcp pool *profile_name* 58
[no] ip dhcp-pool *profile_name* 59
[no] ip dns server a-record *fqdn w.x.y.z* 312
[no] ip dns server mx-record *domain_name* {*w.x.y.z*|*fqdn*} 312
[no] ip dns server zone-forwarder {<1..32>|append|insert <1..32>} {*domain_zone_name*|*} inter-face *interface_name* 313
[no] ip ftp server 320
[no] ip ftp server cert *certificate_name* 320
[no] ip ftp server port <1..65535> 320
[no] ip ftp server tls-required 320
[no] ip gateway *ip* 55
[no] ip helper-address *ip* 59
[no] ip http authentication *auth_method* 315
[no] ip http port <1..65535> 315
[no] ip http secure-port <1..65535> 315
[no] ip http secure-server 315
[no] ip http secure-server auth-client 315
[no] ip http secure-server cert *certificate_name* 315
[no] ip http secure-server force-redirect 316
[no] ip http server 316
[no] ip load-balancing link-sticking activate 83
[no] ip load-balancing link-sticking timeout *timeout* 84
[no] ip ospf authentication-key *password* 62
[no] ip ospf cost <1..65535> 62
[no] ip ospf dead-interval <1..65535> 63
[no] ip ospf hello-interval <1..65535> 63
[no] ip ospf priority <0..255> 62
[no] ip ospf retransmit-interval <1..65535> 63
[no] ip rip {send | receive} version <1..2> 62
[no] ip rip v2-broadcast 62
[no] ip route {*w.x.y.z*} {*w.x.y.z*} {*interface*|*w.x.y.z*} <0..127> 90
[no] ip ssh server 318
[no] ip ssh server cert *certificate_name* 318
[no] ip ssh server port <1..65535> 318
[no] ip ssh server v1 318
[no] ip telnet server 319
[no] ip telnet server port <1..65535> 319
[no] ip-select {iface | auto | custom} 102
[no] ip-select-backup {iface | auto | custom} 102
[no] isakmp policy *policy_name* 127
[no] isdn <*isdn*> {bri|fxs} 149
[no] isup <overlap-receiving | enbloc> 149
[no] item cpu-usage 347
[no] item mem-usage 347
[no] item port-usage 347
[no] item session-usage 347
[no] item traffic-report 348
[no] join *interface_name* 78
[no] ldap 251
[no] ldap-server basedn *basedn* 288

[no] ldap-server binddn *binddn* 288
[no] ldap-server cn-identifier *uid* 288
[no] ldap-server host *ldap_server* 288
[no] ldap-server password *password* 288
[no] ldap-server port *port_no* 288
[no] ldap-server search-time-limit *time* 288
[no] ldap-server ssl 288
[no] lease {<0..365> [<0..23> [<0..59>]] | infinite} 59
[no] limit <0..8192> 123
[no] local 251
[no] local-address <*ip*> 72
[no] local-address *ip* 69
[no] log [alert] 120
[no] logging console 343
[no] logging console category *module_name* 344
[no] logging debug suppression 341
[no] logging debug suppression interval <10..600> 341
[no] logging mail <1..2> 342
[no] logging mail <1..2> {send-log-to | send-alerts-to} *e_mail* 343
[no] logging mail <1..2> address {*ip* | *hostname*} 342
[no] logging mail <1..2> authentication 342
[no] logging mail <1..2> authentication username *username* password *password* 342
[no] logging mail <1..2> category *module_name* level {alert | all} 343
[no] logging mail <1..2> port <1..65535> 343
[no] logging mail <1..2> schedule {full | hourly} 343
[no] logging mail <1..2> subject *subject* 343
[no] logging syslog <1..4> 341
[no] logging syslog <1..4> {disable | level normal | level all} 341
[no] logging syslog <1..4> address {*ip* | *hostname*} 341
[no] logging syslog <1..4> facility {local_1 | local_2 | local_3 | local_4 | local_5 | local_6 | local_7} 341
[no] logging syslog <1..4> format {cef | vrpt} 341
[no] logging system-log suppression 340
[no] logging system-log suppression interval <10..600> 340
[no] logging usb-storage 75
[no] login-page color-background 309
[no] login-page color-window-background 309
[no] login-page message-text % *message* 309
[no] mail-subject append date-time 347
[no] mail-subject append system-name 347
[no] metric <0..15> 55
[no] mss <536..1452> 69
[no] mss <536..1460> 55
[no] mtu <576..1500> 55
[no] mwi 155
[no] mx {*ip* | *domain_name*} 103
[no] nail-up 130
[no] natt 128
[no] negotiation auto 66
[no] netbios-broadcast 130
[no] network *interface* area IP 95
[no] network *interface_name* 61
[no] network *interface_name* 94
[no] network *interface_name* area *ip* 62
[no] network-selection {auto|home} 70
[no] next-hop {auto|gateway *address object* |interface *interface_name* |trunk *trunk_name*|tunnel *tunnel_name*} 87
[no] night-service active 198
[no] ntp 311

[no] ntp server {*fqdn*|*w.x.y.z*} 311
[no] number *emer_num* 220
[no] object-group address *group_name* 279
[no] object-group *group_name* 279
[no] object-group *group_name* 283
[no] object-group service *group_name* 282
[no] office-hour dow {sun|mon|tue|wed|thu|fri|sat} 151
[no] office-hour dow {sun|mon|tue|wed|thu|fri|sat} 156
[no] office-hour dow {sun|mon|tue|wed|thu|fri|sat} time <0..23>: <0..59>-<0..23>:<0..59> 151
[no] office-hour dow {sun|mon|tue|wed|thu|fri|sat} time <0..23>: <0..59>-<0..23>:<0..59> 156
[no] office-hour dow *dow* 254
[no] office-hour dow *dow* time *time* 254
[no] office-hour holiday <01-12>/<01-31> 151
[no] office-hour holiday <01-12>/<01-31> 156
[no] office-hour holiday *date* 254
[no] office-hour user-defined 157
[no] on-demand activate 228
[no] outgoing-cgpn-ton < unknown | national | international | network-specific | subscriber | abbreviated > 149
[no] outgoing-cgpn-ton-prefix *number_prefix* 150
[no] outonly-interface *interface_name* 62
[no] outonly-interface *interface_name* 94
[no] out-snat activate 130
[no] packet-capture activate 359
[no] passive-interface *interface_name* 61
[no] passive-interface *interface_name* 62
[no] passive-interface *interface_name* 94
[no] passive-interface *interface_name* 95
[no] password *password* 303
[no] password *password* 304
[no] pbx attack-prevent {web-login|sip} activate 134
[no] pbx cac activate 176
[no] pbx call-block anonymous-block activate 221
[no] pbx callxfer local-handling activate 221
[no] pbx meetme *meetme_num* 230
[no] pbx moh *moh_name* 220
[no] pbx outbound-bri *obtrunk_name* 190
[no] pbx outbound-fxo *obtrunk_name* 188
[no] pbx paging-group PG_NUM 231
[no] pbx phonebook local <1..200> 248
[no] pbx system-sound language *sound_language* 243
[no] phone *phone_number* 304
[no] pin <*pin code*> 72
[no] ping-check activate 64
[no] policy controll-ipsec-dynamic-rules activate 88
[no] policy override-direct-route activate 88
[no] policy-enforcement 130
[no] port *interface_name* 77
[no] prompt activate 228
[no] radius-server host *radius_server* auth-port *auth_port* 289
[no] radius-server key *secret* 289
[no] radius-server timeout *time* 289
[no] redistribute {static | ospf} 94
[no] redistribute {static | rip} 94
[no] redistribute {static | rip} metric-type <1..2> metric <0..16777214> 94
[no] remote-address <*ip*> 72
[no] remote-address *ip* 69
[no] replay-detection 130
[no] report 345

[no] reset-counter 348
[no] router-id IP 95
[no] rule *cb_bkid* 221
[no] rx-volume *gain_level* 147
[no] rx-volume *gain_level* 150
[no] schedule active PBX_AA_SCHEDULE_OPTION 197
[no] schedule *schedule_name* 274
[no] schedule *schedule_object* 120
[no] schedule *schedule_object* 87
[no] second-dial <0-9> 143
[no] second-dns-server {*ip* | *interface_name* {1st-dns | 2nd-dns | 3rd-dns}} 59
[no] second-wins-server *ip* 59
[no] server alternative-cn-identifier *uid* 290
[no] server alternative-cn-identifier *uid* 291
[no] server basedn *basedn* 290
[no] server basedn *basedn* 291
[no] server binddn *binddn* 290
[no] server binddn *binddn* 291
[no] server cn-identifier *uid* 290
[no] server cn-identifier *uid* 291
[no] server description *description* 290
[no] server description *description* 291
[no] server description *description* 292
[no] server group-attribute <1-255> 292
[no] server group-attribute *group-attribute* 290
[no] server group-attribute *group-attribute* 291
[no] server host *ad_server* 290
[no] server host *ldap_server* 291
[no] server host *radius_server* 292
[no] server *ip* 304
[no] server key *secret* 292
[no] server password *password* 290
[no] server password *password* 291
[no] server port *port_no* 290
[no] server port *port_no* 291
[no] server search-time-limit *time* 290
[no] server search-time-limit *time* 292
[no] server ssl 290
[no] server ssl 292
[no] server timeout *time* 292
[no] service {*service_name*|any} 87
[no] service *service_name* 120
[no] service-name {*ip* | *hostname* | *service_name*} 304
[no] service-object *object_name* 283
[no] service-type {dyndns | dyndns_static | dyndns_custom | dynu-basic | dynu-premium | no-ip | peanut-hull | 3322-dyn | 3322-static} 102
[no] session-limit activate 123
[no] shutdown 55
[no] slot *obtrunk_slot* port *obtrunk_port* 188
[no] slot *obtrunk_slot* port *obtrunk_port* 191
[no] smtp-auth activate 145
[no] smtp-auth activate 347
[no] snat {outgoing-interface|pool {*address_object*}} 87
[no] snmp-server 322
[no] snmp-server community *community_string* {ro|rw} 322
[no] snmp-server contact *description* 322
[no] snmp-server enable {informs|traps} 322
[no] snmp-server host {*w.x.y.z*} [*community_string*] 322
[no] snmp-server location *description* 322

[no] snmp-server port <1..65535> 322
[no] software-watchdog-timer <10..600> 365
[no] source {*address_object* | *group_name*} 275
[no] source {*address_object*|any} 87
[no] sourceip *address_object* 120
[no] sourceport {tcp|udp} {eq <1..65535>|range <1..65535> <1..65535>} 120
[no] speed <100,10> 66
[no] ssl 249
[no] starting-address *ip* pool-size <1..65535> 59
[no] system default-snat 81
[no] tei-number *number_tei* 150
[no] temp-voice-file active 197
[no] third-dns-server {*ip* | *interface_name* {1st-dns | 2nd-dns | 3rd-dns}} 59
[no] to {*zone_object*|Device} 120
[no] trigger <1..8> incoming *service_name* trigger *service_name* 87
[no] trunk *trunk_name* 228
[no] tunnel *tunnel_name* 88
[no] tx-volume *gain_level* 147
[no] tx-volume *gain_level* 150
[no] upstream <0..1048576> 55
[no] usb-storage activate 75
[no] user *user_name* 120
[no] user *user_name* 123
[no] user *username* 271
[no] user *username* 303
[no] user *username* 304
[no] user *user_name* 88
[no] username *username* password *password* 102
[no] users idle-detection 272
[no] users idle-detection timeout <1..60> 272
[no] users lockout-period <1..65535> 272
[no] users retry-count <1..99> 272
[no] users retry-limit 272
[no] users simultaneous-logon {administration | access} enforce 272
[no] users simultaneous-logon {administration | access} limit <1..1024> 272
[no] users update-lease automation 272
[no] version <1..2> 94
[no] vlan-id <1..4094> 77
[no] voice-mail attached-voice-msg 157
[no] voice-mail delete-voice-msg 157
[no] voice-port <*voiceport*> {fxo|fxs} 147
[no] vpn-concentrator *profile_name* 131
[no] wan-iface *interface_name* 103
[no] wildcard 103
[no] xauth type {server *xauth_method* | client name *username* password *password*} 128
[no] zone *profile_name* 98
[offset *lcr_offset*] [length *lcr_length*] 214
[prefix *lcr_prefix*] [postfix *lcr_postfix*] 214
{sip|audio} <0..63> 146
{sip|audio} class {default|af11|af12|af13|af21|af22|af23|af31|af32|af33|af41|af42|af43} . 146
<*channel_id*> 135
aaa authentication rename *profile-name-old profile-name-new* 294
aaa group server ad *group-name* 290
aaa group server ad rename *group-name group-name* 289
aaa group server ldap *group-name* 291
aaa group server ldap rename *group-name group-name* 291
aaa group server radius *group-name* 292
aaa group server radius rename {*group-name-old*} *group-name-new* 292
access-page message-color {*color-rgb* | *color-name* | *color-number*} 309

access-page title *title* 309
access-page window-color {*color-rgb* | *color-name* | *color-number*} 309
action {allow|deny|reject} 120
action-id <0..9> {*skill_num*|exit} 238
activate 127
activate 129
address-object *object_name* {*ip* | *ip_range* | *ip_subnet* | interface-ip | interface-subnet | interface-gateway} {*interface_name*} 278
address-object rename *object_name object_name* 278
ad-server password-encrypted *password* 288
algorithm {wrr|llf|spill-over} 80
_announce *music_name* 235
announce-freq {<0..99999>|default} 234
apply 33
apply /conf/*file_name.conf* [ignore-error] [rollback] 329
area IP virtual-link IP message-digest-key <1..255> md5 *authkey* 96
arp IP *mac_address* 362
associate authority-group all 216
atse 33
authentication {pre-share | rsa-sig} 127
authentication key <1..255> key-string *authkey* 94
authentication-name *obtrunk_username* 182
authentication-password *obtrunk_passwd* 182
auth-name *auth-name* 155
auth-password *auth-password* 155
auto-attendant {aa|acd|ext|fax} *obtrunk_aa_name* 188
auto-attendant {aa|acd|ext|fax} *obtrunk_aa_name* 191
auto-attendant {aa|fax|ext|acd} *obtrunk_aa_name* 185
auto-attendant {aa|fax|ext|acd} *obtrunk_aa_name* 185
autoprov_phone_name autoprov_url 246
basedn STRING_128 249
beep-frequency <0 or 5-60> 228
binddn STRING_128 249
body *body_string* 247
budget {log|log-alert}[recursive <1..65535>] 71
budget {log-percentage|log-percentage-alert} [recursive <1..65535>] 71
budget current-connection {keep|drop} 71
budget new-connection {allow|disallow} 71
budget percentage {ptime|pdata} <0..99> 71
budget reset-counters 71
budget reset-day <0..31> 71
ca enroll cmp name *certificate_name* cn-type {ip cn *cn_address*|fqdn cn *cn_domain_name*|mail cn *cn_email*} [ou *organizational_unit*] [o *organization*] [c *country*] key-type {rsa|dsa} key-len *key_length* num <0..99999999> password *password* ca *ca_name* url *url*; 298
ca enroll scep name *certificate_name* cn-type {ip cn *cn_address*|fqdn cn *cn_domain_name*|mail cn *cn_email*} [ou *organizational_unit*] [o *organization*] [c *country*] key-type {rsa|dsa} ... key-len *key_length* password *password* ca *ca_name* url *url* 298
ca generate pkcs10 name *certificate_name* cn-type {ip cn *cn_address*|fqdn cn *cn_domain_name*|mail cn *cn_email*} [ou *organizational_unit*] [o *organization*] [c *country*] key-type {rsa|dsa} key-len *key_length* 299
ca generate pkcs12 name *name* password *password* 299
ca generate x509 name *certificate_name* cn-type {ip cn *cn_address*|fqdn cn *cn_domain_name*|mail cn *cn_email*} [ou *organizational_unit*] [o *organization*] [c *country*] key-type {rsa|dsa} key-len *key_length* 299
ca rename category {local|remote} *old_name new_name* 299
ca validation *remote_certificate* 299
cac *cac_code* 151
caller-id {ext_ext|ext_rep|rep_rep|ext_rep_ddi|rep_rep_ddi} 182
caller-id {ext_ext|ext_rep|rep_rep|ext_rep_ddi|rep_rep_ddi} 184

caller-id-prefix *obtrunk_callprefix* 182
caller-id-prefix *obtrunk_callprefix* 183
caller-id-prefix-flag {disable|enable} 182
caller-id-prefix-flag {disable|enable} 183
call-forward blind extension *pbx_exten_num* 156
call-forward blind voice-mail 156
call-forward busy extension *pbx_exten_num* 156
call-forward busy voice-mail 156
call-forward follow-me extension *pbx_exten_num* 156
call-forward night-service extension *pbx_exten_num* 156
call-forward night-service voice-mail 156
call-forward noanswer extension move *pbx_exten_num* to *pbx_exten_num* 156
call-forward noanswer extension *pbx_exten_num* 156
call-forward noanswer voice-mail 156
calling-party-num {directory-num | user-define | extension | force-directory-num | force-user-define} 192
calling-party-num-define *obtrunk_cpn_num* 192
calling-party-num-prefix *obtrunk_cpn_prefix* 192
call-recording-on-demand *feature_code* 143
call-transfer *feature_code* 143
cdp {activate|deactivate} 299
certificate *certificate-name* 127
channel *lcr_channel* 214
channel-limit <1..128> 181
channel-limit <1..128> 183
clear 33
clear aaa authentication *profile-name* 294
clear aaa group server ad [*group-name*] 289
clear aaa group server ldap [*group-name*] 291
clear aaa group server radius *group-name* 292
clear ip dhcp binding {*ip* | *} 60
clear logging debug buffer 341
clear logging system-log buffer 340
clear report [*interface_name*] 345
clock date *yyyy-mm-dd* time *hh:mm:ss* 310
clock time *hh:mm:ss* 310
codec default 157
codec move *pbx_codec* to *pbx_codec* 157
codec *obtrunk_codec* 182
codec *obtrunk_codec* 184
configure 33
connectivity {nail-up | dial-on-demand} 72
copy 33
copy {/cert | /conf | /packet_trace | /script | /tmp}*file_name-a.conf* {/cert | /conf | /packet_trace | /script | /tmp}/*file_name-b.conf* 329
copy running-config /conf/*file_name.conf* 329
copy running-config startup-config 329
country PHBOOK_VAL 249
crypto map dial *map_name* 129
crypto map *map_name* 129
crypto map *map_name* 131
crypto map rename *map_name map_name* 129
custom-busytone frequency *busytone_frequency1* [*busytone_frequency2*] cadence *busytone_ontime busytone_offtime* 147
daily-report 347
ddi-flag {disable|enable} 185
ddi-mapping *obtrunk_ddi_match* 184
ddi-mapping *obtrunk_ddi_match* 185
ddi-mapping *obtrunk_ddi_match* 191

ddi-mask <0..20> 191
ddi-match-digit <0..4> 184
ddi-match-digit <0..4> 185
ddi-rewrite-callerid {disable|enable} 185
deactivate 127
deactivate 129
debug (*) 33
debug [cmdexec|corefile|ip |kernel|mac-id-rewrite|observer|switch |system|zyinetpkt|zysh-ipt-op] (*) 35
debug alg 35
debug ca (*) 35
debug force-auth (*) 35
debug gui (*) 35
debug hardware (*) 35
debug interface 35
debug interface ifconfig [interface] 35
debug interface-group 35
debug ip dns 35
debug ip virtual-server 35
debug ipsec 35
debug logging 35
debug manufacture 35
debug myzyxel server (*) 35
debug network arpignore (*) 35
debug no myzyxel server (*) 35
debug pbx call progress start level *pbx_debug_level* 259
debug pbx call progress stop 259
debug pbx call progress with-sip start level *pbx_debug_level* 259
debug pbx call progress with-sip stop 259
debug pbx show calls 259
debug pbx show channels 259
debug pbx show database status 259
debug pbx show sip-setting 259
debug pbx show uptime 259
debug pbx tapi dump {on|off} 35
debug policy-route (*) 35
debug service-register 35
debug show ipset 35
debug show myzyxel server status 35
debug show myzyxel server status 35
debug update server (*) 35
debug voice-sniffer *port* <start | stop> 259
delete 33
delete {/cert | /conf | /packet_trace | /script | /tmp}/*file_name* 329
department department 155
department PHBOOK_VAL 249
description *acd_description* 233
description *acd_description* 234
description *acd_description* 236
description *acd_description* 238
description *description* 155
description *description2* 220
description *description2* 230
description *description2* 231
description *lcr_desc* 214
description *obtrunk_desc* 181
description *obtrunk_desc* 182
description *obtrunk_desc* 188
description *obtrunk_desc* 190

description *pbx_description* 151
description *pbx_description* 195
details 33
device-register checkuser *user_name* 46
device-register username *user_name* password *password* [e-mail *user@domainname*] [country-code *country_code*] [reseller-name *name*] [reseller-mail *email-address*] [reseller-phone *phone-number*] [vat *vat-number*] 46
diag 33
diag-info 33
diag-info collect 353
dial-condition *lcr_dialcond* 214
dial-extension active 196
dir 33
dir {/cert | /conf | /packet_trace | /script | /tmp} 329
direct-forward active 195
direct-forward active 198
directfw-action acd PBX_ACD_NUM 195
directfw-action acd PBX_ACD_NUM 198
directfw-action extension PBX_EXTEN_NUM 195
directfw-action extension PBX_EXTEN_NUM 198
directfw-action hunt PBX_HUNT_NUM 195
directfw-action hunt PBX_HUNT_NUM 198
directfw-action other PBX_OTHER_NUM 196
directfw-action other PBX_OTHER_NUM 198
directfw-action page PBX_PAGE_NUM 195
directfw-action page PBX_PAGE_NUM 198
directory-num *obtrunk_dir_num* 191
direct-pickup *feature_code* 143
disable 34
dnd voice-mail 157
dns-srv {disable|enable} 140
dscp-marking <0..63> 87
dscp-marking class {default | *dscp_class*} 87
dtmf {rfc2833|inband|info} 155
dtmf-mode {info|rfc2833|inband} 181
dtmf-mode {info|rfc2833|inband} 183
duration <0..300> 360
enable 34
encapsulation {tunnel | transport} 129
exit 123
exit 141
exit 143
exit 145
exit 146
exit 148
exit 150
exit 152
exit 153
exit 158
exit 178
exit 182
exit 184
exit 184
exit 185
exit 185
exit 185
exit 188
exit 192
exit 194

exit 195
exit 196
exit 197
exit 197
exit 199
exit 200
exit 214
exit 217
exit 220
exit 220
exit 221
exit 228
exit 228
exit 230
exit 232
exit 234
exit 235
exit 236
exit 237
exit 237
exit 238
exit 245
exit 246
exit 246
exit 247
exit 249
exit 250
exit 251
exit 255
exit 34
exit 348
exit 55
exit 66
exit 80
expire <60..300> 219
ext PHBOOK_NUM 248
exten *ctt_extension* description *description* 177
exten *ctt_extension* dialnum *ctt_dialnumber* server {*ipv4*|*hostname*} 177
external-aa {disable|enable} 141
fakeip-address {*ipv4*|*hostname*} 141
fakeip-status {disable|enable} 141
fall-back-check-interval <60..86400> 127
files-size <1..10000> 360
file-suffix <*profile_name*> 360
firewall append 119
firewall default-rule action {allow | deny | reject} { no log | log [alert] } 119
firewall delete *rule_number* 119
firewall flush 119
firewall insert *rule_number* 119
firewall move *rule_number* to *rule_number* 119
firewall *rule_number* 118
firewall *zone_object* {*zone_object*|Device} append 118
firewall *zone_object* {*zone_object*|Device} delete <1..5000> 119
firewall *zone_object* {*zone_object*|Device} flush 119
firewall *zone_object* {*zone_object*|Device} insert *rule_number* 119
firewall *zone_object* {*zone_object*|Device} move *rule_number* to *rule_number* 119
firewall *zone_object* {*zone_object*|Device} *rule_number* 118
first-name *name* 155
flush 80

followme-off *feature_code* 143
followme-on *feature_code* 143
force-auth [no] exceptional-service *service_name* 273
force-auth default-rule authentication {required | unnecessary} {no log | log [alert]} .. 273
force-auth policy <1..1024> 273
force-auth policy append 273
force-auth policy delete <1..1024> 274
force-auth policy flush 274
force-auth policy insert <1..1024> 273
force-auth policy move <1..1024> to <1..1024> 274
group *pbx_grp_name* 155
group1 128
group2 128
group5 128
group-id *pbx_grp_id* 151
groupname rename *groupname groupname* 271
group-pickup *feature_code* 143
home PHBOOK_NUM 249
host {HOSTNAME|IPv4} 249
host-ip {*ip-address* | *profile_name* | any> 360
host-port <0..65535> 360
htm 34
iface {add | del} {*interface_name* | *virtual_interface_name*} 360
in-dnat <1..10> protocol {all | tcp | udp} original-ip *address_name* <0..65535> <0..65535>
mapped-ip address_name <0..65535> <0..65535> 130
in-dnat append protocol {all | tcp | udp} original-ip *address_name* <0..65535> <0..65535> mapped-
ip *address_name* <0..65535> <0..65535> 130
in-dnat delete <1..10> 130
in-dnat insert <1..10> protocol {all | tcp | udp} original-ip *address_name* <0..65535> <0..65535>
mapped-ip *address_name* <0..65535> <0..65535> 130
in-dnat move <1..10> to <1..10> 130
in-snat source *address_name* destination *address_name* snat *address_name* 130
interface 34
interface {*num*|append|insert *num*} *interface-name* [weight <1..10>|limit <1..2097152>|passive]
80
interface cellular budget-auto-save <5..1440> 72
interface dial *interface_name* 68
interface disconnect *interface_name* 68
interface *interface_name* 59
interface *interface_name* 62
interface *interface_name* 62
interface *interface_name* 64
interface *interface_name* 65
interface *interface_name* 68
interface *interface_name* 77
interface *interface_name* 78
interface reset {*interface_name*|*virtual_interface_name*|all} 55
interface send statistics interval <15..3600> 56
interface-name {*ppp_interface* | *ethernet_interface*} *user_defined_name* 56
interface-rename *old_user_defined_name new_user_defined_name* 56
internal-aa {disable|enable} 141
internal-operator {0|9} extension *exten_num* 143
ip dhcp pool rename *profile_name profile_name* 58
ip dns server -flush 312
ip dns server rule {<1..32>|append|insert <1..32>} access-group {ALL|*address_object*} zone
{ALL|*address_object*} action {accept|deny} 312
ip dns server rule move <1..32> to <1..32> 312
ip dns server zone-forwarder {<1..32>|append|insert <1..32>} {*domain_zone_name*|*} user-defined
w.x.y.z [private | interface {*interface_name* | auto}] 313

ip dns server zone-forwarder move <1..32> to <1..32> 313
ip ftp server rule {*rule_number*|append|insert *rule_number*} access-group {ALL|*address_object*} zone {ALL|*zone_object*} action {accept|deny} 320
ip ftp server rule move *rule_number* to *rule_number* 320
ip gateway *ip* metric <0..15> 55
ip http secure-server cipher-suite {*cipher_algorithm*} [*cipher_algorithm*] [*cipher_algorithm*] [*cipher_algorithm*] 316
ip http secure-server table {admin|user} rule {*rule_number*|append|insert *rule_number*} access-group {ALL|*address_object*} zone {ALL|*zone_object*} action {accept|deny} 316
ip http secure-server table {admin|user} rule move *rule_number* to *rule_number* 316
ip http server table {admin|user} rule {*rule_number*|append|insert *rule_number*} access-group {ALL|*address_object*} zone {ALL|*zone_object*} action {accept|deny} 316
ip http server table {admin|user} rule move *rule_number* to *rule_number* 316
ip http-redirect activate *description* 112
ip http-redirect deactivate *description* 112
ip http-redirect *description* interface *interface_name* redirect-to *w.x.y.z* <1..65535> 112
ip http-redirect *description* interface *interface_name* redirect-to *w.x.y.z* <1..65535> deactivate 112
ip http-redirect flush 112
ip ospf authentication 62
ip ospf authentication message-digest 62
ip ospf authentication same-as-area 62
ip ospf message-digest-key <1..255> md5 *password* 62
ip route replace {*w.x.y.z*} {*w.x.y.z*} {*interface*|*w.x.y.z*} <0..127> with {*w.x.y.z*} {*w.x.y.z*} {*interface*|*w.x.y.z*} <0..127> 90
ip ssh server rule {*rule_number*|append|insert *rule_number*} access-group {ALL|*address_object*} zone {ALL|*zone_object*} action {accept|deny} 318
ip ssh server rule move *rule_number* to *rule_number* 318
ip telnet server rule {*rule_number*|append|insert *rule_number*} access-group {ALL|*address_object*} zone {ALL|*zone_object*} action {accept|deny} 319
ip telnet server rule move *rule_number* to *rule_number* 319
ip virtual-server {activate | deactivate} *profile_name* 107
ip virtual-server delete *profile_name* 107
ip virtual-server flush 107
ip virtual-server *profile_name* interface *interface_name* original-ip {any | *ip* | *address_object*} map-to {*address_object* | *ip*} map-type any [nat-loopback [nat-1-1-map] [deactivate] | nat-1-1-map [deactivate] | deactivate] 106
ip virtual-server *profile_name* interface *interface_name* original-ip {any | IP | *address_object*} map-to {*address_object* | *ip*} map-type original-service *service_object* mapped-service *service_object* [nat-loopback [nat-1-1-map] [deactivate] | nat-1-1-map [deactivate] | deactivate] 107
ip virtual-server *profile_name* interface *interface_name* original-ip {any | IP | *address_object*} map-to {*address_object* | *ip*} map-type port protocol {any | tcp | udp} original-port <1..65535> mapped-port <1..65535> [nat-loopback [nat-1-1-map] [deactivate] | nat-1-1-map [deactivate] | deactivate] 106
ip virtual-server *profile_name* interface *interface_name* original-ip {any | IP | *address_object*} map-to {*address_object* | *ip*} map-type ports protocol {any | tcp | udp} original-port-begin <1..65535> original-port-end <1..65535> mapped-port-begin <1..65535> [nat-loopback [nat-1-1-map] [deactivate] | nat-1-1-map [deactivate] | deactivate] 107
ip virtual-server rename *profile_name profile_name* 107
ipsec-isakmp *policy_name* 129
ip-type {icmp | igmp | igrp | pim | ah | esp | vrrp | udp | tcp | any} 360
isakmp keepalive <2..60> 127
isakmp policy rename *policy_name policy_name* 128
keystring *pre_shared_key* 128
language <English | Simplified_Chinese | Traditional_Chinese> 324
last-name *name* 155
ldap {activate|deactivate} 299
ldap ip {*ip*|*fqdn*} port <1..65535> [id *name* password *password*] [deactivate] 299

lifetime <180..3000000> 128
loadbalancing-index <outbound|inbound|total> 81
local-id type {ip *ip* | fqdn *domain_name* | mail *e_mail* | dn *distinguished_name*} 128
local-ip {ip {*ip* | *domain_name*} | interface *interface_name*} 128
local-ip *ip* 131
local-policy *address_name* 130
log cdr backup forward *cdr_backup_index* 137
log cdr backup now 137
log cdr config aged-action *cdr_aged_act* 137
log cdr config alert *cdr_flag* 137
log cdr config backup-type *cdr_backup_type* 137
log cdr config email *e-mail* 137
log cdr config internal-call *cdr_flag* 137
log cdr database connect_timeout *cdr_conn_timeout* 137
log cdr database dbname *cdr_db_name* 137
log cdr database hostname *fqdn* 137
log cdr database password *cdr_db_password* 137
log cdr database port *port* 137
log cdr database remote *cdr_flag* 137
log cdr database table *cdr_db_table* 137
log cdr database user *cdr_db_user* 137
logging console category *module_name* level {alert | crit | debug | emerg | error | info | notice | warn} 344
logging mail <1..2> schedule daily hour <0..23> minute <0..59> 343
logging mail <1..2> schedule weekly day *day* hour <0..23> minute <0..59> 343
logging mail <1..2> sending_now 342
logging system-log category *module_name* {disable | level normal | level all} 340
logging usb-storage category *category* disable 75
logging usb-storage category *category* level <all|normal> 75
logging usb-storage flushThreshold <1..100> 75
login-page background-color {*color-rgb* | *color-name* | *color-number*} 309
login-page message-color {*color-rgb* | *color-name* | *color-number*} 309
login-page title *title* 309
login-page title-color {*color-rgb* | *color-name* | *color-number*} 309
login-page window-color {*color-rgb* | *color-name* | *color-number*} 309
logo background-color {*color-rgb* | *color-name* | *color-number*} 309
logon-name PHBOOK_LOGON_NAME 249
mac *mac* 65
mail E_MAIL 249
mail-from *e_mail* 145
mail-from *e_mail* 347
mail-subject set *subject* 347
mail-to-1 *e_mail* 347
mail-to-2 *e_mail* 347
mail-to-3 *e_mail* 347
mail-to-4 *e_mail* 347
mail-to-5 *e_mail* 347
max-call-time *lcr_maxcalltime* 214
maxlength {<1..90>|default} 246
max-members *max_conference_seats* 230
max-paging-time PG_TIME 231
max-wait-call {<1..99999>|default} 234
max-wait-call {<1..99999>|default} 237
member *skill_member* priority <1..5> 235
member *skill_member* priority <1..5>; 237
menu *menuname* 236
mobile PHBOOK_NUM 249
mobile-extension dial-rule *dial_rule* 158
mobile-extension extension *pbx_exten_num* 157

mobile-extension option {manually|force-enable} 157
mobile-extension status [0|1] 157
mobile-extension-auto *feature_code* 143
mobile-extension-off *feature_code* 143
mobile-extension-on *feature_code* 143
mode {main | aggressive} 127
mode {normal|trunk} 81
move <1..8> to <1..8> 81
move channel *lcr_channel* to *lcr_channel* 214
move dial-condition *lcr_dialcond* to *lcr_dialcond* 214
move pbx lcr LCR_NAME to *lcr_name* 214
mtu <576..1492> 69
mtu <576..1492> 72
name *agent_name* 233
name PHBOOK_NAME 248
name *skill_name* 234
name *skill_name* 236
network *ip mask* 59
network IP/<1..32> 59
no action-id {<0..9>|all} 238
no address-object *object_name* 278
no announce 235
no announce-freq 234
no area IP virtual-link IP message-digest-key <1..255> 96
no arp *ip* 362
no associate lcr all 217
no authentication key 94
no auto-attendant 188
no auto-attendant 191
no basedn 249
no binddn 250
no black-list extension all 157
no budget log [recursive] 71
no budget log-percentage [recursive] 72
no ca category {local|remote} *certificate_name* 300
no ca validation *name* 300
no cac 151
no call-forward blind extension 156
no call-forward busy extension 156
no call-forward night-service extension 156
no call-forward noanswer extension all 156
no call-forward noanswer extension *pbx_exten_num* 156
no calling-party-num-define 192
no calling-party-num-prefix 192
no channel { all|*lcr_channel* } 214
no country 249
no custom-busytone 147
no ddi-mapping {*obtrunk_ddi_match*|all} 184
no ddi-mapping {*obtrunk_ddi_match*|all} 185
no ddi-mapping {*obtrunk_ddi_match*|all} 191
no department 249
no description 151
no description 155
no description 188
no description 190
no description 195
no description 214
no description 220
no description 230

no description 231
no description 233
no description 234
no description 236
no description 238
no dial-condition { all|*lcr_dialcond* } 214
no dial-extension active 196
no direct-forward active 195
no direct-forward active 198
no directfw-action acd 195
no directfw-action acd 198
no directfw-action extension 195
no directfw-action extension 198
no directfw-action hunt 195
no directfw-action hunt 198
no directfw-action page 195
no directfw-action page 198
no directory-num 191
no dnd white-list extension all 157
no dscp-marking 87
no ext 249
no exten *ctt_extension* 177
no exten *ctt_extension* description 178
no first-name 155
no home 249
no host 249
no internal-operator 143
no ip dns server rule <1..32> 313
no ip ftp server rule *rule_number* 320
no ip http secure-server cipher-suite {*cipher_algorithm*} 316
no ip http secure-server table {admin|user} rule *rule_number* 316
no ip http server table {admin|user} rule *rule_number* 316
no ip http-redirect *description* 112
no ip ospf authentication 62
no ip ospf message-digest-key 63
no ip ssh server rule *rule_number* 318
no ip telnet server rule *rule_number* 319
no ip virtual-server *profile_name* 106
no last-name 155
no log cdr backup *cdr_backup_index* 138
no log cdr config aged-action 138
no log cdr config alert 138
no log cdr config all 138
no log cdr config backup-type 138
no log cdr config email 138
no log cdr config internal-call 138
no log cdr database remote 138
no logon-name 249
no mac 65
no mail 249
no mail-from 145
no mail-subject set 347
no max-call-time 214
no max-members 230
no max-paging-time 231
no member {*skill_member*|all} 235
no member {*skill_member*|all}; 237
no menu 236
no mobile 249

no mobile-extension dial-rule 158
no mobile-extension extension 158
no name 248
no network 59
no office-hour dow {sun|mon|tue|wed|thu|fri|sat} time all 151
no office-hour dow {sun|mon|tue|wed|thu|fri|sat} time all 156
no office-hour dow *dow* time all 254
no office-hour holiday <01-12>/<01-31> description 151
no office-hour holiday <01-12>/<01-31> description 157
no office-hour holiday all 151
no office-hour holiday all 156
no office-hour holiday all 254
no office-hour holiday *date* description 254
no operator 194
no operator 195
no operator 198
no option 191
no option PBX_AA_OPTION 196
no option PBX_AA_OPTION 197
no option PBX_AA_OPTION 199
no option PBX_AA_OPTION 200
no option PBX_AA_OPTION description 196
no option PBX_AA_OPTION description 196
no option PBX_AA_OPTION description 199
no option PBX_AA_OPTION description 199
no outbound-line bri <1..4> 220
no outbound-line fxo <1..4> 220
no outbound-line sip-trunk *emer_outboundline* 220
no packet-trace 34
no param all 214
no param dial-condition *lcr_dialcond* channel *lcr_channel* 214
no password 249
no pbx acd agent {all | *agent_id*} 233
no pbx acd hunt {all | *skill_num*} 236
no pbx acd skill {all | *skill_num*} 234
no pbx acd skill-menu {all | *menuname*} 237
no pbx authority-group *pbx_grp_name* 151
no pbx authority-tapi 153
no pbx authority-tapi server1 username *tapi_user_name* 153
no pbx authority-tapi server2 username *tapi_user_name* 153
no pbx auto-attendant PBX_GRP_NAME 195
no pbx auto-provision *autoprov_extension* {system|customize} 245
no pbx auto-provision firmware *autoprov_phone_name* 246
no pbx clicktotalk-group *ctt_grp_name* 177
no pbx extension *pbx_exten_num* 155
no pbx lcr {all| *lcr_name*} 214
no pbx monit-status channel 135
no pbx outbound-fxo all 188
no pbx outbound-sip-trunk *obtrunk_name* 184
no pbx outbound-sip-trunk *obtrunk_name* proxy-require 184
no pbx outbound-trust-peer *obtrunk_name* 184
no pbx outbound-trust-peer *obtrunk_name* proxy-require 184
no pbx phonebook ldap attr country 250
no pbx phonebook ldap attr department 250
no pbx phonebook ldap attr ext 250
no pbx phonebook ldap attr home 250
no pbx phonebook ldap attr logon-name 250
no pbx phonebook ldap attr mail 250
no pbx phonebook ldap attr mobile 250

no pbx phonebook ldap attr name 250
no pbx record-exten 243
no periodic 235
no periodic-freq 234
no pincode 230
no pincode 231
no play-audio-file active 196
no play-audio-file active 199
no port 249
no port <1..*x*> 66
no rule all 221
no sa spi *spi* 132
no sa tunnel-name *map_name* 132
no schedule {time1|time2|time3|time4|time5|time6} 197
no schedule-object *object_name* 285
no search-time-limit 250
no service-object *object_name* 281
no slot all 188
no smtp-address 145
no smtp-address 347
no smtp-auth username 145
no smtp-auth username 347
no snmp-server rule *rule_number* 322
no tapi-line *exten_num* 153
no update-time 250
no use-defined-mac 66
no username *username* 270
no voice-mail address 157
no-available-action {[join]|[hangup]|[backup *skill_name*]|[page *ext_num*]|[hunt *ext_num*]|[aa *aa_name*]|[extension *ext_num*]|[voicemail *ext_num*]} 236
no-login-action {[hangup]|[backup *skill_name*]|[page *ext_num*]|[hunt *ext_num*]|[aa *aa_name*]|[extension *ext_num*]|[voicemail *ext_num*]} 235
nslookup 34
ntp sync 311
object-group address rename *group_name group_name* 279
object-group service rename *group_name group_name* 283
ocsp {activate|deactivate} 299
ocsp url *url* [id *name* password *password*] [deactivate] 300
office-hour apply {default|from-system|to-extension} 152
office-hour apply {default|to-authority|to-extension} 254
office-hour holiday <01-12>/<01-31> description *pbx_description* 151
office-hour holiday <01-12>/<01-31> description *pbx_description* 156
office-hour holiday *date* description *pbx_description* 254
operator PBX_OPERATOR_KEY extension PBX_EXTEN_NUM 194
operator PBX_OPERATOR_KEY extension PBX_EXTEN_NUM 195
operator PBX_OPERATOR_KEY extension PBX_EXTEN_NUM 198
option { ddi | aa | direct | msn } 191
option PBX_AA_OPTION action {forward-to-operator|repeat|sub-menu} 196
option PBX_AA_OPTION action {forward-to-operator|repeat|sub-menu} 199
option PBX_AA_OPTION action forward-to-aa PBX_GRP_NAME 196
option PBX_AA_OPTION action forward-to-aa PBX_GRP_NAME 197
option PBX_AA_OPTION action forward-to-aa PBX_GRP_NAME 199
option PBX_AA_OPTION action forward-to-aa PBX_GRP_NAME 200
option PBX_AA_OPTION action forward-to-acd PBX_EXTEN_NUM 196
option PBX_AA_OPTION action forward-to-acd PBX_EXTEN_NUM 197
option PBX_AA_OPTION action forward-to-acd PBX_EXTEN_NUM 199
option PBX_AA_OPTION action forward-to-acd PBX_EXTEN_NUM 200
option PBX_AA_OPTION action forward-to-extension PBX_EXTEN_NUM 196
option PBX_AA_OPTION action forward-to-extension PBX_EXTEN_NUM 196

option PBX_AA_OPTION action forward-to-extension PBX_EXTEN_NUM 199
option PBX_AA_OPTION action forward-to-extension PBX_EXTEN_NUM 199
option PBX_AA_OPTION action forward-to-hunt PBX_HUNT_NUM 196
option PBX_AA_OPTION action forward-to-hunt PBX_HUNT_NUM 197
option PBX_AA_OPTION action forward-to-hunt PBX_HUNT_NUM 199
option PBX_AA_OPTION action forward-to-hunt PBX_HUNT_NUM 200
option PBX_AA_OPTION action forward-to-operator 197
option PBX_AA_OPTION action forward-to-operator 200
option PBX_AA_OPTION action forward-to-other PBX_OTHER_NUM 196
option PBX_AA_OPTION action forward-to-other PBX_OTHER_NUM 197
option PBX_AA_OPTION action forward-to-other PBX_OTHER_NUM 199
option PBX_AA_OPTION action forward-to-other PBX_OTHER_NUM 200
option PBX_AA_OPTION action forward-to-page PBX_PAGE_NUM 196
option PBX_AA_OPTION action forward-to-page PBX_PAGE_NUM 197
option PBX_AA_OPTION action forward-to-page PBX_PAGE_NUM 199
option PBX_AA_OPTION action forward-to-page PBX_PAGE_NUM 200
option PBX_AA_OPTION action repeat 197
option PBX_AA_OPTION action repeat 200
option PBX_AA_OPTION action return-previous-menu 197
option PBX_AA_OPTION action return-previous-menu 200
option PBX_AA_OPTION action sub-menu 197
option PBX_AA_OPTION action sub-menu 199
option PBX_AA_OPTION description PBX_DESCRIPTION 196
option PBX_AA_OPTION description PBX_DESCRIPTION 196
option PBX_AA_OPTION description PBX_DESCRIPTION 199
option PBX_AA_OPTION description PBX_DESCRIPTION 199
outbound-line bri <1..4> prefix {none|*emer_prefix*} 220
outbound-line fxo <1..4> prefix {none|*emer_prefix*} 220
outbound-line sip-trunk *emer_outboundline* prefix {none|*emer_prefix*} 220
outbound-proxy {*ipv4*|*hostname*} 181
outbound-proxy {*ipv4*|*hostname*} 183
outbound-proxy-flag {disable|enable} 181
outbound-proxy-flag {disable|enable} 183
outbound-proxy-port <1..65535> 181
outbound-proxy-port <1..65535> 183
out-snat source *address_name* destination *address_name* snat *address_name* 130
p2p-status {disable|enable} 141
packet-capture configure 359
packet-trace 34
packet-trace [interface *interface_name*] [ip-proto {<0..255> | *protocol_name* | any}] [src-host {*ip* | *hostname* | any}] [dst-host {*ip* | *hostname* | any}] [port {<1..65535> | any}] [file] [duration <1..3600>] [extension-filter *filter_extension*] 359
param dial-condition *lcr_dialcond* channel *lcr_channel* 214
password *agent_pwd* 234
password PASSWORD 249
pbx acd agent [*agent_id*] 233
pbx acd hunt [*skill_num*] 236
pbx acd hunt [*skill_num*] advanced 237
pbx acd skill [*skill_num*] 234
pbx acd skill [*skill_num*] advanced 235
pbx acd skill-menu [*menuname*] 238
pbx acd wrap-up-time {*wrapup_time*|default} 233
pbx attack-prevent {web-login|sip} block-time <1..1440> 134
pbx attack-prevent {web-login|sip} fail-access <1..10> 134
pbx attack-prevent {web-login|sip} unlock {all|*pbx_exten_num*} 134
pbx authority-group *pbx_grp_name* 151
pbx authority-tapi 153
pbx authority-tapi {client|server} 153
pbx authority-tapi server1 username *tapi_user_name* password *tapi_password* 153

pbx authority-tapi server2 username *tapi_user_name* password *tapi_password* 154
pbx auto-attendant default 194
pbx auto-attendant greeting PBX_GRP_NAME 197
pbx auto-attendant night-service PBX_GRP_NAME 198
pbx auto-attendant night-service PBX_GRP_NAME path PBX_AA_PATH 199
pbx auto-attendant office-hour PBX_GRP_NAME 195
pbx auto-attendant office-hour PBX_GRP_NAME path PBX_AA_PATH 196
pbx auto-attendant PBX_GRP_NAME 195
pbx autocallback 219
pbx auto-provision *autoprov_extension* 245
pbx auto-provision autoprov-status {enable|disable} 246
pbx auto-provision feature-key 245
pbx auto-provision feature-key *autoprov_fkey_index autoprov_feature_type* {on|off} 246
pbx auto-provision firmware 246
pbx call-block black-list 221
pbx callpark 219
pbx callrecord full-time 228
pbx callrecord global 228
pbx callwait 220
pbx callxfer digit-timeout <1..99> 221
pbx clicktotalk-group *ctt_grp_name* 177
pbx dscp 146
pbx emergency-call 220
pbx extension *pbx_exten_num* 155
pbx feature-code 143
pbx global 140
pbx group-management *pbx_grp_name* 216
pbx lcr % *lcr_name* 214
pbx mail 145
pbx moh set-default { built-in | *moh_name* } 220
pbx outbound-sip-trunk *obtrunk_name* 181
pbx outbound-sip-trunk *obtrunk_name* 184
pbx outbound-sip-trunk *obtrunk_name* 185
pbx outboundtrust-peer *obtrunk_name* 182
pbx outbound-trust-peer *obtrunk_name* 184
pbx outbound-trust-peer *obtrunk_name* 185
pbx phonebook ldap attr country PHBOOK_VAL 250
pbx phonebook ldap attr department PHBOOK_VAL 250
pbx phonebook ldap attr ext PHBOOK_VAL 250
pbx phonebook ldap attr home PHBOOK_VAL 250
pbx phonebook ldap attr logon-name PHBOOK_VAL 250
pbx phonebook ldap attr mail PHBOOK_VAL 250
pbx phonebook ldap attr mobile PHBOOK_VAL 250
pbx phonebook ldap attr name PHBOOK_VAL 250
pbx phonebook ldap server 249
pbx phonebook ldap update 250
pbx phonebook selection 251
pbx record-exten *pbx_exten_num* 243
pbx system 254
pbx system-sound default *sound_language* 243
pbx voicemail 246
peer-id type {any | ip *ip* | fqdn *domain_name* | mail *e_mail* | dn *distinguished_name*} 128
peer-ip {*ip* | *domain_name*} [*ip* | *domain_name*] 128
peer-ip *ip* 131
_periodic *music_name* 235
periodic-freq {<0..99999>|default} 234
phone-mac *autoprov_mac* 245
phone-name *autoprov_phone_name* 245
pincode *meetme_pincode* 230

pin-code *pbx_exten_num* 155
pincode PG_PINCODE 231
ping 34
ping-check {*domain_name* | *ip* | default-gateway} 64
ping-check {*domain_name* | *ip* | default-gateway} fail-tolerance <1..10> 64
ping-check {*domain_name* | *ip* | default-gateway} method {icmp | tcp} 64
ping-check {*domain_name* | *ip* | default-gateway} period <5..30> 64
ping-check {*domain_name* | *ip* | default-gateway} port <1..65535> 64
ping-check {*domain_name* | *ip* | default-gateway} timeout <1..10> 64
play-audio-file active 196
play-audio-file active 198
policy {*policy_number* | append | insert *policy_number*} 86
policy default-route 88
policy delete *policy_number* 88
policy flush 88
policy list table 88
policy move *policy_number* to *policy_number* 88
port <1..65535> 140
port <1..65535> 249
port status Port<1..*x*> 66
port-grouping *representative_interface* port <1..*x*> 66
privacy {disable|enable} 181
privacy {disable|enable} 183
proxy-require {*ipv4*|*hostname*} 181
proxy-require {*ipv4*|*hostname*} 183
psm 34
queue-size <1..5> 219
quota {<1..600>|default} 247
quota *callrecord_quota* 228
realm *sipconf_realmname* 140
reboot 34
redistribute {static | ospf} metric <0..16> 94
register-server-address {*ipv4*|*hostname*} 181
register-server-port <1..65535> 181
register-timeout <2..32> 140
register-timer-nat <60..86400> 140
register-timer-nat-tcp <60..86400> 140
register-timer-nonat <60..86400> 140
release 34
release dhcp *interface-name* 60
remote-policy *address_name* 130
rename 34
rename {/cert | /conf | /packet_trace | /script | /tmp}/*old-file_name* {/cert | /conf | /packet_trace | /script | /tmp}/*new-file_name* 330
rename /script/*old-file_name* /script/*new-file_name* 330
renew 34
renew dhcp *interface-name* 60
rep-extension <100-99999999> slot-number <1-99> 219
representative-number *obtrunk_rep_num* 181
representative-number *obtrunk_rep_num* 182
reset-counter-now 348
ring-buffer <enable|disable> 360
ring-member-timeout {<1..99999>|default} 234
ring-member-timeout {<1..99999>|default} 237
ring-timer <1..300> 141
router ospf 62
router ospf 94
router ospf 95
router ospf 95

router rip 61
router rip 94
rtcp-status {disable|enable} 140
rtp-port-end <1..65535> 140
rtp-port-start <1..65535> 140
run 34
run /script/*file_name.zysh* 330
scenario {site-to-site-static|site-to-site-dynamic|remote-access-server|remote-access-client} 129
schedule {time1|time2|time3|time4|time5|time6} OH_TIME 197
schedule hour <0..23> minute <00..59> 348
schedule-object *object_name date time date time* 286
schedule-object *object_name time time* [*day*] [*day*] [*day*] [*day*] [*day*] [*day*] [*day*] 286
search-time-limit <1..300> 250
send-now 348
service-domain {*ipv4*|*hostname*} 181
service-domain {*ipv4*|*hostname*} 183
service-domain-flag {disable|enable} 181
service-domain-flag {disable|enable} 183
service-object *object_name* {tcp | udp} {eq <1..65535> | range <1..65535> <1..65535>} 281
service-object *object_name* icmp *icmp_value* 282
service-object *object_name* protocol <1..255> 282
service-object rename *object_name object_name* 282
service-register checkexpire 46
service-register service-type standard license-key *key_value* 46
service-register service-type trial service {call-recording|smartphone} 46
session timeout {udp-connect <1..300> | udp-deliver <1..300> | icmp <1..300>} 351
session timeout session {tcp-established | tcp-synrecv | tcp-close | tcp-finwait | tcp-synsent | tcp-closewait | tcp-lastack | tcp-timewait} <1..300> 351
session-limit append 123
session-limit delete *rule_number* 123
session-limit flush 123
session-limit insert *rule_number* 123
session-limit limit <0..8192> 123
session-limit move *rule_number* to *rule_number* 123
session-limit *rule_number* 123
session-timer-expires <60..86400> 140
session-timer-expires <90..86400> 181
session-timer-expires <90..86400> 183
session-timer-minse <90..1800> 140
session-timer-minse <90..1800> 181
session-timer-minse <90..1800> 183
session-timer-mode {originate|refuse} 140
session-timer-mode *obtrunk_st_mode* 181
session-timer-mode *obtrunk_st_mode* 183
set pfs {group1 | group2 | group5 | none} 130
set security-association lifetime seconds <180..3000000> 130
set session-key {ah <256..4095> *auth_key* | esp <256..4095> [cipher *enc_key*] authenticator *auth_key*} 131
setenv 34
setenv-startup stop-on-error off 330
show 188
show 192
show 197
show 214
show 217
show 220
show 221
show 234

show 235
show 238
show 247
show 271
show 275
show 34
show 58
show aaa authentication {*group-name*|default} 294
show aaa group server ad *group-name* 289
show aaa group server ldap *group-name* 291
show aaa group server radius *group-name* 292
show access-page settings 309
show account [pppoe *profile_name* | pptp *profile_name*] 303
show account cellular *profile_name* 304
show address-object [*object_name*] 278
show ad-server 287
show all-outbound-line 220
show app-watch-dog config 366
show app-watch-dog monitor-list 366
show arp-table 362
show available-exten 231
show black-list 157
show boot status 41
show bridge available member 78
show bwm activation 88
show bwm-usage < [policy-route *policy_number*] | [interface *interface_name*] 88
show ca category {local|remote} [name *certificate_name* format {text|pem}] 300
show ca category {local|remote} name *certificate_name* certpath 300
show ca spaceusage 300
show ca validation name *name* 300
show clock date 311
show clock status 311
show clock time 311
show codec 157
show comport status 41
show conn [user {*username*|any|unknown}] [service {*service-name*|any|unknown}] [source {*ip*|any}] [destination {*ip*|any}] [begin <1..128000>] [end <1..128000>] 346
show conn ip-traffic destination 346
show conn ip-traffic source 346
show conn status 346
show connectivity-check continuous-log status 340
show connectivity-check continuous-log status 64
show connlimit max-per-host 119
show console 311
show corefile copy usb-storage 76
show cpu status 41
show crypto map [*map_name*] 129
show daily-report status 347
show ddns [*profile_name*] 102
show device-register status 46
show diag-info 353
show diag-info copy usb-storage 76
show disk 41
show dnd 157
show extension-slot 41
show fan-speed 41
show firewall 119
show firewall *rule_number* 119
show firewall status 119

show firewall *zone_object* {*zone_object*|Device} 119
show firewall *zone_object* {*zone_object*|Device} *rule_number* 119
show force-auth activation 274
show force-auth exceptional-service 274
show force-auth policy {<1..1024> | all} 274
show fqdn 310
show groupname [*groupname*] 271
show hardware-watchdog-timer status 365
show interface {ethernet | vlan | bridge | ppp} status 54
show interface {*interface_name* | ethernet | vlan | bridge | ppp | virtual ethernet | virtual vlan | virtual bridge | all} 54
show interface cellular [corresponding-slot|device-status|support-device] 72
show interface cellular budget-auto-save 72
show interface cellular corresponding-slot 72
show interface cellular device-status 72
show interface cellular status 72
show interface cellular support-device 72
show interface *interface_name* [budget] 72
show interface *interface_name* device profile 72
show interface *interface_name* device status 72
show interface ppp system-default 69
show interface ppp user-define 69
show interface send statistics interval 54
show interface summary all 54
show interface summary all status 54
show interface-group {system-default|user-define|*group-name*} 80
show interface-name 56
show ip dhcp binding [*ip*] 60
show ip dhcp pool [*profile_name*] 58
show ip dns server 313
show ip dns server database 313
show ip dns server status 313
show ip ftp server status 320
show ip http server secure status 316
show ip http server status 316
show ip http-redirect [*description*] 112
show ip load-balancing link-sticking status 84
show ip pbx server status 259
show ip route [kernel | connected | static | ospf | rip | bgp] 96
show ip route static-dynamic 355
show ip route-settings 90
show ip ssh server status 318
show ip telnet server status 319
show ip virtual-server [*profile_name*] 106
show isakmp keepalive 127
show isakmp policy [*policy_name*] 127
show isakmp sa 132
show isdn <*isdn* | all> 150
show language {setting | all} 324
show ldap-server 288
show led status 41
show lockout-users 275
show log cdr backup 137
show log cdr config 137
show log cdr database 137
show log cdr database usage 137
show log cdr report offset *cdr_row_offset* limit *cdr_row_limit* order *cdr_db_field* in *cdr_db_order* condition *cdr_query_condition* 137
show logging debug entries [priority *pri]* [category *module_name*] [srcip *ip*] [dstip *ip*] [service

service_name] [begin <1..512> end <1..512>] [keyword *keyword*] 341
show logging debug entries field *field* [begin <1..1024> end <1..1024>] 341
show logging debug status 341
show logging entries [priority *pri*] [category *module_name*] [srcip *ip*] [dstip *ip*] [service *service_name]* [begin <1..512> end <1..512>] [keyword *keyword*] 339
show logging entries field *field* [begin <1..512> end <1..512>] 339
show logging status console 343
show logging status mail 342
show logging status syslog 341
show logging status system-log 340
show logging status usb-storage 75
show login-page default-title 309
show login-page settings 309
show logo settings 309
show mac 41
show mem status 41
show mobile-extension 158
show ntp server 311
show object-group address [*group_name*] 279
show object-group service *group_name* 282
show office-hour 157
show office-hour [dow|dow-time|holiday] 254
show ospf area IP virtual-link 95
show packet-capture config 360
show packet-capture status 360
show page-customization 309
show pbx acd hunt {all | *skill_num*} 237
show pbx acd hunt *skill_num* member 237
show pbx acd realtime agent status 236
show pbx acd realtime waiting calls 236
show pbx acd skill {all | *skill_num*} 235
show pbx acd skill *skill_num* member 235
show pbx acd skill-menu {all | *menuname*} 238
show pbx acd skill-menu *menuname* code 238
show pbx acd wrap-up-time 233
show pbx attack-prevent {web-login|sip} 134
show pbx attack-prevent {web-login|sip} lock-list 134
show pbx authority-group *pbx_grp_name* office-hour [|dow|dow-time|holiday] 152
show pbx authority-group *pbx_grp_name* 152
show pbx authority-group 152
show pbx authority-group-extension *pbx_grp_name* 152
show pbx authority-group-extension 152
show pbx authority-group-list 152
show pbx authority-tapi {server|client} tapi-line 154
show pbx authority-tapi status 154
show pbx auto-attendant file space usage 200
show pbx auto-attendant greeting PBX_GRP_NAME 200
show pbx auto-attendant night-service PBX_GRP_NAME 200
show pbx auto-attendant night-service PBX_GRP_NAME option 200
show pbx auto-attendant night-service PBX_GRP_NAME path PBX_AA_PATH_SHOW 200
show pbx auto-attendant office-hour PBX_GRP_NAME 200
show pbx auto-attendant office-hour PBX_GRP_NAME option 200
show pbx auto-attendant office-hour PBX_GRP_NAME path PBX_AA_PATH_SHOW 200
show pbx autocallback 219
show pbx auto-provision *autoprov_extension* 245
show pbx auto-provision config 245
show pbx auto-provision extension-list 245
show pbx auto-provision feature-key 245
show pbx auto-provision firmware 245

show pbx cac 176
show pbx call-block 221
show pbx call-block black-list 221
show pbx callpark 219
show pbx callrecord full-time 228
show pbx callrecord global 228
show pbx callwait 219
show pbx callxfer digit-timeout 220
show pbx callxfer local-handling 221
show pbx clicktotalk-group [*ctt_grp_name*] 178
show pbx clicktotalk-group *ctt_grp_name* exten 178
show pbx clicktotalk-group *ctt_grp_name* exten *ctt_extension* samplecode 178
show pbx dscp 146
show pbx emergency-call number 220
show pbx emergency-call outbound-line 220
show pbx extension available-fxs 158
show pbx extension *pbx_exten_num* 158
show pbx extension *pbx_exten_num* basic 158
show pbx extension *pbx_exten_num* black-list 158
show pbx extension *pbx_exten_num* call-forward noanswer 158
show pbx extension *pbx_exten_num* codec 158
show pbx extension *pbx_exten_num* dnd 158
show pbx extension *pbx_exten_num* office-hour dow 158
show pbx extension *pbx_exten_num* office-hour holiday 158
show pbx feature-code all 143
show pbx group-management 217
show pbx group-management *pbx_grp_name* 217
show pbx lcr {all|*lcr_name*} 214
show pbx mail 145
show pbx meetme 230
show pbx moh default 220
show pbx moh list 220
show pbx moh usage 220
show pbx monit-status {all|fakeip-info|p2p-info|p2p-localnet} 140
show pbx monit-status {bri-trunk|cti-peer|fxo-trunk|fxs-peer|sip-peer|sip-trunk} all 135
show pbx outbound-bri {all | *obtrunk_name*} 190
show pbx outbound-bri {ddi | line} *obtrunk_name* 190
show pbx outbound-fxo {all | *obtrunk_name*} 188
show pbx outbound-sip-trunk aa-info *obtrunk_name* 180
show pbx outbound-sip-trunk ddi-info *obtrunk_name* 180
show pbx outbound-sip-trunk ddi-matchpart *obtrunk_name* 180
show pbx outbound-sip-trunk *obtrunk_name* 180
show pbx outbound-sip-trunk sip-trunk-list 180
show pbx outbound-sip-trunk sip-trunk-usedip 180
show pbx outbound-trust-peer ddi-info *obtrunk_name* 180
show pbx outbound-trust-peer ddi-matchpart *obtrunk_name* 180
show pbx outbound-trust-peer *obtrunk_name* 180
show pbx outbound-trust-peer *obtrunk_name* 180
show pbx outbound-trust-peer trust-peer-list 180
show pbx outbound-trust-peer trust-peer-usedip 180
show pbx paging-group 232
show pbx paging-group PG_NUM exten 232
show pbx phonebook ldap attr 251
show pbx phonebook ldap last-update 251
show pbx phonebook ldap server 251
show pbx phonebook local 249
show pbx phonebook selection 251
show pbx record-exten 243
show pbx system office-hour [dow|dow-time|holiday] 255

show pbx system-sound all 243
show pbx system-sound default 243
show ping-check [*interface_name* | status] 64
show ping-check [*interface_name*] 64
show policy-route [*policy_number*] 88
show policy-route begin <1..200> end <1..200> 88
show policy-route controll-ipsec-dynamic-rules 88
show policy-route override-direct-route 88
show policy-route rule_count 88
show policy-route underlayer-rules 88
show port setting 67
show port status 67
show port vlanid 77
show port-grouping 66
show radius-server 289
show ram-size 41
show reference object aaa authentication [default | *auth_method*] 39
show reference object account pppoe [*profile*] 39
show reference object account pptp [*profile*] 39
show reference object address [*profile*] 39
show reference object ca category {local|remote} [*cert_name*] 39
show reference object crypto map [*crypto_name*] 39
show reference object interface [*interface_name* | *virtual_interface_name*] 39
show reference object isakmp policy [*isakmp_name*] 39
show reference object schedule [*profile*] 39
show reference object service [*profile*] 39
show reference object username [*username*] 39
show reference object zone [*profile*] 39
show reference object-group aaa ad [*group_name*] 40
show reference object-group aaa ldap [*group_name*] 40
show reference object-group aaa radius [*group_name*] 40
show reference object-group address [*profile*] 39
show reference object-group interface [*profile*] 40
show reference object-group service [*profile*] 40
show reference object-group username [*username*] 39
show report [*interface_name* {ip | service | url}] 345
show report status 345
show rip {global | interface {all | *interface_name*}} 62
show route order 355
show running-config 330
show sa monitor [{begin <1..1000>} | {end <1..1000>} | {crypto-map *regexp*} | {policy *regexp*} |{rsort *sort_order*} | {sort *sort_order*}] 132
show schedule-object 285
show serial-number 41
show service-object [*object_name*] 281
show service-register server-type 46
show service-register status all 46
show session timeout {icmp | tcp-timewait | udp} 351
show session-limit 123
show session-limit begin *rule_number* end *rule_number* 123
show session-limit *rule_number* 123
show session-limit status 123
show setenv-startup 330
show snmp status 322
show socket listen 41
show socket open 41
show software-watchdog-timer log 365
show software-watchdog-timer status 365
show system default-interface-group 81

show system default-interface-group system-service 81
show system default-snat 81
show system route default-wan-trunk 355
show system route dynamic-vpn 355
show system route nat-1-1 355
show system route policy-route 355
show system route site-to-site-vpn 355
show system snat default-snat 356
show system snat nat-1-1 355
show system snat nat-loopback 356
show system snat order 355
show system snat policy-route 355
show system uptime 41
show usb-storage 75
show username [*username*] 270
show users {*username* | all | current} 275
show users default-setting {all | user-type {admin|user|guest|limited-admin|ext-user}} .. 271
show users idle-detection-settings 272
show users retry-settings 272
show users simultaneous-logon-settings 272
show users update-lease-settings 272
show version 41
show voice-mail 157
show voice-port <*voiceport* | all> 148
show vpn-concentrator [*profile_name*] 131
show vpn-counters 132
show vrpt send device information interval 342
show vrpt send interface statistics interval 342
show vrpt send system status interval 342
show zone [*profile_name*] 98
show zone binding-iface 98
show zone default-binding 98
show zone none-binding 98
show zone system-default 98
show zone user-define 98
shutdown 34
sip-server-address {*ipv4*|*hostname*} 181
sip-server-address {*ipv4*|*hostname*} 182
sip-server-port <1..65535> 181
sip-server-port <1..65535> 182
slot *obtrunk_slot* port *obtrunk_port* msn *obtrunk_msn_port* 191
smtp-address {*ip* | *hostname*} 145
smtp-address {*ip* | *hostname*} 347
smtp-auth username *username* password *password* 145
smtp-auth username *username* password *password* 347
snaplen <68..1512> 360
snmp-server rule {*rule_number*|append|insert *rule_number*} access-group {ALL|*address_object*}
zone {ALL|*zone_object*} action {accept|deny} 322
snmp-server rule move *rule_number* to *rule_number* 322
split-size <1..2048> 360
storage <internal|usbstorage> 360
strategy {least-recent|round-robin|fewest-call|random|ring-all} 234
strategy {least-recent|round-robin|fewest-call|random|ring-all} 237
subject *subject_string* 247
system default-interface-group *group-name* 81
system default-interface-group system-service *group-name* 81
tapi-line *exten_num* 153
telnet 34
test aaa 34

test aaa {server|secure-server} {ad|ldap} host {*hostname*|*ipv4-address*} [host {*hostname*|*ipv4-address*}] port <1..65535> base-dn *base-dn-string* [bind-dn *bind-dn-string* password *password*] login-name-attribute *attribute* [alternative-login-name-attribute *attribute*] account *account-name* 296
timeout {<1..99999>|default} 234
timeout {<1..99999>|default} 237
timeout-action {[no-timeout]|[hangup]|[backup *skill_name*]|[hunt *ext_num*]|[aa *aa_name*]|[extension *ext_num*]|[voicemail *ext_num*]} 237
timeout-action {[no-timeout]|[hangup]|[backup *skill_name*]|[page *ext_num*]|[hunt *ext_num*]|[aa *aa_name*]|[extension *ext_num*]|[voicemail *ext_num*]} 236
timeout-action {hangup|operator} 194
timeout-action {hangup|operator} 195
timeout-action {hangup|operator} 198
timeout-action aa PBX_GRP_NAME 194
timeout-action aa PBX_GRP_NAME 195
timeout-action aa PBX_GRP_NAME 198
timeout-action acd PBX_ACD_NUM 194
timeout-action acd PBX_ACD_NUM 195
timeout-action acd PBX_EXTEN_NUM 198
timeout-action extension PBX_EXTEN_NUM 194
timeout-action extension PBX_EXTEN_NUM 195
timeout-action extension PBX_EXTEN_NUM 198
timeout-action hunt PBX_HUNT_NUM 194
timeout-action hunt PBX_HUNT_NUM 195
timeout-action hunt PBX_HUNT_NUM 198
timeout-action other PBX_OTHER_NUM 194
timeout-action other PBX_OTHER_NUM 195
timeout-action other PBX_OTHER_NUM 198
timeout-action page PBX_PAGE_NUM 194
timeout-action page PBX_PAGE_NUM 195
timeout-action page PBX_PAGE_NUM 198
traceroute 34
traceroute {*ip* | *hostname*} 359
traceroute {*ip* | *hostname*} 359
traffic-prioritize {tcp-ack|content-filter|dns|ipsec-vpn} bandwidth <0..1048576> priority <1..7> [maximize-bandwidth-usage]; 55
traffic-prioritize {tcp-ack|content-filter|dns|ipsec-vpn} deactivate 55
transform-set {ah-md5 | ah-sha} [{ah-md5 | ah-sha} [{ah-md5 | ah-sha}]] 129
transform-set *esp_crypto_algo* [*esp_crypto_algo* [*esp_crypto_algo*]] 129
transform-set isakmp-algo [isakmp_algo [isakmp_algo]] 128
trigger append incoming *service_name* trigger *service_name* 87
trigger delete <1..8> 87
trigger insert <1..8> incoming *service_name* trigger *service_name* 87
trigger move <1..8> to <1..8> 87
type {internal|external|general} 66
unlock lockout-users *ip* | console 275
update-policy *autoprov_policy* 245
update-time hour <0..23> minute <0..59> 250
usb-storage mount 75
usb-storage umount 75
usb-storage warn *number* <*percentage*|megabyte> 75
use-defined-mac 66
username rename *username username* 270
username *username* [no] description *description* 270
username *username* [no] logon-lease-time <0..1440> 271
username *username* [no] logon-re-auth-time <0..1440> 271
username *username* [no] logon-time-setting <default | manual> 270
username *username* nopassword user-type {admin | guest | limited-admin | user} 270
username *username* password *password* user-type {admin | guest | limited-admin | user} 270

username *username* user-type ext-user 270
users default-setting [no] logon-lease-time <0..1440> 271
users default-setting [no] logon-re-auth-time <0..1440> 272
users default-setting [no] user-type <admin |ext-user|guest|limited-admin|user> 272
users force-logout *ip* | *username* 275
voice-mail address *e-mail* 157
voicemail *feature_code* 143
vpn-concentrator rename *profile_name profile_name* 132
vrpt send device information interval <15..3600> 342
vrpt send interface statistics interval <15..3600> 342
vrpt send system status interval <15..3600> 342
wait-music *music_name* 234
wait-music *music_name* 237
write 330
write 34
zone *profile_name* 98