

User's Guide

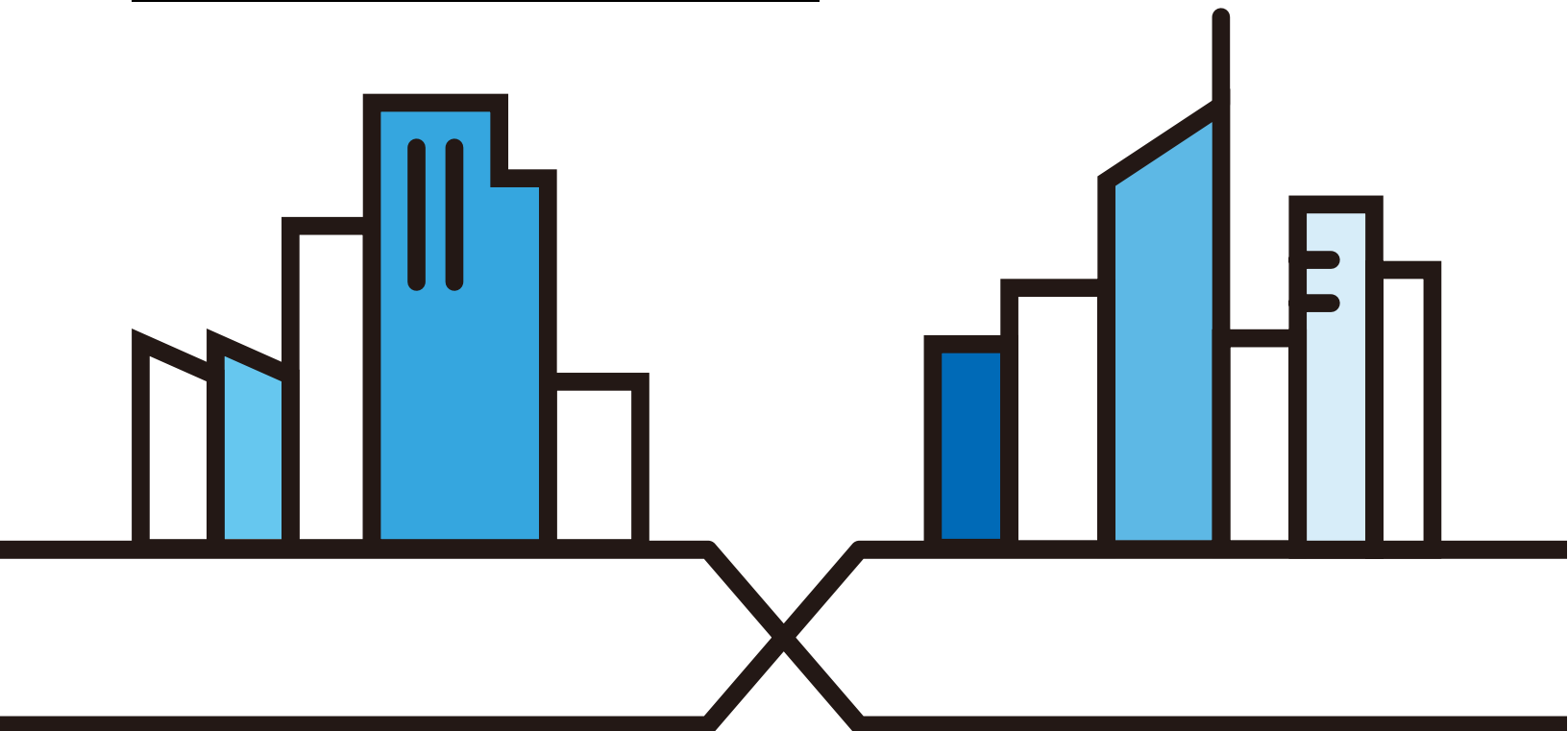
IES4105

2U 5-slot Temperature-Hardened Chassis MSAN

Default Login Details

In-band IP Address	http://192.168.1.1
Out-of-band IP Address	http://192.168.0.1
User Name	admin
Password	1234

Version 3.60 Edition 1, 2/2020



IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

Screenshots and graphics in this book may differ slightly from your product due to differences in your product firmware or your computer operating system. Every effort has been made to ensure that the information in this manual is accurate.

Related Documentation

- More Information

Go to **support.zyxel.com** to find other information on the IES.



Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this 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 IES4105 may be referred to as the “IES” in this guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A right angle bracket (>) within a navigation path or screen name denotes a mouse click. For example, **Sys** > **IP Setup** > **IPv6 Setup** means you first click **Sys** in the navigation panel, then the **IP Setup** sub menu and finally the **IPv6 Setup** tab to get to that screen.

Command Syntax Conventions

- Required input values are in angle brackets <>; for example, ping <ip-address> means that you must specify an IP number for this command.
- Lists (such as <port-list>) consist of one or more elements separated by commas. Each element might be a single value (1, 2, 3, ...) or a range of values (1-2, 3-5, ...) separated by a dash. Use an asterisk (*) to indicate all possible elements.
- The | (bar) symbol means “or”.
- Optional fields are in square brackets [].
- The <cr> means press the [ENTER] key.

Icons Used in Figures

Figures in this user guide may use the following generic icons. The IES icon is not an exact representation of your device.

IES 	DSL Router 	Switch 
Router 	ONT 	Splitter 

Server 	Remote MSAN 	MDF 
Street Pole 	Street Cabinet 	Home 
Hotel 	Branch Office 	

Contents Overview

Introduction and Hardware	19
System Introduction	20
Specifications	33
Hardware Installation and Connections	37
Maintenance	58
Web Configurator	64
The Web Configurator	65
Access Control List Screens	75
Alarm Screens	96
Diagnostic Screens	111
Line Card	117
Maintenance Screens	119
Multicast Screens	122
Port Setup Screens	139
Profile Screens	167
Statistics Screens	208
Switch Screens	232
Sys Screens	243
VLAN Screens	268
VoIP	283
Config Save	298
Commands	300
The CLI	301
Initial Setup	311
Management	315
Line Card Management	344
Switch Features	346
ADSL	364
DHCP	366
Multicast	372
Static Multicast Commands	379
IP	381
IPv6	383
MTU	389
PPPoE Intermediate Agent	390
QoS	394

Static Route	403
VDSL	404
FE	419
VLAN	420
VoIP	434
IEEE 802.1x Authentication	461
Troubleshooting, Appendices, and Index	467
Troubleshooting	468

Table of Contents

Document Conventions	3
Contents Overview	5
Table of Contents	7
 Part I: Introduction and Hardware.....	 19
Chapter 1	
System Introduction	20
1.1 Introduction	20
1.2 IES Front Panel	20
1.3 Management Card	21
1.4 ADSL Line Card	22
1.4.1 Ports	23
1.4.2 Pin Assignments	23
1.5 VDSL Line Card	24
1.5.1 Ports	25
1.5.2 Pin Assignments	25
1.6 VoIP Line Card	26
1.6.1 Ports	27
1.6.2 Pin Assignments	27
1.7 AC Power Module	28
1.7.1 Port	29
1.8 DC Power Module	29
1.8.1 Ports	29
1.9 Dual Power Module	30
1.9.1 Ports	30
1.10 Fan Module	30
1.10.1 Heat Dissipation	31
1.10.2 Monitoring	31
1.10.3 LED Indicators	31
1.10.4 Speed Control	32
1.10.5 Alarm Thresholds	32
 Chapter 2	
Specifications	33
2.1 Management Card	34

2.2 ADSL2+ Line Card	35
2.3 VDSL2+ Line Card	35
2.4 VoIP Line Card	35
2.5 Firmware Naming Conventions	36

Chapter 3

Hardware Installation and Connections.....37

3.1 Overview	37
3.2 Installing the IES	37
3.2.1 Installing the IES in a Rack	37
3.3 Bonding the IES	40
3.4 Grounding Yourself	41
3.5 Installing the Cards	42
3.5.1 Installing the Controller and Line Cards	42
3.5.2 Removing Controller and Line Cards	43
3.6 Connecting the MSC	45
3.6.1 Connecting the COM Connector	45
3.6.2 Connecting the Gigabit Ethernet Interfaces	46
3.7 Installing a Transceiver	47
3.8 Removing a Transceiver	47
3.8.1 Connecting the Console Port	48
3.8.2 Connecting the MGMT Port	49
3.9 Connecting Service Cables	49
3.9.1 Connecting DSL Cards	50
3.9.2 Connecting VoIP Line Cards	51
3.10 Connecting to an MDF	52
3.11 Connecting the Power	52
3.11.1 Procedure to Connect the AC Power	53
3.11.2 Procedure to Connect the DC Power	55
3.11.3 Powering the IES	57

Chapter 4

Maintenance.....58

4.1 Fan Maintenance	58
4.1.1 Procedure to Remove and Install the Fan Module	58
4.2 Power Maintenance	60
4.2.1 Procedure to Change an AC Power Module	60
4.2.2 Procedure to Change a DC Power Module	61

Part II: Web Configurator..... 64

Chapter 5**The Web Configurator.....65**

5.1 Web Configurator Introduction	65
5.2 System Login	65
5.3 Navigation Panel	66
5.4 Saving Your Configuration	68
5.5 Logging Out of the Web Configurator	69
5.6 System Info (Home) Screen	69
5.6.1 Card Status Details	70
5.7 Enable Privilege Screen	73
5.8 Enable Password Screen	74

Chapter 6**Access Control List Screens 75**

6.1 Anti-MAC Spoofing Screen	75
6.2 DHCP Transparent Screen	75
6.3 DHCP L2 Agent Screen	76
6.4 IEEE 802.1x	78
6.4.1 General Setup	78
6.4.2 RADIUS Server	79
6.4.3 User Profile	80
6.4.4 Port Setting	81
6.4.5 Port Status	83
6.5 Loop Guard	84
6.5.1 Loopguard Setup	86
6.5.2 Statistics Screen	88
6.6 Packet Filter Screen	90
6.7 PPPoE	92
6.7.1 PPPoE Intermediate Agent	92
6.7.2 PPPoE Screen	92
6.8 ACL Rule Screen	94

Chapter 7**Alarm Screens 96**

7.1 Current Alarm Screen	96
7.2 History Alarm Screen	97
7.3 Alarm Input Screens	98
7.3.1 Alarm Input Screen	98
7.3.2 CPU Overload Alarm	99
7.3.3 System Suppress	100
7.4 Alarm Definition Screen	100
7.4.1 DSL	100
7.4.2 Equipment	102

7.4.3 System	104
7.4.4 Ethernet	105
7.4.5 VoIP	107
7.4.6 FE	109

Chapter 8

Diagnostic Screens 111

8.1 DELT Test Screen	111
8.2 IP Ping Screen	112
8.3 MLT Screen	113
8.4 SELT Test Screen	115

Chapter 9

Line Card 117

9.1 Line Card	117

Chapter 10

Maintenance Screens 119

10.1 Configuration Backup Screen	119
10.2 Configuration Restore Screen	119
10.3 Configuration Reset Screen	120
10.4 Firmware Upgrade Screen	120
10.5 Reboot Screen	121

Chapter 11

Multicast Screens 122

11.1 IGMP Introduction	122
11.1.1 IP Multicast Addresses	122
11.1.2 IGMP Snooping	122
11.1.3 IGMP Proxy	123
11.1.4 IGMP Snooping and Proxy Note	123
11.1.5 IGMP Fast Leave	124
11.1.6 Multicast Listener Discovery	124
11.2 IGMP Setup Screens	124
11.2.1 IGMP Setup Screen	124
11.2.2 Port Setup Screen	126
11.2.3 Port MVLAN Setup Screen	126
11.3 IGMP Privilege Profile Screen	128
11.4 IGMP Status Screens	129
11.4.1 IGMP Status	129
11.4.2 IGMP Port Group	131
11.4.3 IGMP Port Statistics	132
11.4.4 IGMP Port Log	134

11.5 MVLAN Setup Screens	135
11.5.1 MVLAN Setup Screen	135
11.5.2 MVLAN Table Screen	136
11.6 Static Multicast Screen	137

Chapter 12

Port Setup Screens 139

12.1 Alarm Port Setup Screen	139
12.2 Port Copy Screen	142
12.3 Port Default Screen	142
12.4 DHCP Screen	143
12.5 DSL	143
12.6 DSL Status	147
12.7 FDB	147
12.8 Permanent Virtual Circuits	149
12.8.1 LLC	150
12.8.2 VC Mux	150
12.8.3 PVC Setup Screen	150
12.9 QoS	153
12.10 H.248 Port Setup	155
12.11 SIP Port Setup	159
12.12 FE	163

Chapter 13

Profile Screens 167

13.1 Profiles Overview	167
13.2 Access Control List (ACL) Screen	167
13.3 Enet Alarm Profile Screens	169
13.4 DSL Screens	171
13.4.1 Line Profile Screen	171
13.4.2 Channel Profile Screen	183
13.4.3 Template Profile Screen	184
13.5 DSL Alarm Profile Screens	185
13.5.1 Alarm Profile Screen	185
13.5.2 Alarm Line Profile Screen	187
13.5.3 Alarm Channel Profile Screen	188
13.5.4 Alarm Template Profile Screen	189
13.6 QoS Screens	190
13.6.1 VC-Shaping Screen	190
13.6.2 Shaping Screen	191
13.6.3 WRR-WFQ Screen	192
13.7 VoIP Alarm Profile Screen	193
13.8 VoIP DSP Profile Screen	194

13.9 FE Alarm Profile Screens	195
13.10 Profile VoIP SIP Screen	197
13.11 Profile VoIP SIP Call Service Screen	200
13.12 Profile VoIP SIP Dial Plan Screen	203
13.13 Xdsl Bonding Profile Screens	206

Chapter 14

Statistics Screens.....208

14.1 ARP Table	208
14.1.1 How ARP Works	208
14.1.2 ARP Table Screen	208
14.2 DHCP Snoop	209
14.3 DDMI	210
14.4 Dot3ad Status	212
14.5 MAC Table Screen	214
14.6 Online Users Screen	216
14.7 Port Statistics	216
14.7.1 Ethernet Port Statistics	217
14.7.2 VoIP Port Statistics	219
14.7.3 DSL Line Card Statistics	222
14.7.4 FE Port Statistics	225
14.8 RSTP Statistics	228
14.9 Bonding Status	229

Chapter 15

Switch Screens 232

15.1 Mirror Screen	232
15.2 RSTP	233
15.2.1 RSTP Setup	235
15.3 Switch Port Setup Screen	236
15.4 Switch Setup	237
15.4.1 General Screen	237
15.4.2 Dot3ad Screen	238
15.4.3 Isolation Screen	239
15.4.4 DSCP Screen	240
15.4.5 Storm Control Screen	241
15.4.6 VC-Shaping Screen	242

Chapter 16

Sys Screens.....243

16.1 Authentication, Authorization and Accounting	243
16.1.1 Local User Accounts	243
16.1.2 RADIUS and TACACS+	244

16.1.3 Accounting Setup	244
16.1.4 Authentication Setup	245
16.1.5 Authorization Screen	246
16.1.6 RADIUS Server Setup	247
16.1.7 TACACS+ Server Setup	249
16.2 Service Access Control	252
16.2.1 SNMP	252
16.2.2 Secured Client Screen	254
16.2.3 Secured Client6 Screen	256
16.3 Syslog	257
16.4 General Setup	257
16.5 IP Setup	259
16.5.1 IPv4 Setup	259
16.5.2 IPv6 Setup	261
16.6 Monitor Screens	261
16.6.1 Monitor	262
16.6.2 Statistics	263
16.6.3 CPU Utilization	265
16.7 System Information	266
16.8 User Account Screen	267

Chapter 17

VLAN Screens 268

17.1 VLAN Introduction	268
17.2 IEEE 802.1Q Tagged VLAN	268
17.2.1 Forwarding Tagged and Untagged Frames	269
17.3 Enet VLAN Screen	269
17.4 Enet VLAN Untag Screen	270
17.5 Port VLAN TLS Screen	271
17.5.1 VLAN TLS Setup Screen	273
17.6 Port VLAN Trunk Screens	273
17.6.1 Uni-Tag Setup	274
17.6.2 Uni-Untag Setup	275
17.7 Port VLAN Translation Screen	278
17.7.1 VLAN Translation Setup	279
17.8 Port VLAN Transparent Screen	280
17.8.1 VLAN Transparent Setup	281
17.9 VLAN S-tag Setup	282

Chapter 18

VoIP 283

18.1 Country Code Screen	283
18.2 H.248 Screens	286

18.2.1 H.248 Setup	287
18.2.2 H.248 Statistics	289
18.3 IP Setup Screens	290
18.3.1 VoIP Interface Screen	290
18.3.2 RTP Interface Screen	291
18.4 VoIP Key Pattern Screen	292
18.5 VoIP Line Info Screen	293
18.6 POTS Ring Screen	295
18.7 POTS Flash Screen	296
Chapter 19	
Config Save	298
19.1 The Config Save Screen	298
 Part III: Commands	 300
Chapter 20	
The CLI	301
20.1 Accessing the CLI	301
20.1.1 Console Port	301
20.1.2 Local Access by Telnet	301
20.1.3 Remote Access by Telnet	302
20.2 Logging in	302
20.3 Using Shortcuts and Getting Help	302
20.3.1 Entering Partial Commands	303
20.4 Common Command Notation	303
20.5 Command Summary	304
20.6 Privilege Levels, Accounts and Passwords	305
20.6.1 Command Example	307
20.6.2 Privilege Levels for Login Accounts	307
20.6.3 Privilege Levels for Sessions	308
20.7 Command Modes	309
20.7.1 Modes for Privilege Levels 0-12	309
20.7.2 Modes for Privilege Levels 13-14	309
20.8 Dual Image Files	310
20.9 Dual Configuration Files	310
20.10 Saving Your Configuration	310
20.11 Logging Out	310
 Chapter 21	
Initial Setup	311

21.1 Changing the Administrator Password	311
21.2 Changing the Enable Password	311
21.3 Changing the Management IP Address	311
21.4 Changing the Management VLAN	312
21.5 Looking at Basic System Information	313
21.6 Looking at the Operating Configuration	313
21.7 Provisioning Slots	314

Chapter 22

Management 315

22.1 Alarm Commands	315
22.2 Date and Time Commands	318
22.3 Hardware Monitor Commands	319
22.4 Running Configuration Commands	320
22.4.1 Command Examples	323
22.5 SNMP Server Commands	323
22.6 System Maintenance Commands	326
22.7 FTP for Configuration and Firmware Files	328
22.7.1 Filename Conventions	328
22.7.2 FTP Command Line Procedure	329
22.8 AAA Commands	329
22.8.1 AAA Command Summary	330
22.8.2 Command Examples	335
22.9 Performance Management	337
22.9.1 Performance Management Commands Summary	337
22.9.2 Command Examples	341
22.10 Remote Management	341
22.10.1 Remote Management Commands Summary	342
22.10.2 Command Examples	343
22.11 Syslog	343
22.11.1 Syslog Commands Summary	343

Chapter 23

Line Card Management.....344

23.1 Line Card Management Commands Summary	344
23.1.1 Command Examples	344

Chapter 24

Switch Features 346

24.1 ACL Commands	346
24.1.1 Command Examples	350
24.2 Broadcast Storm Commands	351
24.3 Daisy Chain Commands	351

24.4 Forwarding Database Commands	352
24.5 GE Uplink Commands	355
24.6 Link Aggregation Commands	357
24.7 Loop Guard Commands	358
24.7.1 Command Examples	360
24.8 Port Isolation Commands	360
24.9 RSTP Commands	361
24.10 Mirror Commands	362
24.10.1 Mirror Commands Summary	362
24.10.2 Command Examples	363
Chapter 25	
ADSL	364
25.1 ATM VC Commands Summary	365
Chapter 26	
DHCP	366
26.1 Command Examples	370
Chapter 27	
Multicast.....	372
27.1 IGMP/MLD Commands	372
27.1.1 Command Examples	377
Chapter 28	
Static Multicast Commands.....	379
28.1 Static Multicast Commands Summary	379
28.1.1 Command Examples	380
Chapter 29	
IP.....	381
29.1 IP Commands Summary	381
Chapter 30	
IPv6	383
30.1 IPv6 Commands Summary	387
Chapter 31	
MTU	389
31.1 MTU Commands Summary	389
Chapter 32	
PPPoE Intermediate Agent	390

32.1 PPPoE Intermediate Agent Commands Summary	391
32.1.1 Command Examples	392
Chapter 33	
QoS.....	394
33.1 DSCP to Priority Bit Mapping Commands	394
33.1.1 Command Examples	395
33.2 QoS Commands	396
33.2.1 Command Examples	400
Chapter 34	
Static Route.....	403
Chapter 35	
VDSL.....	404
35.1 VDSL Commands	408
Chapter 36	
FE	419
Chapter 37	
VLAN.....	420
37.1 VLAN Overview	420
37.1.1 Transparent VLAN Mode	421
37.1.2 VLAN Tagging and Trunk Mode	421
37.1.3 Stacking VLAN Tagging and Trunk Mode	421
37.1.4 VLAN Translation and Aggregation Mode	422
37.1.5 Stacking VLAN Translation and Aggregation Mode	423
37.1.6 VLAN TLS Mode	423
37.1.7 Multicast VLAN	424
37.1.8 Management and VoIP VLAN	424
37.2 General VLAN Commands	425
37.2.1 Command Examples	426
37.3 Transparent VLAN Commands	426
37.3.1 Command Examples	427
37.4 VLAN TLS Commands	427
37.4.1 Command Examples	429
37.5 VLAN Translation and Aggregation Commands	429
37.5.1 Command Examples	430
37.6 VLAN Trunk Commands	431
37.6.1 Command Examples	433
Chapter 38	
VoIP	434

38.1 VoIP Overview	434
38.2 H.248 and SIP	434
38.3 H.248	434
38.4 SIP	435
38.5 VoIP Commands	435
38.6 H.248 Command Examples	449
38.7 VoIP SIP Commands (SIP Firmware Only)	450
38.8 SIP Command Examples	458
Chapter 39	
IEEE 802.1x Authentication	461
39.1 802.1x Command Summary	462
39.1.1 Command Examples	464
 Part IV: Troubleshooting, Appendices, and Index.....	 467
Chapter 40	
Troubleshooting.....	468
40.1 LEDs	468
40.2 Power, Hardware Connection, and LED Problems	468
40.3 Voice Problems	469
40.3.1 No Voice on an ADSL Connection	469
40.3.2 No Voice on a VoIP Connection	469
40.3.3 Testing Wiring	469
Appendix A Customer Support	470
Appendix B Legal Information	476

PART I

Introduction and Hardware

CHAPTER 1

System Introduction

This chapter describes the system features, specifications and applications of the IES.

1.1 Introduction

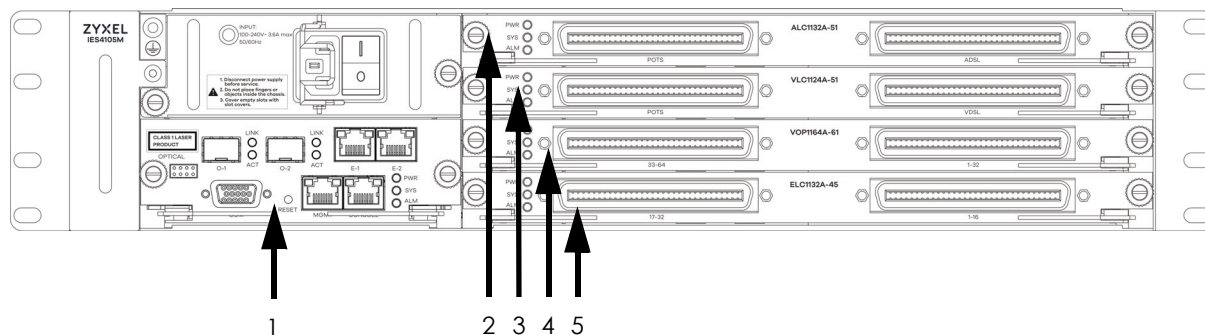
The Integrated Ethernet Switch (IES) Multi-Service Access Node (MSAN) is Zyxel's next-generation MDU (Multi-Dwelling Unit) solution for providing both data and VoIP services using copper wires as the last mile media. The IES can be deployed in a basement or street cabinet for fiber-to-the-building or fiber-to-the-curb (FTTC) applications. The IES is compact and offers high density ADSL, VDSL, POTS, and Fast Ethernet interface cards to provide triple play services (high speed Internet, IPTV, and voice). It supports active Gigabit Ethernet deployment scenarios.

The hot-swappable fan module and line cards provide plug-and-play, on-site operation and minimize the maintenance window. The management switch card provides the convenience of centralized network traffic supervision.

The IES employs mounting brackets for standard 19-inch (482 mm) rack mounting.

1.2 IES Front Panel

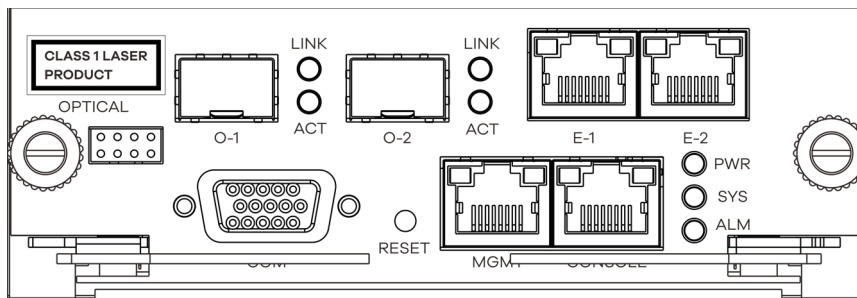
The following figure shows the chassis front panel with cards installed. The front of the IES features the modules, ports, and interfaces.

Figure 1 IES Front Panel**Table 1** Slots, Cards, and Modules

SLOTS	SLOT TYPE	MODULE OR CARD NAME	FUNCTION
	Fan Module	IES4105M-FAN	Houses, controls, and monitors the fans.
	Power Module	IES4105M-ACA IES4105M-DCA IES4105M-DU	Power module (AC, DC, or AC/DC).
1	Management Card	MSC1002GA	Install a management card in slot 1. Manage and monitor the system and centralize network traffic supervision. Connects the IES to the backbone.
2 ~ 5	Line Card	ALC1132A-51 VLC1124A-51 VOP1164A-61	Install line cards in slots 2 to 5. The ALC (ADSL Line Card) with built-in splitter provides 32-line Annex A ADSL2/2+ connection for broadband data services and IPTV applications. The VLC (VDSL Line Card) with built-in splitter provides 24-line VDSL2 connection for broadband data services and IPTV applications. The VOP (VoIP) line card provides 64-line SIP/H.248 VoIP POTS connections for VoIP services.

1.3 Management Card

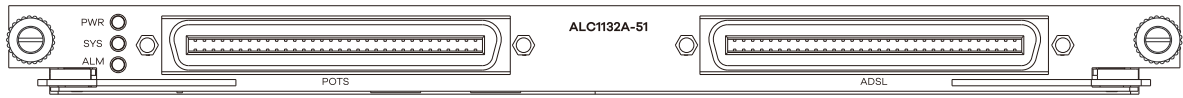
The Management Switch Card (MSC) aggregates the upstream service through active Gigabit Ethernet optical or electrical connections, manages the IES, and manages the services of the line cards. This card is hot-swappable.

Figure 2 MSC Front Panel**Table 2** MSC LEDs

LED	COLOR	STATUS	DESCRIPTION
PWR	Green	On	The management card is installed and receiving power from the chassis.
		Off	The management card is not receiving power from the chassis.
SYS	Green	Blinking	The system is initializing.
		On	The system is on and functioning properly.
		Off	The management card is not receiving power, is not ready or has malfunctioned.
ALM	Red	On	The IES has a critical alarm.
		Off	The IES has not detected a critical alarm.
LNK	Green	On	The optical Ethernet link is up.
		Off	There is no optical Ethernet link.
ACT	Green	Blinking	There is optical Ethernet activity.
		Off	The connection is idle.
The following LEDs apply to the Gigabit ports.			
Green	Blinking	There is Ethernet traffic at 1000 Mbps.	
	On	A 1000 Mbps Ethernet link is up.	
	Off	The 1000 Mbps Ethernet link is down.	
Amber	Blinking	There is Ethernet traffic at 10/100 Mbps.	
	On	A 10/100 Mbps Ethernet link is up.	
	Off	The 10/100 Mbps Ethernet link is down.	
The following LEDs apply to the Ethernet management port.			
Green	On	The Ethernet link is up at 10 Mbps.	
	Blinking	There is Ethernet traffic at 10 Mbps.	
	Off	There is no 10 Mbps Ethernet link.	
Amber	On	A 100 Mbps Ethernet link is up.	
	Blinking	There is Ethernet traffic at 100 Mbps.	
	Off	There is no 100 Mbps Ethernet link.	

1.4 ADSL Line Card

The ALC provides up to 32 ADSL2+ lines for data and IPTV services and includes internal splitters. This card is hot-swappable.

Figure 3 ALC Front Panel**Table 3** ALC LEDs

LED	COLOR	STATUS	DESCRIPTION
PWR	Green	On	The line card is turned on.
		Off	The line card is turned off or has failed.
SYS	Green	On	The line card is running.
		Off	The line card is not ready or has failed.
ALM	Red	On	The line card has a critical alarm.
		Off	The line card is operating normally.

1.4.1 Ports

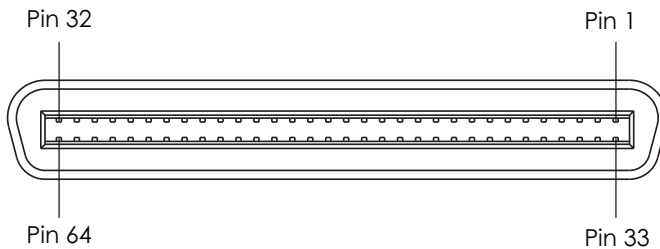
This table describes the ports on the ALC front panel.

Table 4 ALC Ports

LABEL	DESCRIPTION
POTS	One 32-line POTS port with Telco 64 connector
ADSL	One 32-line data and voice port with Telco 64 connector

1.4.2 Pin Assignments

The line card Telco 64 connectors (also known as Champ 64) are female. The following figure and table describe the pinouts of the Telco 64 connectors.

Figure 4 Telco 64 Connector Pins**Table 5** ALC POTS 1-32 and ADSL 1-32 Telco 64 Connector Pin Layout

POTS 1-32			ADSL 1-32		
Ring Pin	Tip Pin	Function	Ring Pin	Tip Pin	Function
1	2	POTS pair 1	1	2	ADSL2+ pair 1
33	34	POTS pair 2	33	34	ADSL2+ pair 2
3	4	POTS pair 3	3	4	ADSL2+ pair 3
35	36	POTS pair 4	35	36	ADSL2+ pair 4
5	6	POTS pair 5	5	6	ADSL2+ pair 5
37	38	POTS pair 6	37	38	ADSL2+ pair 6

Table 5 ALC POTS 1-32 and ADSL 1-32 Telco 64 Connector Pin Layout (continued)

POTS 1-32			ADSL 1-32		
7	8	POTS pair 7	7	8	ADSL2+ pair 7
39	40	POTS pair 8	39	40	ADSL2+ pair 8
9	10	POTS pair 9	9	10	ADSL2+ pair 9
41	42	POTS pair 10	41	42	ADSL2+ pair 10
11	12	POTS pair 11	11	12	ADSL2+ pair 11
43	44	POTS pair 12	43	44	ADSL2+ pair 12
13	14	POTS pair 13	13	14	ADSL2+ pair 13
45	46	POTS pair 14	45	46	ADSL2+ pair 14
15	16	POTS pair 15	15	16	ADSL2+ pair 15
47	48	POTS pair 16	47	48	ADSL2+ pair 16
17	18	POTS pair 17	17	18	ADSL2+ pair 17
49	50	POTS pair 18	49	50	ADSL2+ pair 18
19	20	POTS pair 19	19	20	ADSL2+ pair 19
51	52	POTS pair 20	51	52	ADSL2+ pair 20
21	22	POTS pair 21	21	22	ADSL2+ pair 21
53	54	POTS pair 22	53	54	ADSL2+ pair 22
23	24	POTS pair 23	23	24	ADSL2+ pair 23
55	56	POTS pair 24	55	56	ADSL2+ pair 24
25	26	POTS pair 25	25	26	ADSL2+ pair 25
57	58	POTS pair 26	57	58	ADSL2+ pair 26
27	28	POTS pair 27	27	28	ADSL2+ pair 27
59	60	POTS pair 28	59	60	ADSL2+ pair 28
29	30	POTS pair 29	29	30	ADSL2+ pair 29
61	62	POTS pair 30	61	62	ADSL2+ pair 30
31	32	POTS pair 31	31	32	ADSL2+ pair 31
63	64	POTS pair 32	63	64	ADSL2+ pair 32

1.5 VDSL Line Card

The VLC provides up to 24 VDSL2 lines for data and IPTV services and includes internal splitters. This card is hot-swappable.

Figure 5 VLC Front Panel

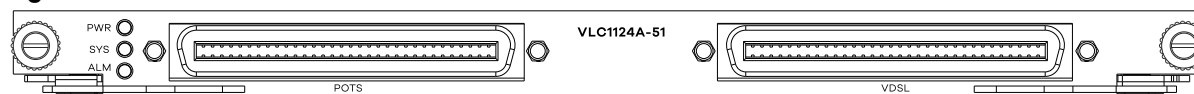


Table 6 VLC LEDs

LED	COLOR	STATUS	DESCRIPTION
PWR	Green	On	The line card is turned on.
		Off	The line card is turned off or has failed.

Table 6 VLC LEDs (continued)

LED	COLOR	STATUS	DESCRIPTION
SYS	Green	On	The line card is running.
		Off	The line card is not ready or has failed.
ALM	Red	On	The line card has a critical alarm.
		Off	The line card is operating normally.

1.5.1 Ports

This table describes the ports on the VLC front panel.

Table 7 VLC Ports

LABEL	DESCRIPTION
POTS	One 24-line POTS port with Telco 64 connector
VDSL	One 24-line data and voice port with Telco 64 connector

1.5.2 Pin Assignments

The line card Telco 64 connectors (also known as Champ 64) are female. The following figure and table describe the pinouts of the Telco 64 connectors.

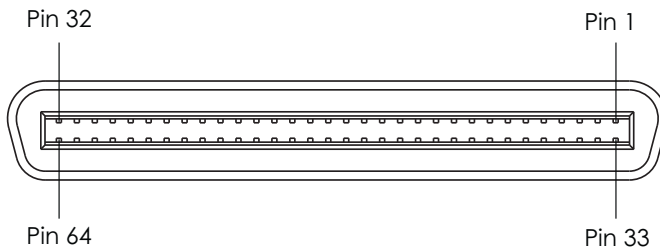
Figure 6 Telco 64 Connector Pins

Table 8 VLC POTS 1-24 and VDSL 1-24 Telco 64 Connector Pin Layout

POTS 1-24			VDSL 1-24		
Ring Pin	Tip Pin	Function	Ring Pin	Tip Pin	Function
1	2	POTS pair 1	1	2	VDSL2 pair 1
33	34	POTS pair 2	33	34	VDSL2 pair 2
3	4	POTS pair 3	3	4	VDSL2 pair 3
35	36	POTS pair 4	35	36	VDSL2 pair 4
5	6	POTS pair 5	5	6	VDSL2 pair 5
37	38	POTS pair 6	37	38	VDSL2 pair 6
7	8	POTS pair 7	7	8	VDSL2 pair 7
39	40	POTS pair 8	39	40	VDSL2 pair 8
9	10	POTS pair 9	9	10	VDSL2 pair 9
41	42	POTS pair 10	41	42	VDSL2 pair 10
11	12	POTS pair 11	11	12	VDSL2 pair 11
43	44	POTS pair 12	43	44	VDSL2 pair 12

Table 8 VLC POTS 1-24 and VDSL 1-24 Telco 64 Connector Pin Layout (continued)

POTS 1-24			VDSL 1-24		
13	14	POTS pair 13	13	14	VDSL2 pair 13
45	46	POTS pair 14	45	46	VDSL2 pair 14
15	16	POTS pair 15	15	16	VDSL2 pair 15
47	48	POTS pair 16	47	48	VDSL2 pair 16
17	18	POTS pair 17	17	18	VDSL2 pair 17
49	50	POTS pair 18	49	50	VDSL2 pair 18
19	20	POTS pair 19	19	20	VDSL2 pair 19
51	52	POTS pair 20	51	52	VDSL2 pair 20
21	22	POTS pair 21	21	22	VDSL2 pair 21
53	54	POTS pair 22	53	54	VDSL2 pair 22
23	24	POTS pair 23	23	24	VDSL2 pair 23
55	56	POTS pair 24	55	56	VDSL2 pair 24
Pins 25~32 and 57~64 are not used					

1.6 VoIP Line Card

The VOP provides up to 64 POTS lines for voice. This card is hot-swappable.

Note: The installed firmware version determines whether the IES uses H.248 or SIP for VoIP (see [Section 2.5 on page 36](#) for details).

Figure 7 VOP Front Panel

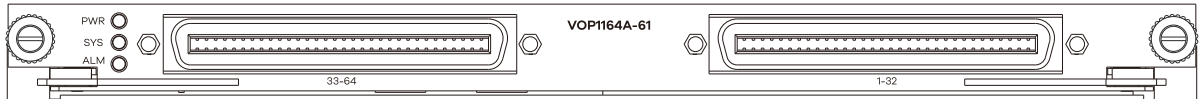


Table 9 VOP LEDs

LED	COLOR	STATUS	DESCRIPTION
PWR	Green	On	The line card is turned on.
		Off	The line card is turned off or has failed.
SYS	Green	On	The line card is running.
		Off	The line card is not ready or has failed.
ALM	Red	On	The line card has a critical alarm.
		Off	The line card is operating normally.

1.6.1 Ports

This table describes the ports on the VOP front panel.

Table 10 VOP Ports

LABEL	DESCRIPTION
1-32	One 32-line POTS port with Telco 64 connector
33-64	One 32-line POTS port with Telco 64 connector

1.6.2 Pin Assignments

The line card Telco 64 connectors (also known as Champ 64) are female. The following figure and table describe the pinouts of the Telco 64 connectors.

Figure 8 Telco 64 Connector Pins

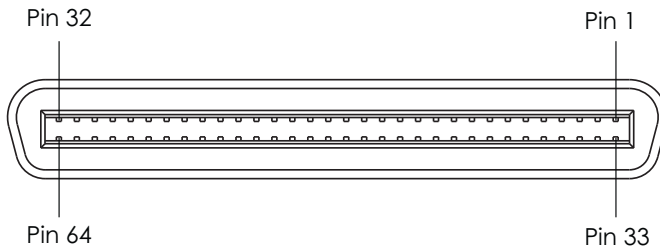


Table 11 VOP 1-32 and 33-64 Telco 64 Connector Pin Layout

1-32			33-64		
Ring Pin	Tip Pin	Function	Ring Pin	Tip Pin	Function
1	2	POTS pair 1	1	2	POTS pair 33
33	34	POTS pair 2	33	34	POTS pair 34
3	4	POTS pair 3	3	4	POTS pair 35
35	36	POTS pair 4	35	36	POTS pair 36
5	6	POTS pair 5	5	6	POTS pair 37
37	38	POTS pair 6	37	38	POTS pair 38
7	8	POTS pair 7	7	8	POTS pair 39
39	40	POTS pair 8	39	40	POTS pair 40
9	10	POTS pair 9	9	10	POTS pair 41
41	42	POTS pair 10	41	42	POTS pair 42
11	12	POTS pair 11	11	12	POTS pair 43
43	44	POTS pair 12	43	44	POTS pair 44
13	14	POTS pair 13	13	14	POTS pair 45
45	46	POTS pair 14	45	46	POTS pair 46
15	16	POTS pair 15	15	16	POTS pair 47
47	48	POTS pair 16	47	48	POTS pair 48
17	18	POTS pair 17	17	18	POTS pair 49
49	50	POTS pair 18	49	50	POTS pair 50
19	20	POTS pair 19	19	20	POTS pair 51

Table 11 VOP 1-32 and 33-64 Telco 64 Connector Pin Layout (continued)

1-32			33-64		
51	52	POTS pair 20	51	52	POTS pair 52
21	22	POTS pair 21	21	22	POTS pair 53
53	54	POTS pair 22	53	54	POTS pair 54
23	24	POTS pair 23	23	24	POTS pair 55
55	56	POTS pair 24	55	56	POTS pair 56
25	26	POTS pair 25	25	26	POTS pair 57
57	58	POTS pair 26	57	58	POTS pair 58
27	28	POTS pair 27	27	28	POTS pair 59
59	60	POTS pair 28	59	60	POTS pair 60
29	30	POTS pair 29	29	30	POTS pair 61
61	62	POTS pair 30	61	62	POTS pair 62
31	32	POTS pair 31	31	32	POTS pair 63
63	64	POTS pair 32	63	64	POTS pair 64

1.7 AC Power Module

The AC power module converts AC input into 14.5 V DC.

Figure 9 AC Power Module Front Panel

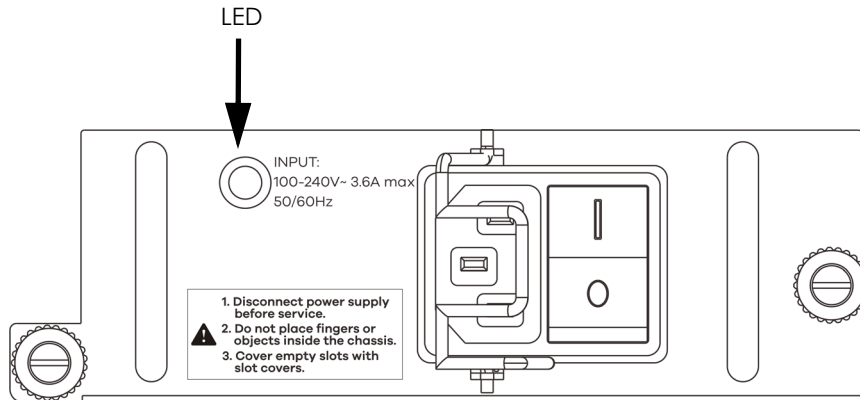


Table 12 AC Power Module LEDs

COLOR	STATUS	DESCRIPTION
Green	On	The power module is turned on and receiving power.
	Off	The power module is turned off or not receiving power.

1.7.1 Port

The port of the AC power module is located on the front panel. This table describes the port.

Table 13 AC Power Module Port

PORT	FUNCTION	CONNECTION
AC input	Allows AC power to enter the AC power module.	Use the AC power cord to connect the port to the AC power outlet. Input voltage range: 100-240 V AC/50-60 Hz

1.8 DC Power Module

The DC power module converts -36 to -72 V DC input into 14.5 V DC.

Figure 10 DC Power Module Front Panel

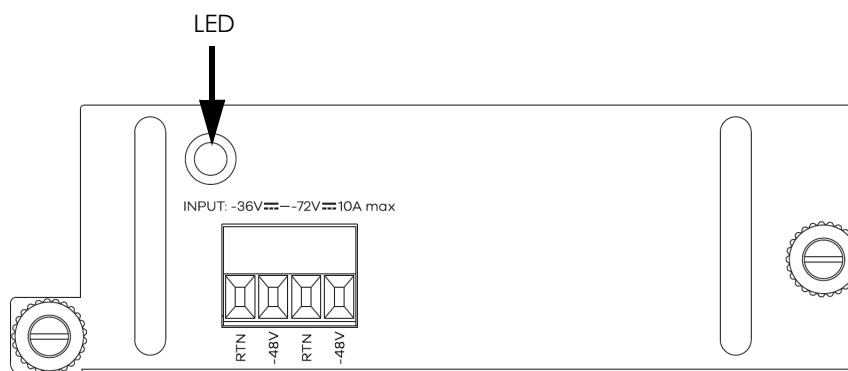


Table 14 DC Power Module LEDs

COLOR	STATUS	DESCRIPTION
Green	On	The power module is turned on and receiving power.
	Off	The power module is turned off or not receiving power.

1.8.1 Ports

The ports of the DC power module are located on the front panel. This table describes the ports.

Table 15 DC Power Module Ports

PORT	FUNCTION	CONNECTION
Input 1 (-48 and ground terminals on the left) Input 2 (-48 and ground terminals on the right)	Allows -48 V power to enter the PSU DC.	See Table 18 on page 33 for the gauge of power wires to use. It is recommended to connect input 1 to the regular DC power source and connect input 2 to a backup DC power source such as batteries.

1.9 Dual Power Module

The dual power module converts AC input into 14.5 V DC and converts -36 to -72 V DC input into 14.5 V DC. The AC/DC dual power module can be connected to both 100-240 V AC/50-60 Hz line power and -36 to -72 V DC line power at the same time and operate on whichever is available. If both are available, the IES operates on the AC power and switches to DC power if the AC power is lost. When you deploy the IES with a UPS (uninterruptible power supply) and the alarm input specified for battery saving is triggered, the IES turns off subscriber data traffic in order to support PSTN calls for as long as possible.

Figure 11 Dual Power Module Front Panel

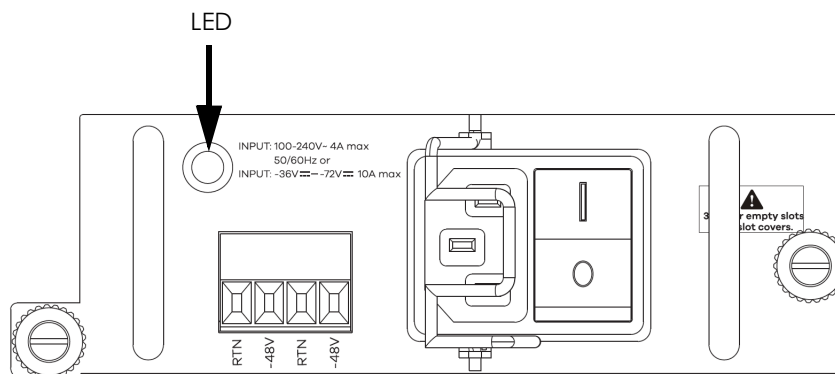


Table 16 Dual Power Module LED

COLOR	STATUS	DESCRIPTION
Green	On	The power module is turned on and receiving power.
	Off	The power module is turned off or not receiving power.

1.9.1 Ports

The ports of the dual power module are located on the front panel.

Table 17 Dual Power Module Ports

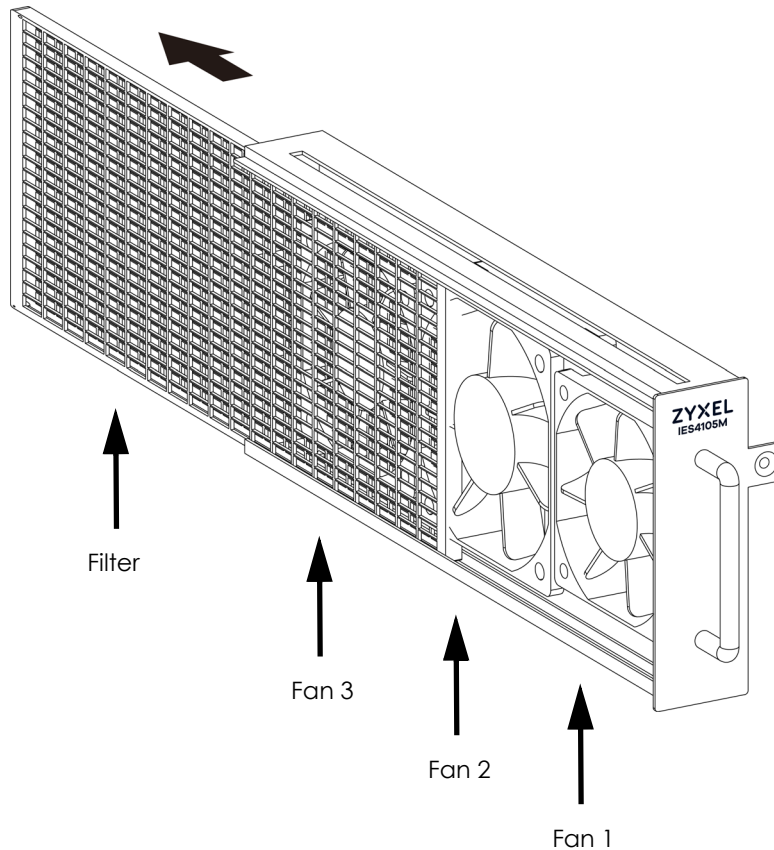
PORT	FUNCTION	CONNECTION
AC input	Allows AC power to enter the dual power module.	Use the AC power cord to connect the port to the AC power outlet. Input voltage range: 100-240 V AC/50-60 Hz
DC input 1 (-48 and ground terminals on the left) DC input 2 (-48 and ground terminals on the right)	Allows -48 V power to enter the dual power module.	See Table 18 on page 33 for the gauge of power wires to use. It is recommended to connect input 1 to the regular DC power source and connect input 2 to a backup DC power source such as batteries.

1.10 Fan Module

The chassis has a hot-swappable fan module. The fan module is at the left on the front panel. Replace the entire fan module if cleaning the fan filter does not solve the problem. Return any malfunctioning fan modules to the manufacturer. The following figure shows the IES chassis fan module with the filter partially removed and identifies the fans.

Warning! Removing the fan module causes the system to shut down after two minutes.

Figure 12 Fan Module



1.10.1 Heat Dissipation

The fan tray is installed at the left side of the IES chassis and blows air to dissipate heat. Air flows into the left side of the chassis and passes the boards before exiting from the right of the chassis.

1.10.2 Monitoring

The fan module monitors to detect whether the fans are operating in the normal state and relays the information to the IES's management card.

1.10.3 LED Indicators

Removing the fan module or fan RPM values outside of the accepted threshold triggers a critical alarm and turns on the management card's **ALM** LED.

1.10.4 Speed Control

The IES automatically adjusts the rotation speed of the fans based on the detected temperature. You can also manually set the high and low fan speed limits for raising an alarm on a specific fan. The following table covers how the IES automatically adjusts the rotation speed of the fans based on the detected temperature.

1.10.5 Alarm Thresholds

Use the Web Configurator (see [Table 163 on page 262](#)) or commands (see [Table 207 on page 320](#)) to set the high and low fan speed limits for raising an alarm on a specific fan.

CHAPTER 2

Specifications

This chapter provides the specifications for the IES and its cards.

Table 18 System Specifications

Physical specifications	
Chassis dimensions	2U Height: 88.9 mm (3.5 inches) Width: 441 mm (17.4 inches) Depth (excluding fan module handle): 266.5mm (10.5 inches)
Weight	5.2 kg including fan and power module weight; excluding card weights 8 kg including fan, power module, and 4 line cards
Rack mounting	The IES is 19-inch (482.6 mm) rack-mountable.
Number of slots	1 for the management card 4 for line cards
Wire gauge specifications	AWG (American Wire Gauge) is a measurement system for wire that specifies its thickness. As the thickness of the wire increases, the AWG number decreases. Make sure you use wires of the specified wire gauge. Ground wire: 18 AWG or larger, go up 1 gauge for a distance of more than 10 feet Telephone wire: 26 AWG or larger DC power wire: 16 AWG or larger AC power cord: 18 AWG
IES4105M-ACA Electrical specifications	
Input Power	AC input voltage range: 100-240 V AC single phase AC input frequency range: 50 Hz to 60 Hz Maximum input AC current: 3.6 A
Power Consumption (Maximum)	360 Watts
IES4105M-DCA Electrical specifications	
Input Power	Voltage range: -36 to -72 V DC, nominal voltage is -48 V DC. There is no tolerance for the DC input voltage. Maximum input DC current: 10 A
Power Consumption (Maximum)	360 Watts
IES4105M-DU Electrical specifications	

Table 18 System Specifications (continued)

Input Power	Power switch: AC only AC input Voltage range: 100-240 V AC single phase Frequency range: 50/60Hz Maximum input AC current: 4 A DC input Voltage range: -36 to -72 V DC, nominal voltage is -48 V DC. There is no tolerance for the DC input voltage. Maximum input DC current: 10 A
Power Consumption (Maximum)	400 Watts
Environmental specifications	
Temperature	IES4105M-DU: -40°C to 55°C (Operating) Other line cards and power modules: -40°C to 65°C (Operating) All: -40°C to 70°C (Storage)
Humidity	5%-95% RH, non-condensing (Operating) 10%-90% RH, non-condensing (Storage)
Atmospheric pressure	86 kPa to 106 kPa (Operating and storage)

2.1 Management Card

Table 19 MSC1002GA Specifications

Physical specifications	
Dimensions	Height: 42 mm (1.7 inches) Width: 130 mm (5.1 inches) Depth: 239.8 mm (9.4 inches)
Physical interfaces	
Gigabit Ethernet	Two Gigabit Ethernet combo interfaces (SFP + RJ45)
Fast Ethernet	One 100/10 Mbps Fast Ethernet port with RJ-45 connector for out of band management
COM	One monitor port with male DB15 connector (RS-232) that can communicate with a UPS and sense up to four external contacts
Console	One console port with RJ-45 connector
Reset button	One recessed hardware reset button

2.2 ADSL2+ Line Card

Table 20 ALC1132A-51 Specifications

Physical specifications	
Dimensions	Height: 20.45 mm (0.8 inches)
	Width: 280 mm (11 inches)
	Depth: 236.8 mm (9.3 inches)
Physical interfaces	
POTS	One 32-line POTS port with Telco 64 connector
ADSL	One 32-line data and voice port with Telco 64 connector

2.3 VDSL2+ Line Card

Table 21 VLC1124A-51 Specifications

Physical specifications	
Dimensions	Height: 20.45 mm (0.8 inches)
	Width: 280 mm (11 inches)
	Depth: 236.8 mm (9.3 inches)
Physical interfaces	
POTS	One 24-line POTS port with Telco 64 connector
VDSL	One 24-line data and voice port with Telco 64 connector

2.4 VoIP Line Card

Table 22 VOP1164A-61 Specifications

Physical specifications	
Dimensions	Height: 20.45 mm (0.8 inches)
	Width: 280 mm (11 inches)
	Depth: 236.8 mm (9.3 inches)
Physical interfaces	
1-32, 33-64	Two 32-line POTS ports with Telco 64 connectors

2.5 Firmware Naming Conventions

A firmware version includes the model code and release number as shown in the following example.

H.248 Firmware Version: V3.60(ABIZ.0)

SIP Firmware Version: V3.60(ABJK.0)

"ABIZ" and "ABJK" are the model codes.

"0" is this firmware's release number. This varies as new firmware is released. Your firmware's release number may not match what is displayed in this User's Guide.

Note: ABIZ model code firmware uses H.248 for VoIP.

ABJK model code firmware uses SIP for VoIP.

H.248 configuration is available when the IES is using the H.248 firmware.

SIP configuration is available when the IES is using the SIP firmware.

CHAPTER 3

Hardware Installation and Connections

3.1 Overview

Installing the IES includes the following steps:

- [Section 3.2 "Installing the IES"](#)
- [Section 3.3 "Bonding the IES"](#)
- [Section 3.4 "Grounding Yourself"](#)
- [Section 3.5 "Installing the Cards"](#)
- [Section 3.6 "Connecting the MSC"](#)
- [Section 3.9 "Connecting Service Cables"](#)
- [Section 3.10 "Connecting to an MDF"](#)
- [Section 3.11 "Connecting the Power"](#)

3.2 Installing the IES

Perform the installation as follows:

Have qualified service personnel install the IES in a restricted access area, such as a street cabinet or data center.

- Make sure the IES's power switch is in the **OFF** position.
- Install the chassis as detailed in this chapter. Make sure you connect the frame grounds before you make any other connections.
- If line cards are not already installed, follow the procedure in the next section to install them.

Caution!

All installation methods must be in accordance with national and local regulations and practices.

3.2.1 Installing the IES in a Rack

Make sure the rack will safely support the combined weight of all the equipment it contains.

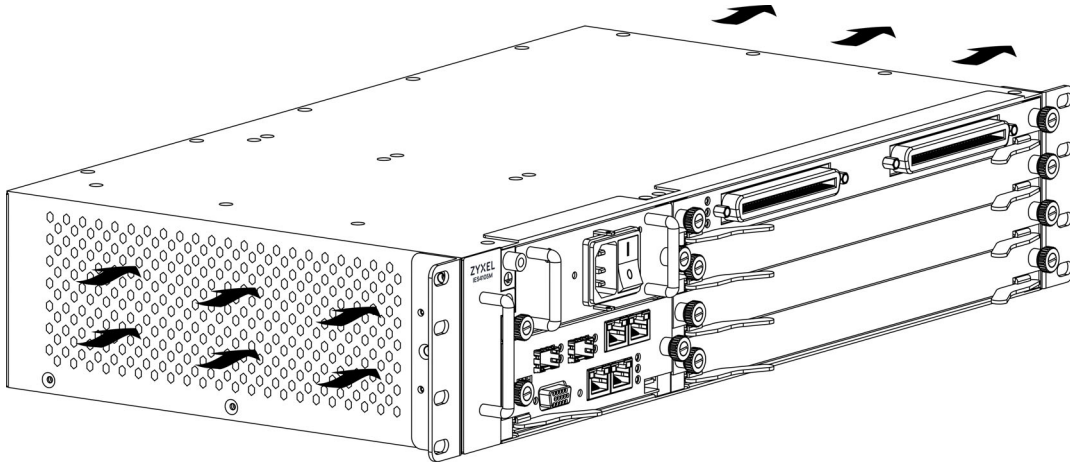
- Use a #2 Phillips screwdriver to install the screws.
- Refer to [Chapter 2 on page 33](#) for the dimensions, weights and power consumption.

Failure to use the proper screws may damage the unit.

Make sure that nothing obstructs the airflow.

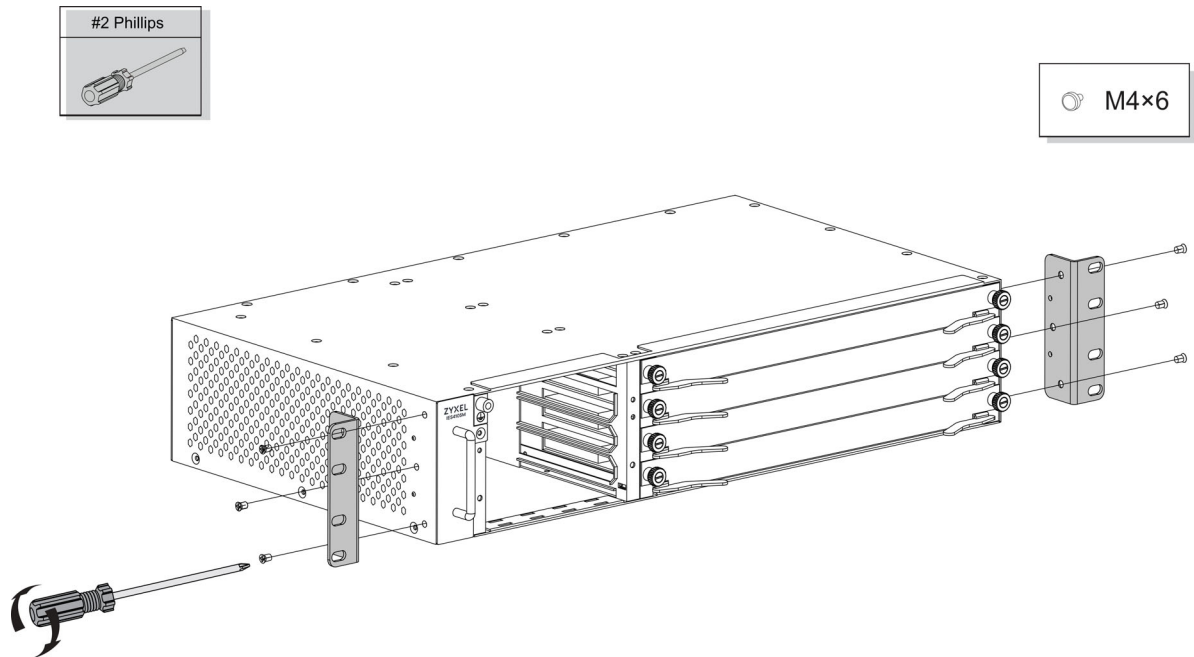
- If you are facing the front panel, the fan exhaust vents are located on the right side panel of the unit and the fans along with the intake vents are located on the left side panel.

Figure 13 Airflow

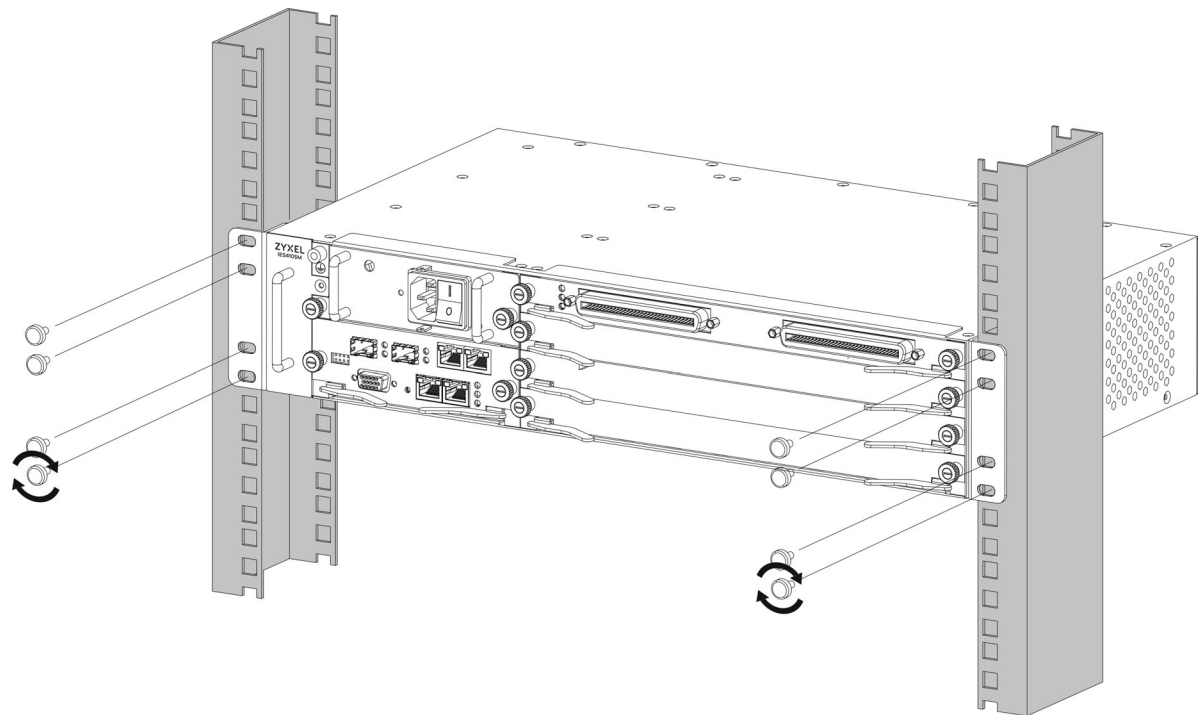


Use the following procedure to install the chassis in the rack.

- 1 Position a mounting bracket on one side of the chassis, making sure the screw holes on the bracket are on the same side as the front panel of the chassis.
- 2 Use the screwdriver to install the screws through the mounting bracket holes into the chassis.
- 3 Repeat steps 1-2 to attach the second mounting bracket on the other side of the chassis.

Figure 14 Attaching Mounting Brackets

- 4 Position a mounting bracket (that is already attached to the chassis) on one side of the rack, lining up the screw holes on the bracket with the screw holes on the side of the rack.
- 5 Use the screwdriver to install the screws through the mounting bracket holes into the rack.
- 6 Repeat steps 4-5 to attach the second mounting bracket on the other side of the rack.

Figure 15 Rack Mounting

3.3 Bonding the IES

Qualified service personnel must confirm that the protective earthing terminal of the building is a valid terminal.

Caution!

All installation methods must be in accordance with national and local regulations and practices.

Note: The IES is protected for overcurrent (short circuit) and overvoltage conditions.

Warning!

Use caution when handling live electrical connections. Do not install electrical equipment in wet or damp conditions. Do not allow anything to rest on the power cable, and do not place the cable where people can stand or walk on it. Verify that the IES is bonded before connecting power.

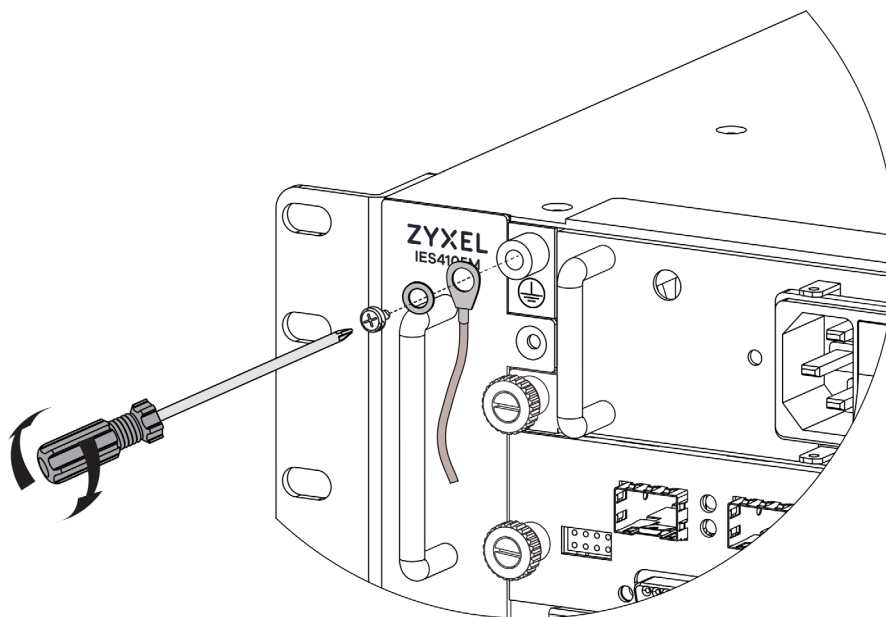
The unit is required to be bonded to a safety earth (ground) using a suitably rated cable:

- Cable gauge: see [Table 18 on page 33](#)
- Cable length: depends on the field environment. Use the shortest path to the ground.
- Type of cable terminal: gauge 4~4.5 mm recommended
- Type of cable: sleeved
- Cable color: green and yellow required by safety

The cable must be attached to the IES using an M4 machine screw with a suitable lock washer. The other end must be securely fastened to the chassis ground with a lug and screw arrangement of M3.5 or greater. An example is shown in [Figure 16 on page 41](#).

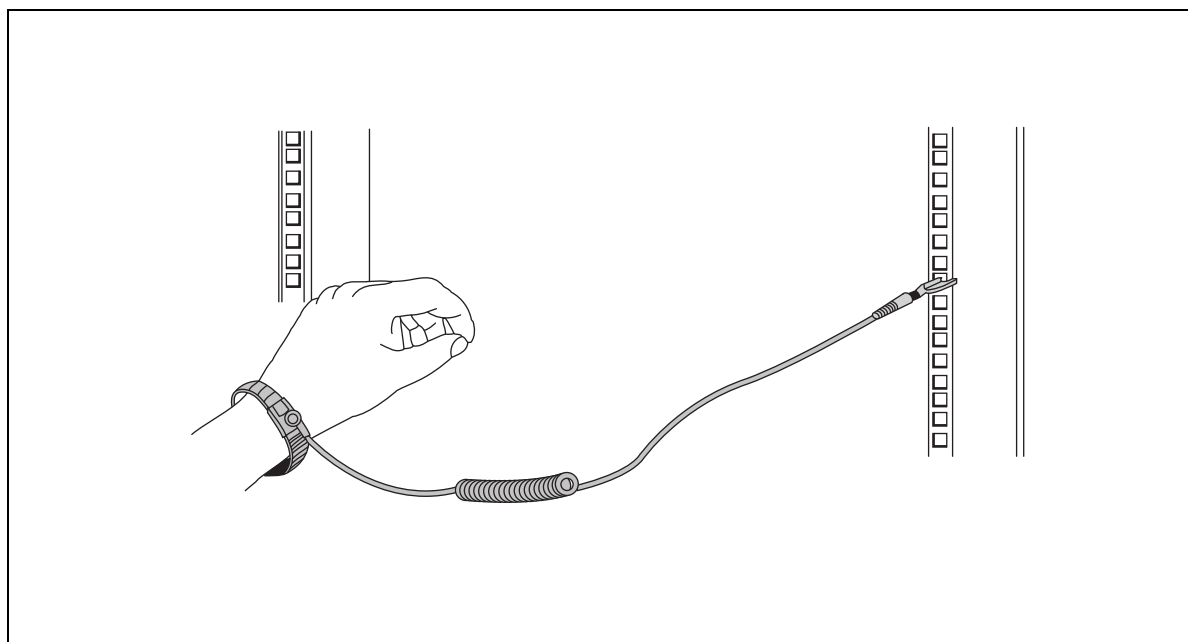
- The frame ground is on the upper left of the chassis front panel.
- Connect the frame ground to a building's protective earthing terminals using a green-and-yellow frame ground wire.

Warning! Bond the frame ground before you connect any other cables or wiring.

Figure 16 Bonding

3.4 Grounding Yourself

Ground yourself using an Electro-Static Discharge (ESD) wrist strap.



3.5 Installing the Cards

This section shows you how to install and remove cards.

- Install the management card in the slot on the left.
- Install the line cards in the chassis slots on the right.
- Leave the slot covers on unused slots.

3.5.1 Installing the Controller and Line Cards

Use the following procedure to install the management card and line cards in the chassis.

- 1 Grasp the center of the front panel of the card with one hand and place the other hand under the card to support it.
- 2 Insert the card halfway into the slot and spread the two ejector levers outward. Make sure the ejector levers are perpendicular to the front panel.
- 3 Slide the card into the slot until it makes contact with the backplane. The ejector levers should be at a small angle to the front panel now.
- 4 Push the two ejector levers firmly until they are flush with the front panel.
- 5 Tighten the two thumbscrews.

Figure 17 Installing a Card

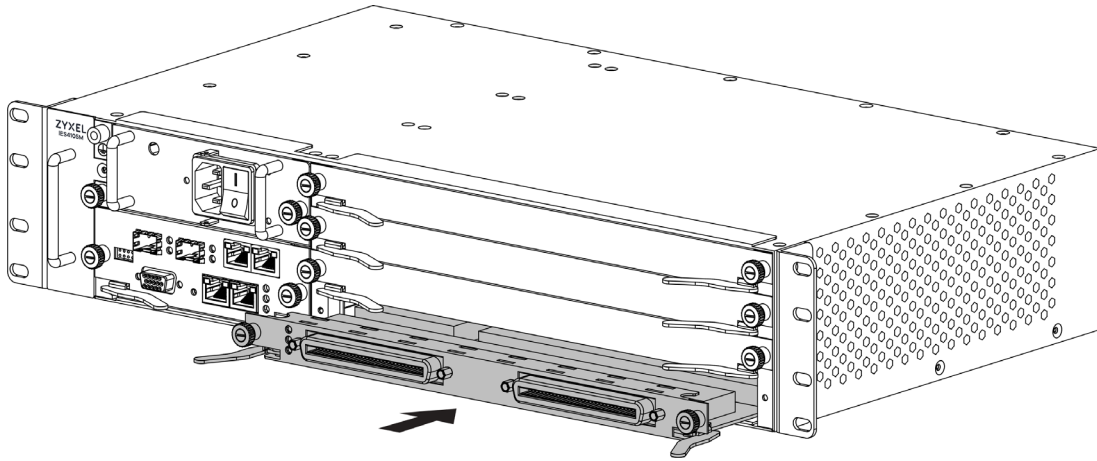
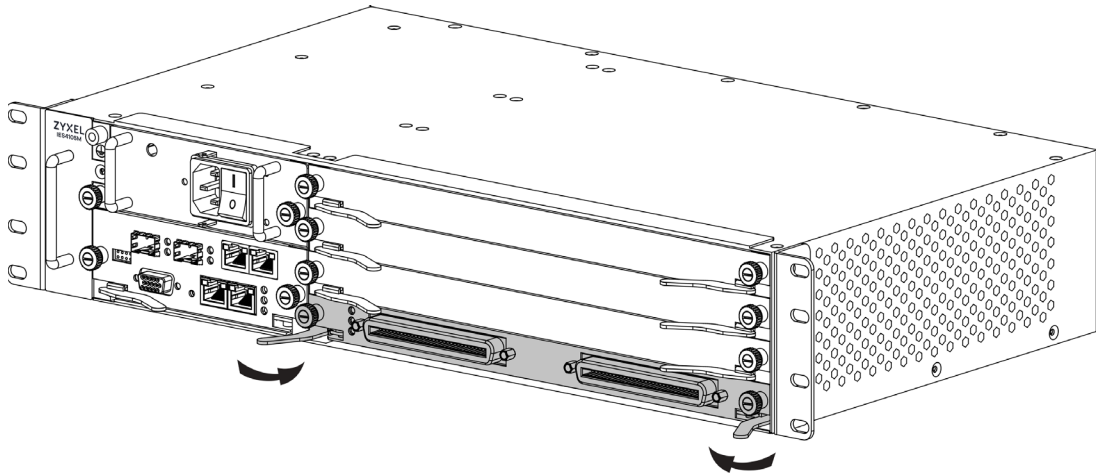
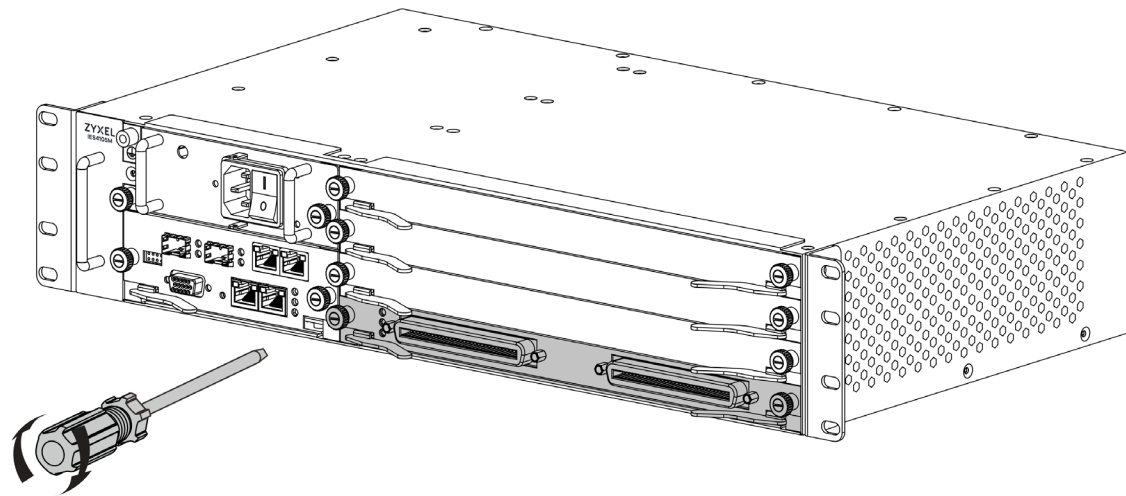


Figure 18 Closing the Ejector Levers**Figure 19** Tightening Card Thumbscrews

3.5.2 Removing Controller and Line Cards

Use the following procedure to remove the management card and line cards from the chassis.

Note: The management card provides power to the fan module. The fan stops rotating when you remove the management card.

- 1 Disconnect all cables from the card.
- 2 Loosen the two thumbscrews.
- 3 Pull the two ejector levers firmly until the front of the card is clear of the chassis. Pull the ejector levers until they are perpendicular to the front panel.

Note: The MSC has more connector pins than the other cards so when removing it you need to exert more force to get the front of the MSC clear of the chassis.

- 4 Grasp the center of the front panel of the card with one hand and place the other hand under the card to support it.
- 5 Slide the card out of the slot.

Figure 20 Loosening Card Thumbscrews

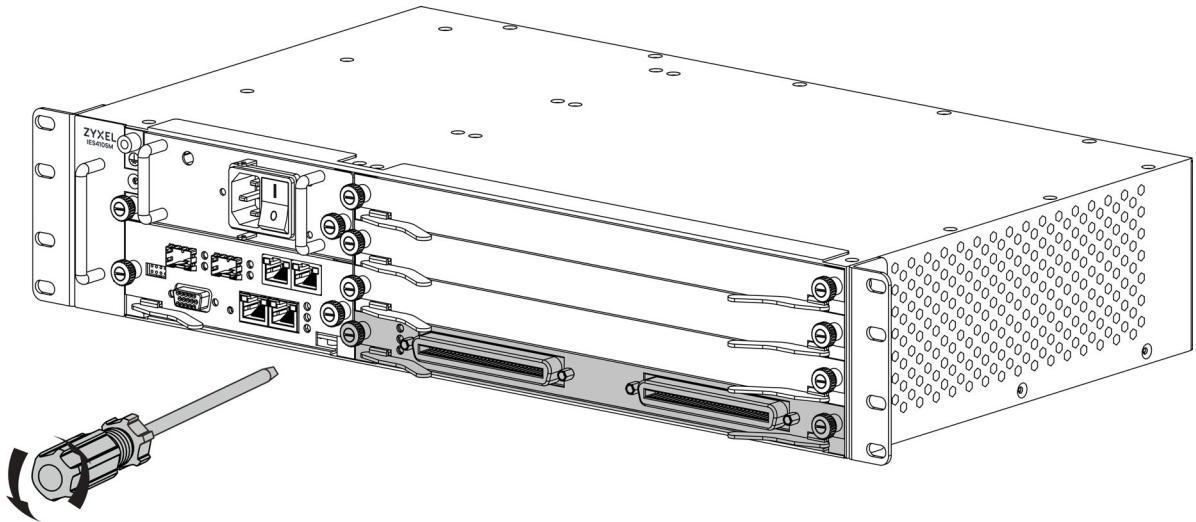


Figure 21 Opening the Ejector Levers

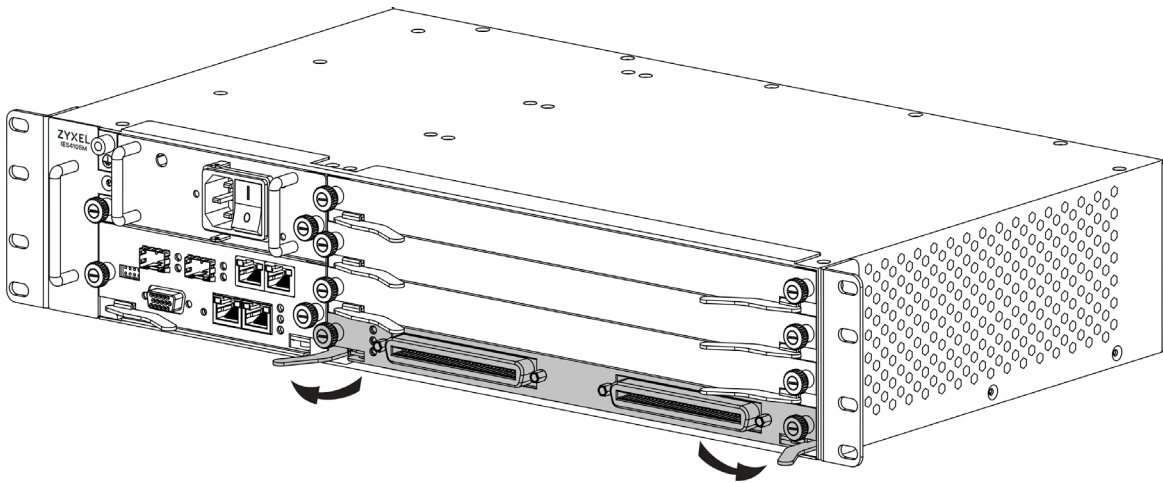
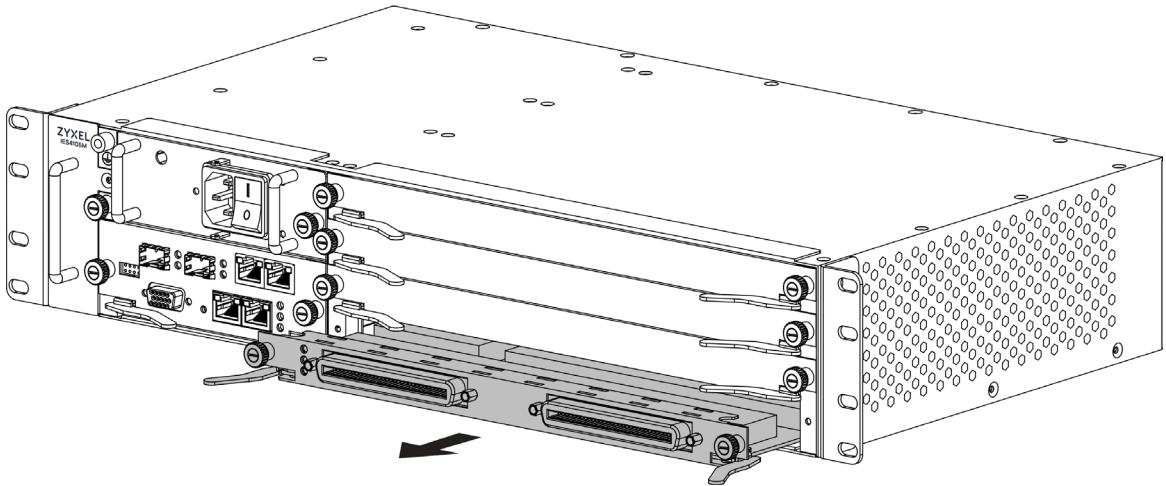


Figure 22 Removing a Chassis Card

3.6 Connecting the MSC

This table describes the ports on the MSC front panel.

Table 23 MSC Front Panel

LABEL	DESCRIPTION
O-1/E-1 O-2/E-2	These combo Gigabit Ethernet interfaces consist of SFP slot + RJ-45 port pairs for connecting to a Gigabit Ethernet device.
COM	This DB15F connector contains a UART interface and four alarm inputs. When you deploy the IES with a UPS (uninterruptible power supply) and the alarm input specified for battery saving is triggered, the IES turns off subscriber data traffic in order to support PSTN calls for as long as possible.
MGMT	This is an RJ-45 Ethernet port for connecting to an Ethernet network for out-of-band management (a separate channel for management that is not part of the channels that are usually used for data transfer).
CONSOLE	This RJ-45 RS-232 port is for connecting to a computer for local management.

3.6.1 Connecting the COM Connector

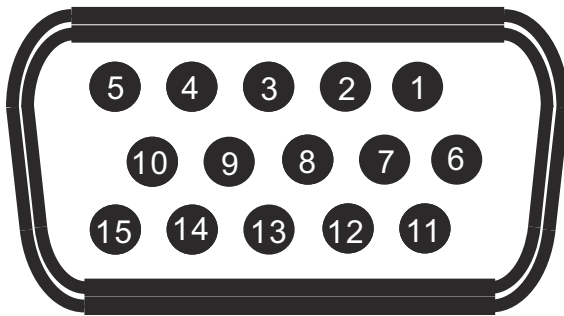
Figure 23 COM Connector Pin Layout

Table 24 COM Connector Pin Layout

PIN NO.,	SIGNAL	DIRECTION	FUNCTION	NOTE
2	RxD	Input	Data receive	These pins are for the UART interface.
3	TxD	Output	Data transmit	
5	GND		Ground	
9, 10	Loop 1#	N/A	Alarm current loop.	These pins are for monitoring.
12, 13	Loop 2#	N/A	Alarm current loop.	
14, 15	Loop 3#	N/A	Alarm current loop.	
6, 11	Loop 4#	N/A	Alarm current loop.	
1			Not connected	
4		Output	Reserved	
7		Output	Reserved	
8		Input	Reserved	

3.6.2 Connecting the Gigabit Ethernet Interfaces

The management card has two Gigabit Ethernet combo interfaces (SFP + RJ45).

The mini-GBIC slots are for fiber optic SFP transceivers that support Gigabit Ethernet connections. The SFP slots have priority over the RJ-45 Gigabit Ethernet ports. This means that if a SFP transceiver and the corresponding Gigabit port are connected at the same time, the Gigabit port will be disabled.

A transceiver is a single unit that houses a transmitter and a receiver. The transceivers are not included.

You can change transceivers while the IES is operating.

The following SFP transceivers have been tested and approved for use with the management card.

Table 25 Supported SFP Transceivers

SPEED	MODEL	PN	DESCRIPTION
Gigabit (with DDML)	SFP-SX-DS	SFP-SX-DS-ZZ01V1F	GbE SFP SX Multi-Mode 550 m (1804 ft) commercial type transceiver, DDML version
	SFP-LX-5DS	SFP-LX-5DS-ZZ01V1F	GbE SFP LX 5 km (5468 yd) commercial type transceiver, DDML version
	SFP-LX-15DS	SFP-LX-15DS-ZZ01V1F	GbE SFP LX 15~20 km (16404~21872 yd) commercial type transceiver, DDML version
	SFP-BXA-20DS	SFP-BXA-20DS-ZZ01V1F	GbE SFP BX 20km (21872 yd) Bidirectional Type-A 1310~1550Tx, DDML version
	SFP-BXB-20DS	SFP-BXB-20DS-ZZ01V1F	GbE SFP BX 20km (21872 yd) Bidirectional Type-B 1550~1310Tx, DDML version
	SFP-BXC-20DS	SFP-BXC-20DS-ZZ01V1F	GbE SFP BX 20km (21872 yd) Bidirectional Type-C 1310~1490Tx, DDML version
	SFP-BXD-20DS	SFP-BXD-20DS-ZZ01V1F	GbE SFP BX 20km (21872 yd) Bidirectional Type-D 1490~1310Tx, DDML version
	SFP-LHX-40DS	SFP-LHX-40DS-ZZ01V1F	GbE SFP LHX wavelength=1310, 40 km (43744 yd) commercial type transceiver, DDML version
	SFP-ZX-80DS	SFP-ZX-80DS-ZZ01V1F	GbE SFP ZX wavelength=1550, 80 km (87488 yd) commercial type transceiver, DDML version

The RJ-45 Gigabit Ethernet ports are auto-negotiating and can detect and adjust to the optimum Ethernet speed (100/1000 Mbps) and duplex mode (full duplex or half duplex) of the connected device. The Ethernet ports are also auto-crossover (auto-MDI/MDI-X), they automatically work with a straight-through or crossover Ethernet cable.

3.7 Installing a Transceiver

Use the following steps to install a mini GBIC transceiver (SFP module) in a slot.

Make sure the SFP transceiver conforms to the following:

CLASS 1 LASER PRODUCT

APPAREIL À LASER DE CLASS 1

PRODUCT COMPLIES WITH 21 CFR 1040.10 AND 1040.11.

PRODUIT CONFORME SELON 21 CFR 1040.10 ET 1040.11.

To avoid possible eye injury, do not look into an operating fiber-optic module's connectors.

- 1 Remove the dust cover from the transceiver.
- 2 For transceivers with a flip-up or flip-down latch, close the latch.
- 3 Insert the fiber-optic cables into the transceiver (you may need to remove cable dust covers).
- 4 Insert the transceiver into the slot with the exposed section of PCB board facing down.
- 5 Press the transceiver firmly until it clicks into place.

Figure 24 Gigabit Ethernet Transceiver Installation

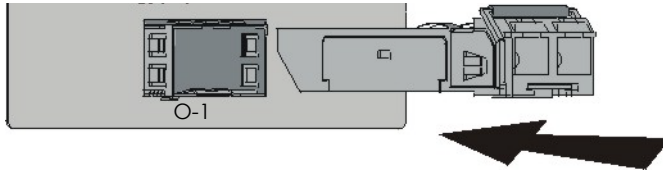
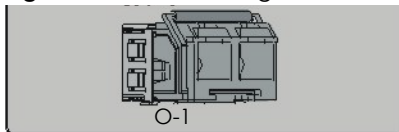


Figure 25 Installed Gigabit Ethernet Transceiver



3.8 Removing a Transceiver

Use the following steps to remove a mini GBIC transceiver (SFP module) from the slot.

- 1 Remove the fiber-optic cables from the transceiver.

- 2 Unlock the transceiver's latch (latch styles vary).
- 3 Pull the transceiver out of the slot.
- 4 Put the transceiver's dust cover on the transceiver.

Figure 26 Opening the Gigabit Ethernet Transceiver Latch

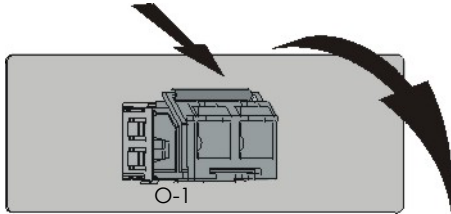
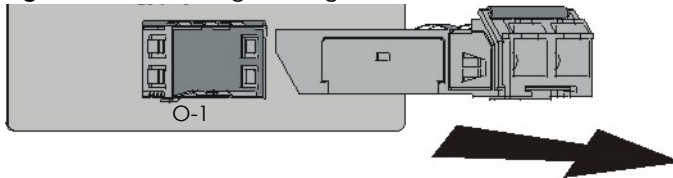


Figure 27 Removing the Gigabit Ethernet Transceiver

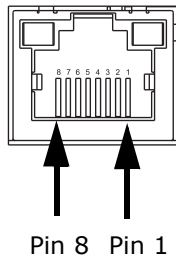


3.8.1 Connecting the Console Port

The **CONSOLE** port is a female RJ-45 serial port used for local management of the IES.

The following figure describes the **CONSOLE** port pin layout.

Figure 28 CONSOLE Port Connector Pins



The following table describes the pinout and signals.

Table 26 CONSOLE Connector Pin Layout

PIN NO.	SIGNAL	DIRECTION	FUNCTION
4	GND		Ground
5	RxD	Input	Data Receive for Network Processor
6	TxD	Output	Data Transmit for Network Processor
3		Input	Reserved
7		Output	Reserved
1-2, 8			Not connected

3.8.2 Connecting the MGMT Port

Use an Ethernet LAN cable (RJ-45 connectors) to connect a computer for out of band management to the **MGMT** port.

3.9 Connecting Service Cables

Connect Telco 64 cables to a line card's front panel Telco 64 connectors.

Telco 64 cables are used for data and voice applications with MDFs (Main Distribution Frame), patch panels and distribution boxes. They can also be used as extension cables. Telco 64 cables are made up of 32 twisted-pair copper wires.

Use No. 26 AWG or larger telephone wire.

Connect a Telco 64 connector to one end of the cable. Follow the pin assignments shown in [Chapter 1 on page 20](#) to wire Telco 64 cables to Telco 64 connectors. Use a screw and a cable tie to secure the Telco 64 connector to the front of the line card. Connect the other end of the cable directly to an MDF. Alternatively, attach RJ-11 connectors and connect directly to DSL modems or telephones.

Figure 29 Securing the Telco 64 Cable with a Screw

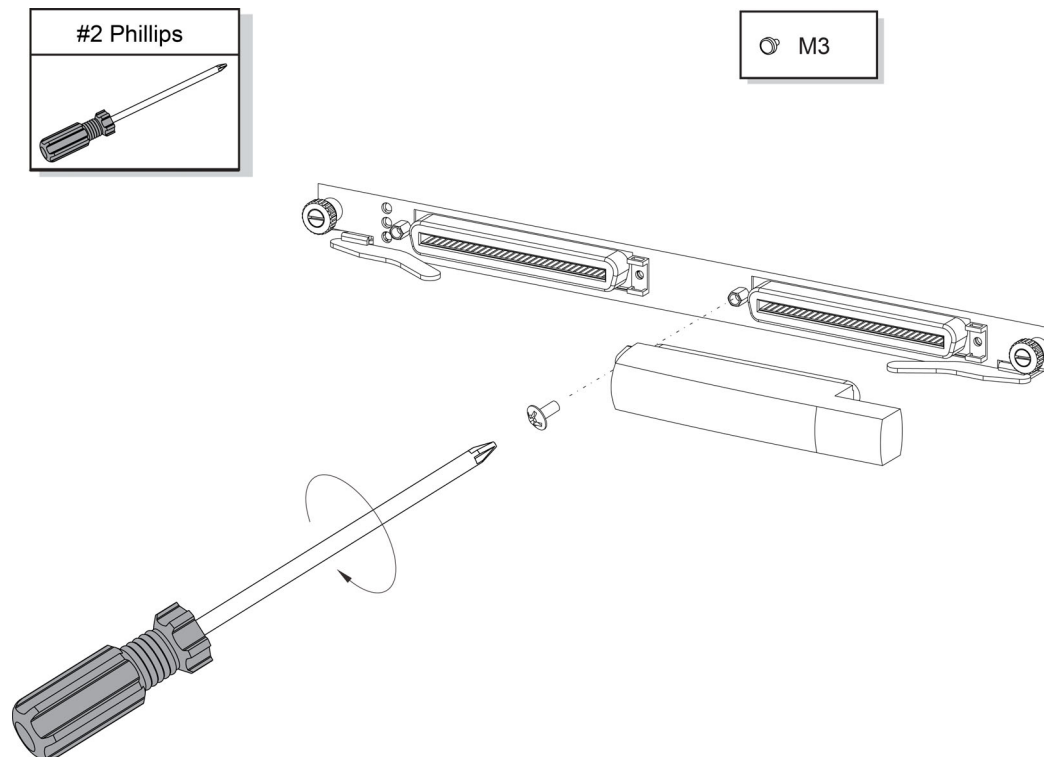
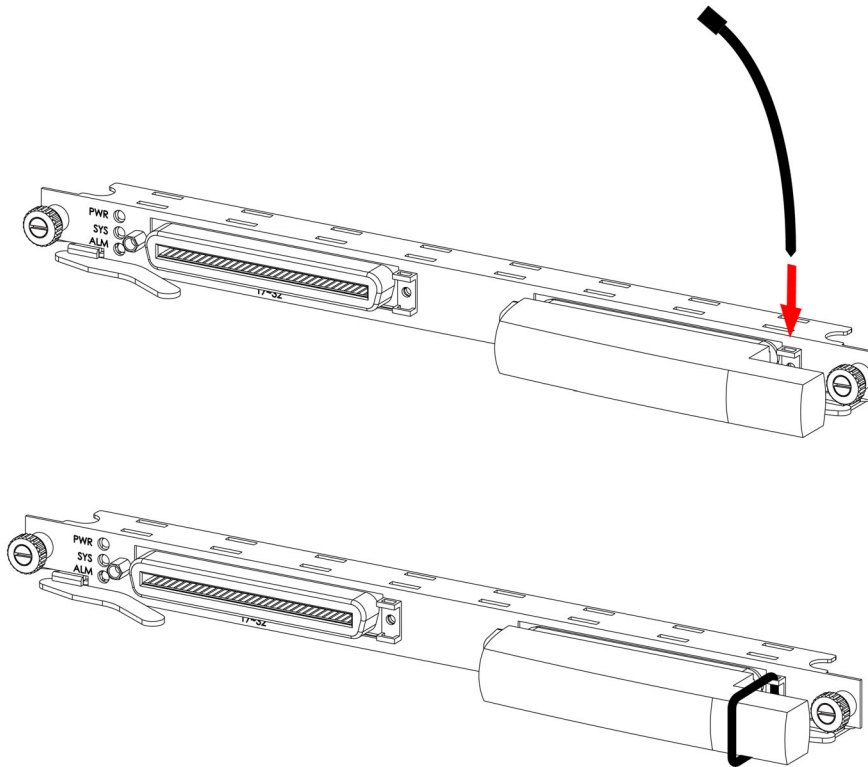


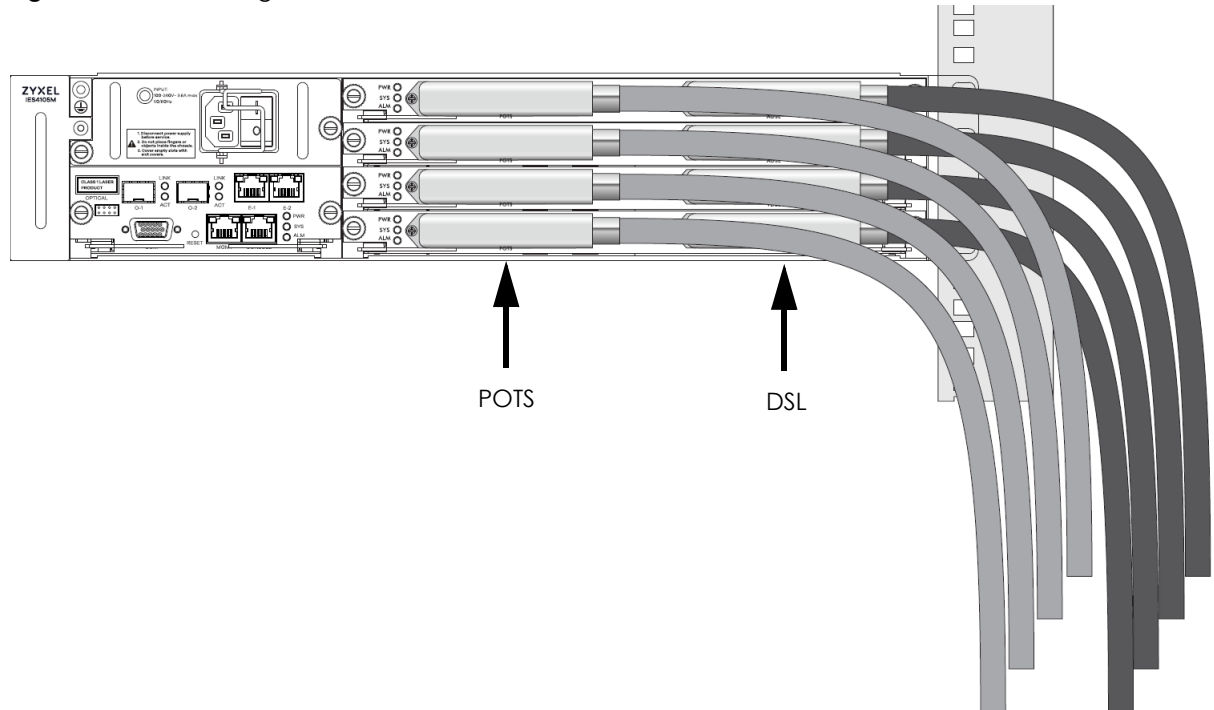
Figure 30 Securing the Telco 64 Cable with a Cable Tie

3.9.1 Connecting DSL Cards

A DSL card separates the voice signal from the DSL signal. It feeds the DSL signals to the DSL line card and diverts the voice signal to the **POTS** Telco 64 connector.

Connect the **POTS** Telco 64 connectors to the PSTN switch or a VoIP line card.

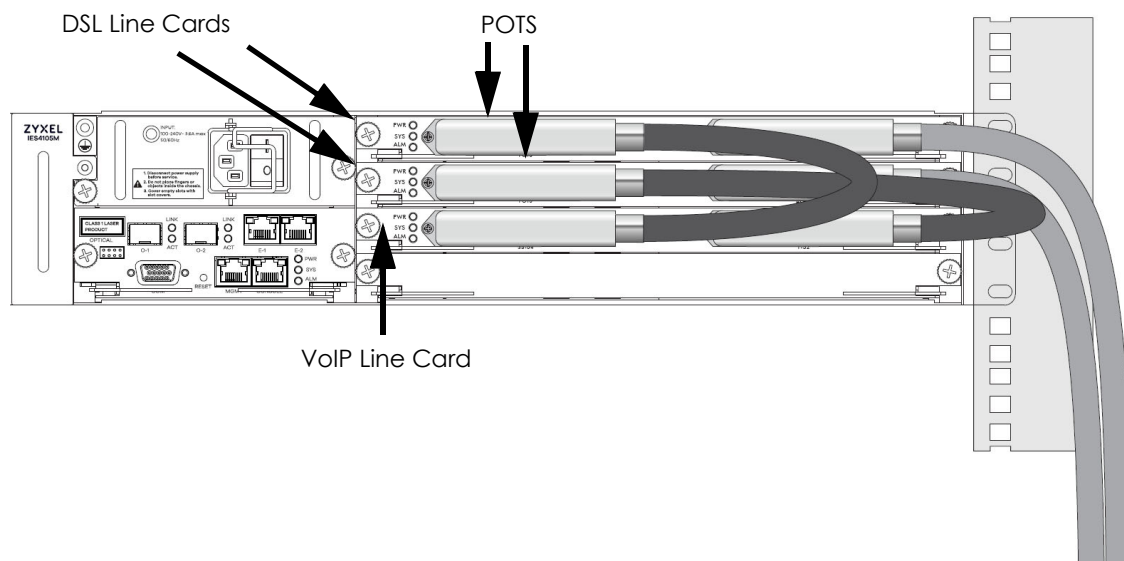
Connect the **DSL** Telco 64 connectors to the subscribers' telephone wiring. In most multi-tenant unit applications, the **DSL** pins connect to the subscribers' telephone wiring via Main Distribution Frame (MDF).

Figure 31 Connecting DSL Cards

3.9.2 Connecting VoIP Line Cards

When using the VoIP line card in conjunction with an ADSL or VDSL card, connect the VoIP line card's Telco 64 connectors to the DSL line card's **POTS** Telco 64 connectors.

For subscribers not using DSL, connect the VoIP line card's Telco 64 connectors to the subscribers' telephone wiring. In most multi-tenant unit applications this connection is through a Main Distribution Frame (MDF).

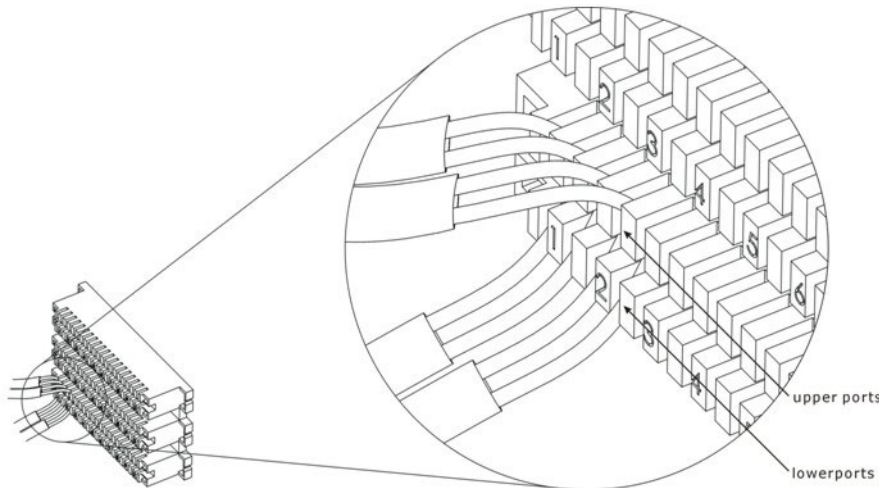
Figure 32 Connecting VoIP Cards

3.10 Connecting to an MDF

This section shows you how to connect the line cards to a Main Distribution Frame (MDF). Follow the pin assignments shown in [Chapter 1 on page 20](#) to wire Telco 64 cables to Telco 64 connectors.

An MDF is usually installed between subscribers' equipment and the telephone company (CO) in a basement or telephone room. The MDF is the point of termination for the outside telephone company lines coming into a building and the telephone wiring in the building.

Figure 33 MDF (Main Distribution Frame) Wiring



- Connect wiring to end-user equipment to the lower ports of an MDF and connect wiring from the telephone company to the upper ports of an MDF (see the previous figure).
- Some MDFs have surge protection circuitry built in between the two banks; thus, do not connect telephone wires from the telephone company directly to your IES.
- Use a punch-down tool to seat telephone lines into MDF blocks.

3.11 Connecting the Power

The chassis uses a power module that supplies power to the line cards. The power connections are on the front of the power module. Install the power module in the upper left of the chassis front panel.

Use the following procedures to connect the IES to a power source after you have installed the chassis in a rack and made the other connections.

Refer to Table 18 on page 33 for power requirements and make sure you are using an appropriate power source.

Keep the power source turned off until you come to the procedure for powering the IES.

The AC/DC dual power module can be connected to both 100-240 V AC/50-60 Hz line power and -48 V DC line power at the same time and operate on whichever is available. If both are available, the IES operates on the AC power and switches to DC power if the AC power is lost.

Caution!

Use caution when handling live electrical connections. Verify the IES is bonded before connecting power.

3.11.1 Procedure to Connect the AC Power

The IES AC power module is powered by 100-240 V AC/50-60 Hz line power. Power is input from a power outlet via an AC power cord. The AC power module is shown here. The procedure for connecting the AC power to the AC/DC dual power module is the same.

- 1 Slide the power module into the IES.
- 2 Tighten the two thumbscrews.
- 3 Connect the female end of the included power cord to the IES's power socket.
- 4 Move the power cord fixture so it holds the power cord in place to avoid unintentional removal.
- 5 Connect the male end of the cord to a power outlet.

Figure 34 Installing the AC Power Module

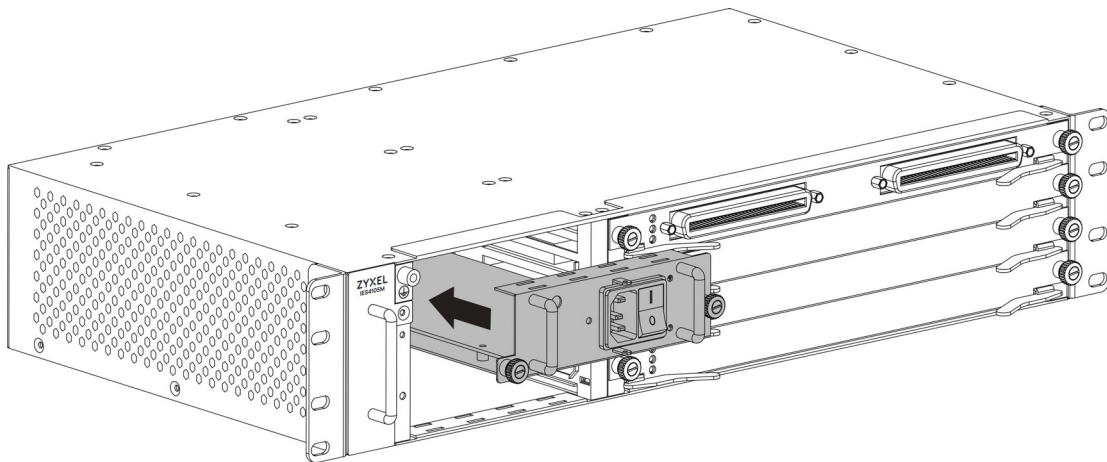


Figure 35 Tightening Power Module Thumbscrews

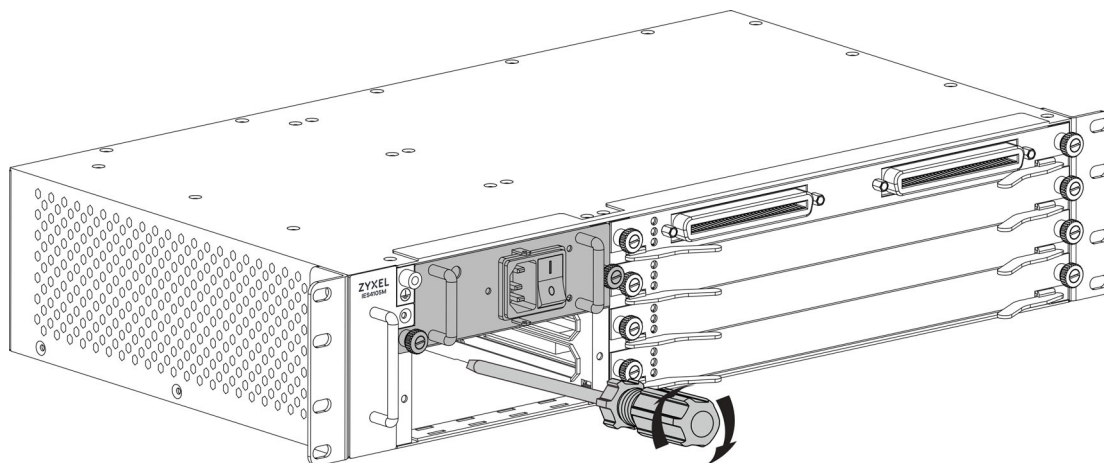


Figure 36 Connecting the AC Power Cord

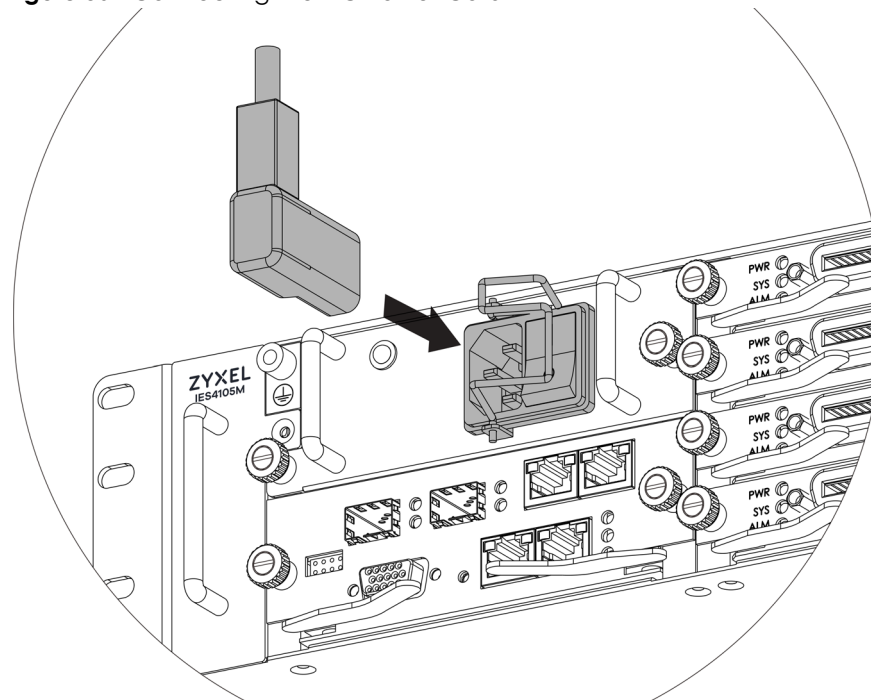
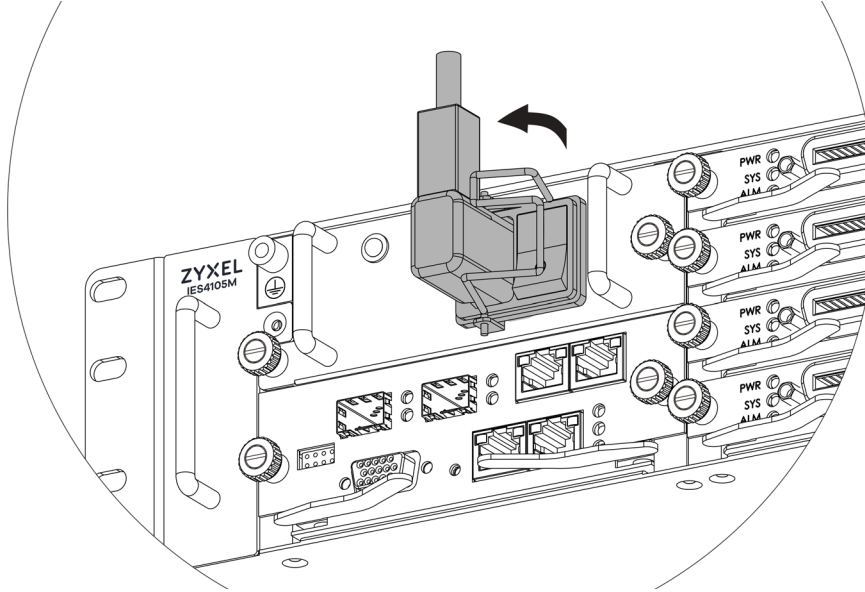


Figure 37 Fixing the AC Power Cord

3.11.2 Procedure to Connect the DC Power

The IES DC power module is powered by -36 to -72 V DC line power.

There is no tolerance for the DC input voltage

When installing the IES power wires, push the wires firmly into the terminals as deep as possible and make sure that no exposed (bare) wires can be seen or touched.

The DC power has two inputs. Use two wires of the gauge specified in [Table 18 on page 33](#) to connect each input. It is recommended to connect input 1 to the regular DC power source and connect input 2 to a backup DC power source such as a battery. The terminals on the left are input 1. The terminals on the right are input 2.

- 1 Turn off the power supplies.
- 2 Remove the green power connector block from the front of the power module.
- 3 Connect power wires to the RTN power terminals on the power connector block and tighten the terminal screws.
- 4 Connect power wires to the -48V power terminals on the power connector block and tighten the terminal screws.
- 5 Connect the other end of the RTN power wires to the positive terminals on the power supplies.
- 6 Connect the other end of the -48V power wires to the negative terminals on the power supplies.
- 7 Push the power connector block back into the front of the power module.

Figure 38 DC Power Terminals

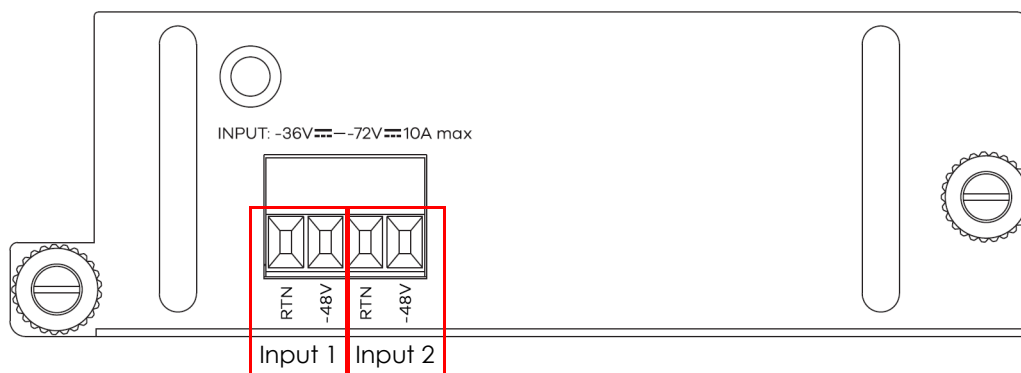


Figure 39 Remove the Power Connector Block

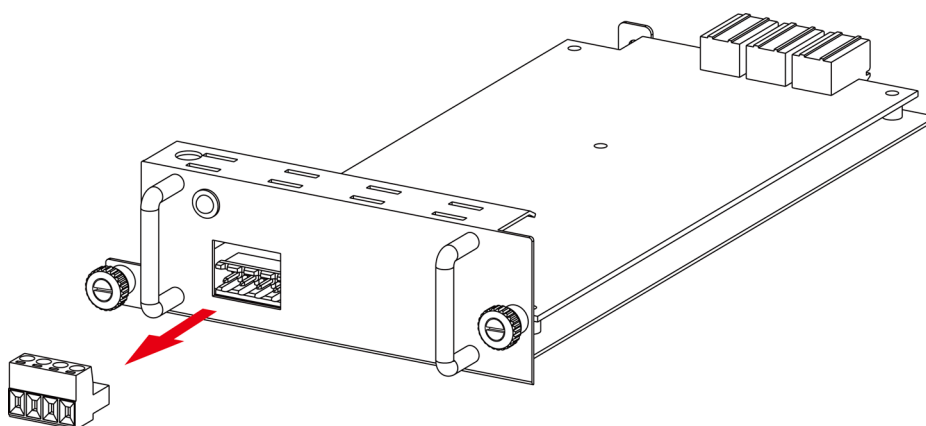


Figure 40 Connect the Power Wires

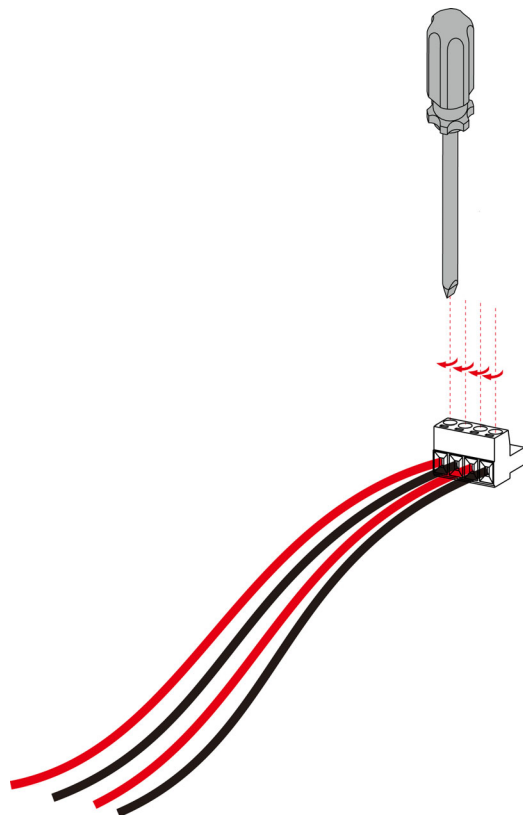
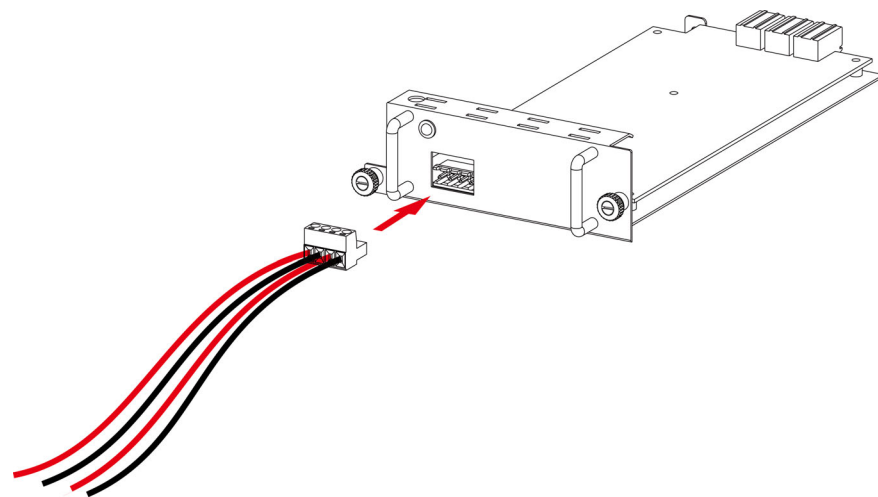


Figure 41 Insert the Power Connector Block



3.11.3 Powering the IES

- 1 Turn on the power source.
- 2 When using AC power, push the IES power switch to the on position.

CHAPTER 4

Maintenance

This chapter describes how to perform maintenance on the system hardware.

4.1 Fan Maintenance

This section describes how to change a fan module on the IES.

4.1.1 Procedure to Remove and Install the Fan Module

The chassis has a hot-swappable fan module. The fan module is at the left on the front panel. Replace the entire fan module if cleaning the fan filter does not solve the problem. Return any malfunctioning fan modules to the manufacturer.

Perform the following procedure to remove the fan module in order to clean the fan filter or change the fan module.

Warning! Removing the fan module causes the system to shut down after two minutes.

- 1 Loosen the screw on the front of the fan module.
- 2 Slide out the fan module.
- 3 Slide out the fan filter. Clean or replace the filter.
- 4 Slide the fan filter back into the fan module.
- 5 Slide the fan module back into the fan module slot (or use a different fan module from the manufacturer).
- 6 Tighten the screw.

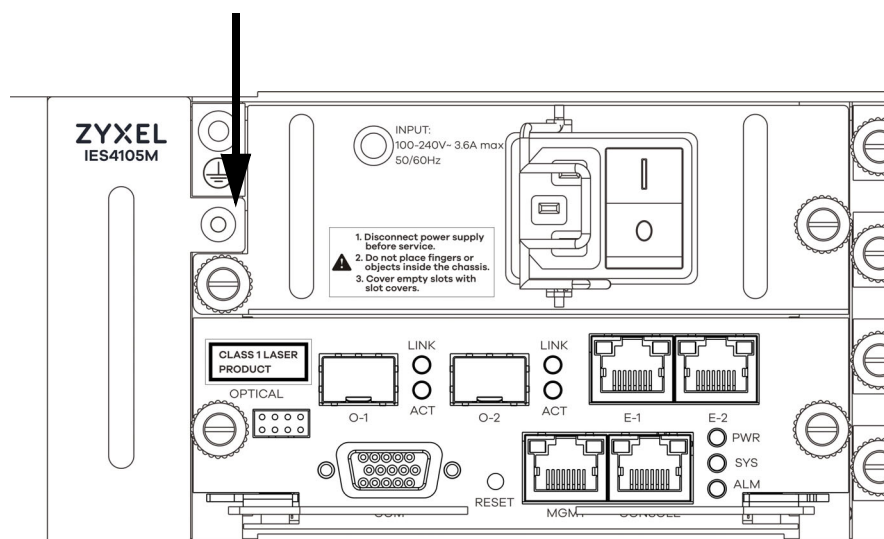
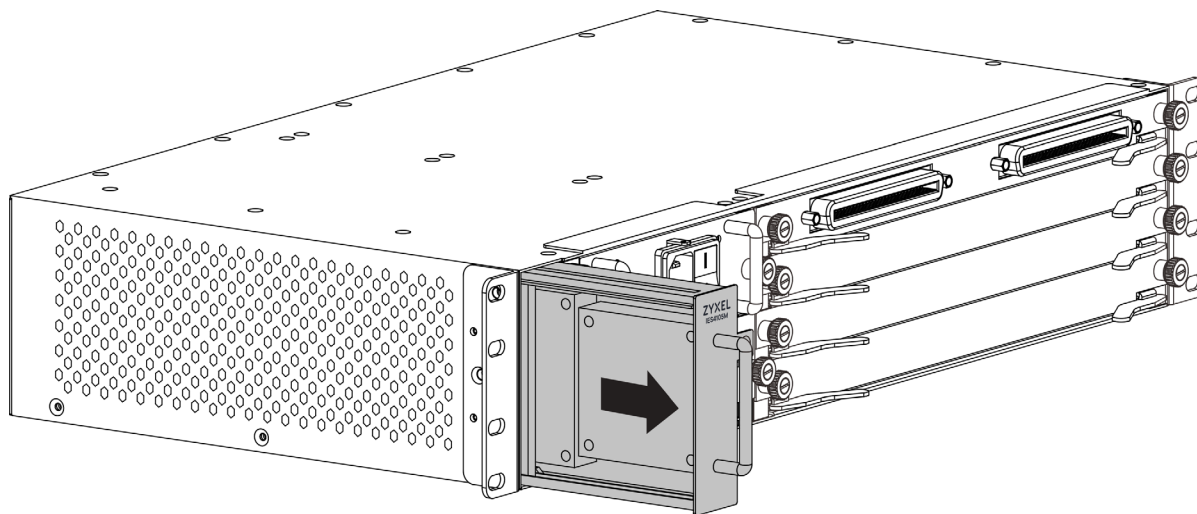
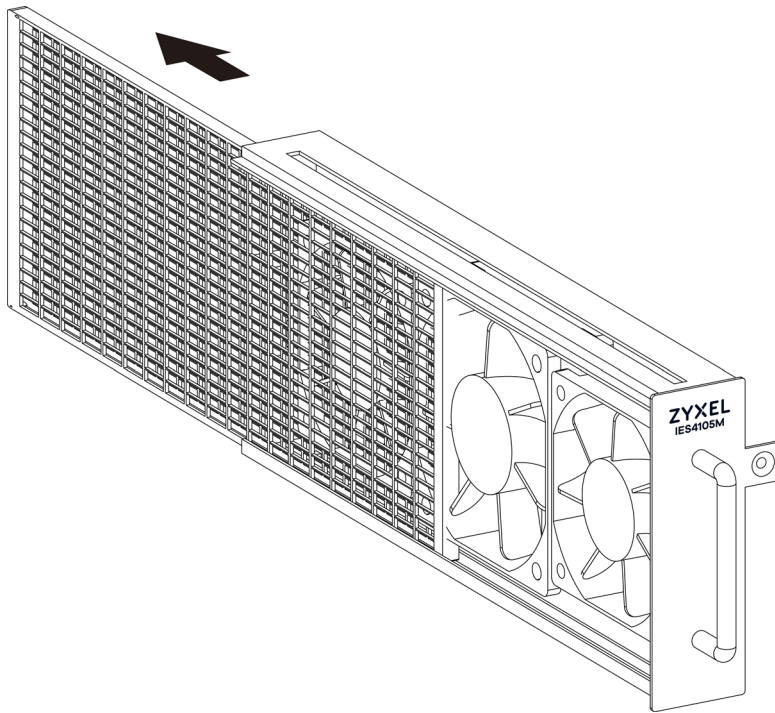
Figure 42 Loosen the Fan Module Screw**Figure 43** Remove the Fan Module

Figure 44 Remove the Filter

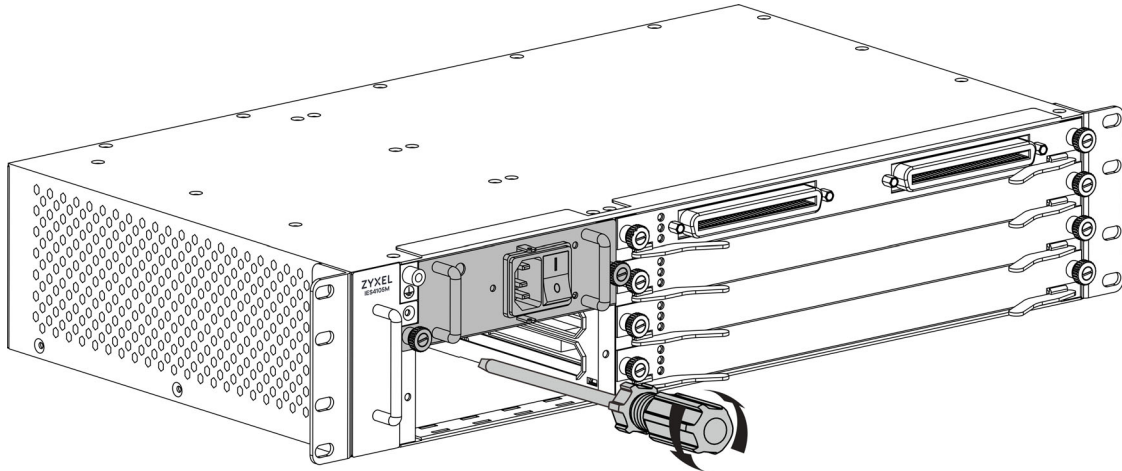
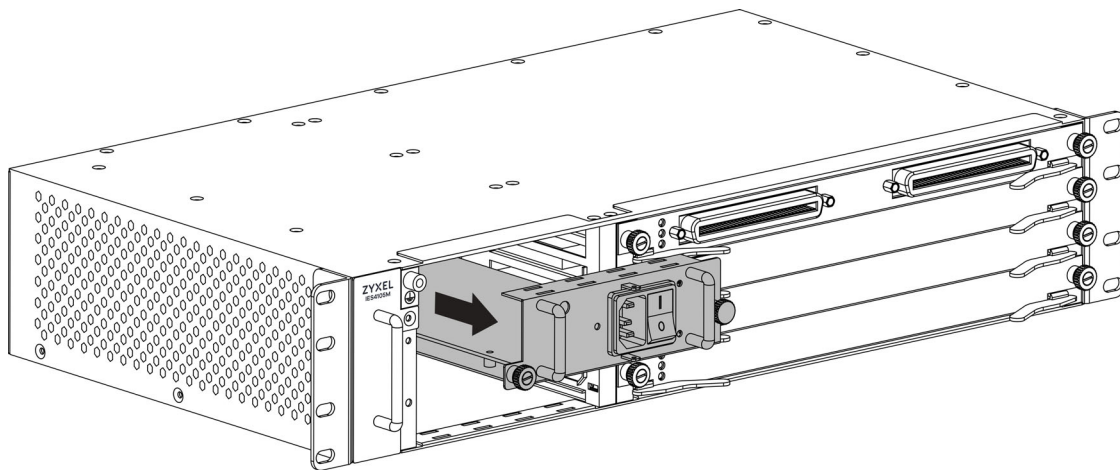
4.2 Power Maintenance

This section describes how to change the power module. The power module is at the upper left of the front panel of the chassis.

4.2.1 Procedure to Change an AC Power Module

The AC power module has a built-in circuit breaker. Before you replace a power module, make sure the circuit breaker is not causing the problem. Use the following procedure to change an AC power module.

- 1 Make sure that the power module has the power switch in the **OFF** position.
- 2 Turn off the power supply.
- 3 Disconnect the power cord from the power source and the power module.
- 4 Use a screw driver to loosen the thumbscrews on the front panel of the IES power supply module.
- 5 Grab the handle, and slide out the power supply module.
- 6 Replace the IES power module with a new one from the manufacturer.
- 7 Tighten the thumbscrews.
- 8 Refer to [Section 3.11.1 on page 53](#) to reconnect the power after you finish.

Figure 45 Loosening AC Power Module Thumbscrews**Figure 46** Sliding Out the AC Power Module

4.2.2 Procedure to Change a DC Power Module

Use the following procedure to change a DC power module.

- 1 Turn off the power supplies.
- 2 Loosen the power module thumbscrews and remove the power module from the IES.
- 3 Remove the green power connector block from the front of the power module.
- 4 Push the power connector block into the front of the new power module.
- 5 Slide the new power module into the IES and tighten the power module thumbscrews.
- 6 Turn on the power source.

Figure 47 Loosen the DC Power Module Thumbscrews

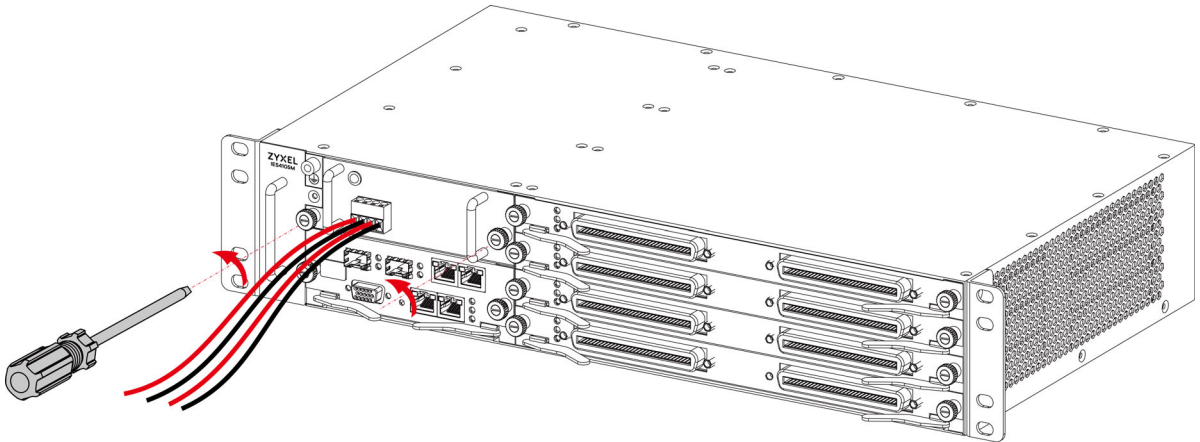


Figure 48 Slide Out the DC Power Module

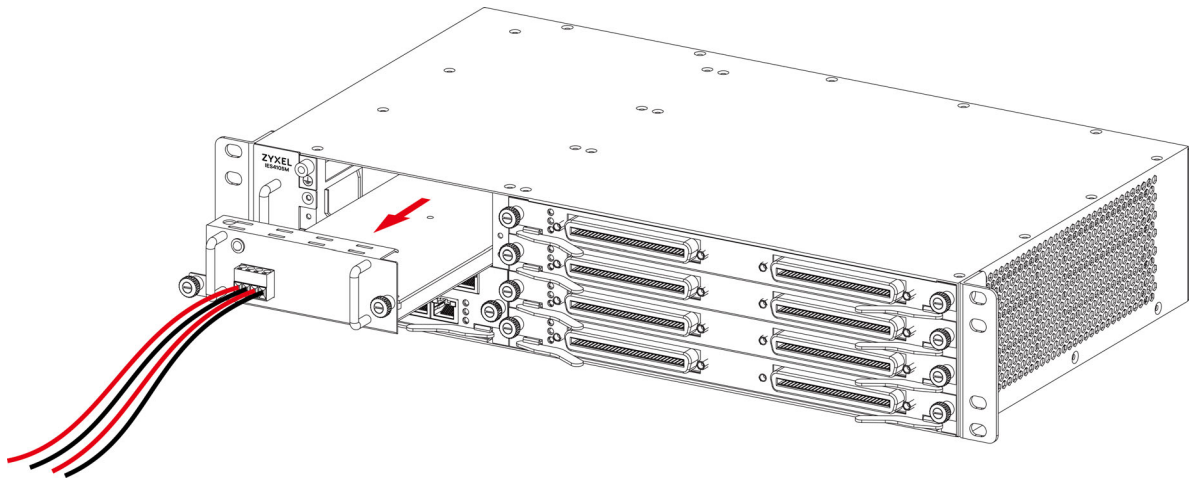


Figure 49 Remove the Power Connector Block

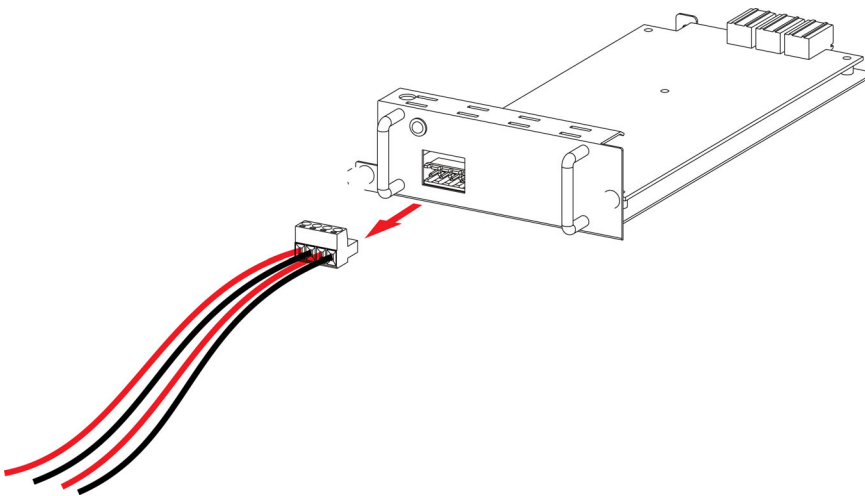


Figure 50 Insert the Power Connector Block in the New Power Module

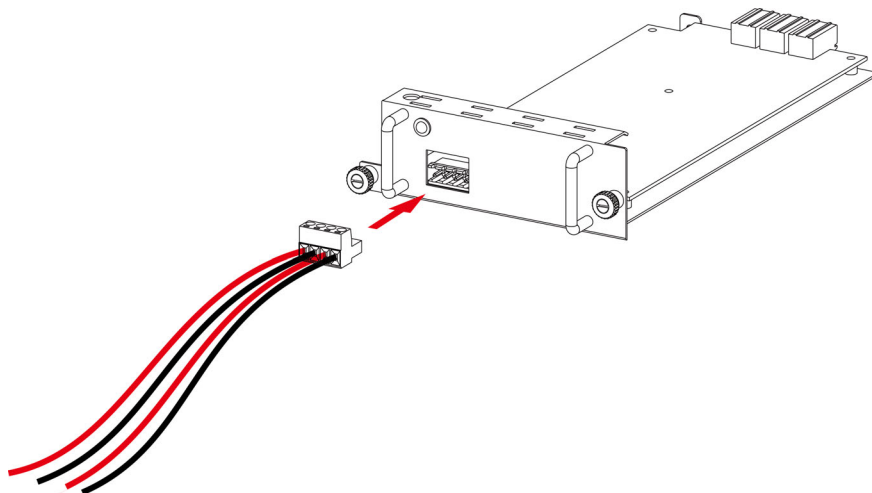


Figure 51 Slide in the New DC Power Module

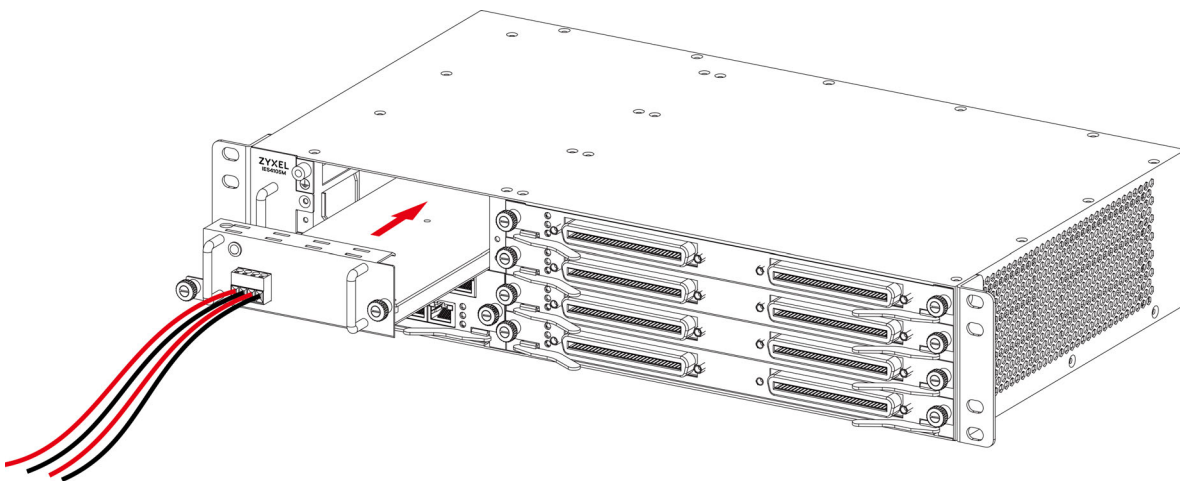
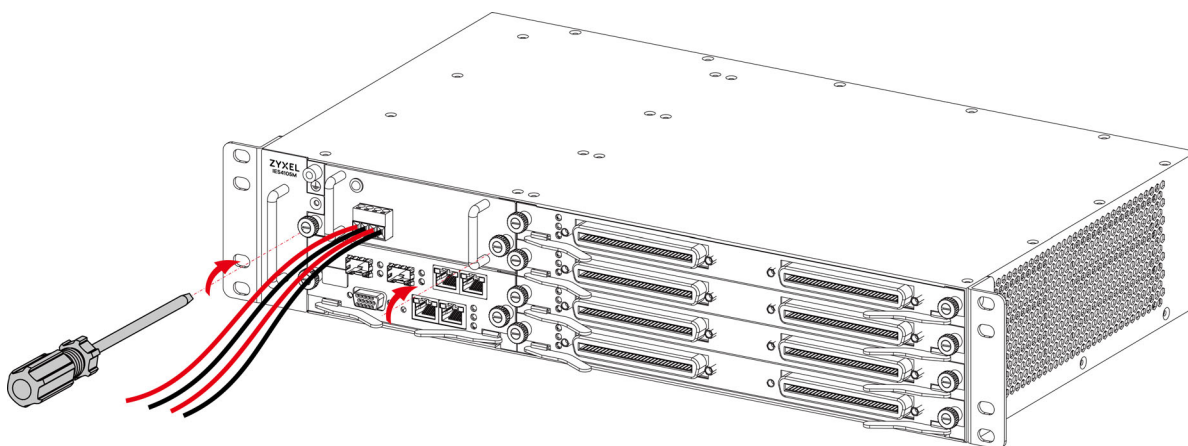


Figure 52 Tighten the DC Power Module Thumbscrews



PART II

Web Configurator

CHAPTER 5

The Web Configurator

This section introduces the configuration and functions of the Web Configurator.

5.1 Web Configurator Introduction

The Web Configurator is an HTML-based management interface that allows easy system setup and management via Internet browser. Use a browser that supports HTML5, such as Internet Explorer 9.0 and later versions, Mozilla Firefox 21 and later versions, Safari 6.0 and later versions or Google Chrome 26.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

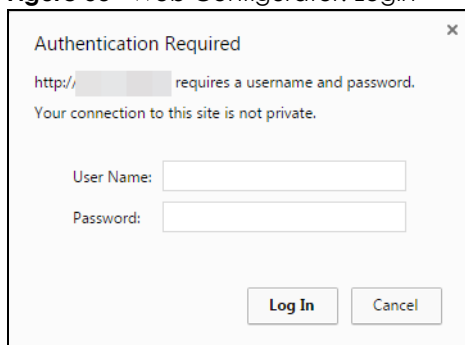
In order to use the Web Configurator you need to allow:

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

5.2 System Login

- 1 Start your web browser.
- 2 Type "http://" and the IP address of the IES in the **Location** or **Address** field. Press [ENTER]. 192.168.1.1 is the default in-band management IP address and 192.168.0.1 is the default out-of-band (management port) IP address.
- 3 The login screen appears. The default username is **admin** and associated default password is **1234**.

Figure 53 Web Configurator: Login



- 4 The **System Info (Home)** screen displays.

Figure 54 System Info (Home) Screen

Zyxel Enable Home Logout

MENU

- ACL
- Alarm
- Diagnostic
- Line Card
- Maintenance
- Multicast
- Port
- Profile
- Statistics
- Switch
- Sys
- VLAN
- VoIP
- Config Save

System Info

Current Alarm

Critical Alarms: 0 Major Alarms: 0 Minor Alarms: 0 Warning Alarms: 0

ID	State	Card Type	Provision Type	Uptime	Heat	Vol	Mon
1	Active	MSC1002GA	-	01:30:28	-	-	-
2	Active	VOP1164A-61	VOP1164A-61	01:29:12	-	-	-
3	Active	ALC1132A-51	ALC1132A-51	01:29:37	-	-	-
4	Active	ELC1132A-45	ELC1132A-45	01:28:56	-	-	-
5	Active	VLC1124A-51	VLC1124A-51	01:28:38	-	-	-

IES4105, Zyxel Communications Corp.

5.3 Navigation Panel

In the navigation panel (the column on the left), click a main link to reveal a list of submenu links. Some screens include different tabs. The following table lists the various Web Configurator screens you can access through the navigation panel.

Table 27 Navigation Panel

ACL Anti Macspoof DHCP 802.1x General Setup Radius Server User Profile Port Setting Port Status Loopguard Loopguard Statistics Packet Filter PPPoE Rule	Alarm Current History Input Alarm Input CPU Overload Alarm System Suppress Definition DSL Eqpt Sys Enet VoIP FE	Diagnostic DELT IP Ping MLT SELT	Line Card Line Card
Maintenance Config Backup Config Restore Config Reset FW Upgrade Reboot	Multicast IGMP IGMP Setup Port Setup Port MVLAN Setup IGMP Privilege Profile IGMP Status IGMP Status IGMP Port Group IGMP Port Statistics IGMP Port Log MVLAN MVLAN MVLAN Table Static Multicast	Port Alarm Copy Default DHCP DSL DSL Status FDB PVC QoS H.248 SIP FE	Profile ACL Enet Alarm Profile DSL Line Profile Channel Profile Template Profile DSL Alarm Profile Alarm Profile Alarm Line Profile Alarm Channel Profile Alarm Template Profile QoS VC-Shaping Shaping WRR-WFQ VoIP Alarm Profile VoIP DSP FE Alarm Profile VoIP SIP VoIP SIP Callservice VoIP SIP Dialplan Xdsl Bonding

Table 27 Navigation Panel (continued)

Statistics ARP Table DHCP Snooping DDMI Dot3ad Status MAC Table Online Users Port RSTP Bonding Status	Switch Mirror RSTP RSTP Bridge RSTP Port Switch Port Setup Switch Setup General Dot3ad Isolation DSCP Storm Control VC-Shaping	Sys AAA Accounting Authentication Authorization Radius Server Tacacs Server Access Control SNMP Secured Client Secured Client6 General Setup IP Setup IPv4 Setup IPv6 Setup Monitor Monitor Statistics CPU Utilization System Information Users Account	VLAN Enet VLAN Enet VLAN Untag Port VLAN TLS Port VLAN Trunk uni-Tag uni-Untag Port VLAN Translation Port VLAN Transparent VLAN s-tag Setup
VoIP Country Code H.248 H.248 Statistics IP Setup VoIP Interface RTP Interface Key Pattern Line Info POTS Ring Flash	Config Save Config Save		

5.4 Saving Your Configuration

Click **Apply** in a configuration screen when you are done modifying the settings in that screen to save your changes back to the run time memory and to make your changes take effect.

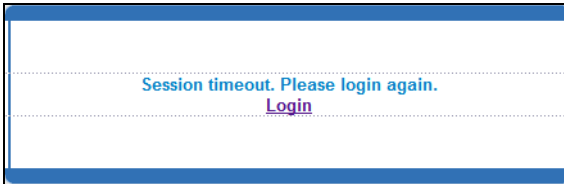
Click **Config Save** in the navigation panel and then the **Save** button to save your configuration to nonvolatile memory. Nonvolatile memory refers to the IES's storage that remains even if the IES's power is turned off.

Unsaved changes are lost when the IES's power is turned off.

5.5 Logging Out of the Web Configurator

Click **Logout** in a screen to exit the Web Configurator. You have to log in with your password again after you log out. This is recommended after you finish a management session both for security reasons and so as you don't lock out other IES administrators.

Figure 55 Web Configurator: Logout Screen



5.6 System Info (Home) Screen

The **System Info (Home)** screen displays when you access the Web Configurator or click **Home**.

Figure 56 System Info (Home)

System Info

Current Alarm

Critical Alarms: 0

Major Alarms: 0

Minor Alarms: 0

Warning Alarms: 0

ID	State	Card Type	Provision Type	Uptime	Heat	Vol	Mon
1	Active	MSC1002GA	-	24:41	-	-	-
2	Active	VOP1164A-61	VOP1164A-61	23:28	-	-	-
3	Active	ALC1132A-51	ALC1132A-51	23:53	-	-	-
4	Active	ELC1132A-45	ELC1132A-45	23:11	-	-	-
5	Active	VLC1124A-51	VLC1124A-51	22:53	-	-	-

The following table describes the labels in this screen.

Table 28 System Info (Home)

LABEL	DESCRIPTION
Current Alarms	Click the links to view detailed alarm information (see Section 7.1 on page 96).
Critical Alarms	This field displays the number of critical alarms that have occurred. Click the link to display the Current Alarm: Critical Alarm screen.
Major Alarms	This field displays the number of major alarms that have occurred. Click the link to display the Current Alarm: Major Alarm screen.
Minor Alarms	This field displays the number of minor alarms that have occurred. Click the link to display the Current Alarm: Minor Alarm screen.
Warning Alarms	This field displays the number of warning alarms that have occurred. Click the link to display the Current Alarm: Warning Alarm screen.
ID	This is the slot number of a line card. Click the index number of an active line card to display the System Info - Slot screen to view detailed status.

Table 28 System Info (Home) (continued)

LABEL	DESCRIPTION
State	This field displays the line card's current operational status. active means the line card is operating normally. init means the IES is initializing the line card. disable means a manager has disabled the line card. inactive means the line card is starting up or is not operating normally. This could be due to the card starting, a firmware upgrade in progress or a malfunction.
Card Type	This field displays the type of a line card.
Provision Type	This field displays the type of card the slot is provisioned for.
Up Time	This field displays how long the line card has been running since the last time it was started.
Heat	This field indicates whether the temperate of the line card is too high.
Vol	This field indicates whether the voltage on the line card is out of the tolerance range.
Mon	This field indicates if there is any abnormal voltage or temperature value.

5.6.1 Card Status Details

To view detailed card status information, click an index number of an active card in the **System Info** screen. The screen varies depending on the type of card you select.

Figure 57 System Info: Slot (MSC)

System Information		
Hardware Version		
Hardware Serial Number		
CLEI Code		
Firmware Version	V3.60(ABJK.0)b2 03/21/2017	
Inband MAC	00:13:49:AB:CD:12	
Outband MAC	00:13:49:AB:CD:12	
Current Voltage Level	Current Temperature	Current Fan Speed
1.790	38.000	1983
1.037	35.000	2983
3.360	33.000	1955
2.486		
14.109		

Figure 58 System Info: Slot (ALC)

System Information	
Hardware Version	R1B
Hardware Serial Number	SN1234
CLEI Code	SBUIAFUEBB
Firmware Version	
dsl driver version	11.0
dsl modem version	11.00.31
Inband MAC	
Outband MAC	

Current Voltage Level	Current Temperature	Current Fan Speed
2.532	34.000	
1.189	40.000	
3.342	42.000	
5.065		
14.296		

Figure 59 System Info: Slot (VLC)

System Information	
Hardware Version	R1B
Hardware Serial Number	SUC70036214
CLEI Code	SBUIAFZEAA
Firmware Version	V3.60(ABJK.0)b2 03/21/2017
dsl driver version	11.0
dsl modem version	11.00.29
Inband MAC	
Outband MAC	

Current Voltage Level	Current Temperature	Current Fan Speed
1.217	40.000	
1.212	41.000	
3.342	37.000	
2.513		
14.577		

Figure 60 System Info: Slot (VOP)

System Information		
Hardware Version		
Hardware Serial Number		
CLEI Code		
Firmware Version	V3.60(ABJK.0)b2 03/21/2017	
codec slc driver version	2.17.3	
codec slc modem version	14.7a	
dsp driver version	01.00.05.03	
dsp modem version	13.7.501.0	
Inband MAC		
Outband MAC		

Current Voltage Level	Current Temperature	Current Fan Speed
1.243	36.000	
1.822	37.000	
3.342	38.000	
1.028		
14.764		

The following table describes the labels in this screen.

Table 29 System Info: Slot

LABEL	DESCRIPTION
Hardware Version	This is the version of the physical device hardware.
Hardware Serial Number	This is the individual identification number assigned to the device at the factory.
CLEI Code	If the card has a Common Language Equipment Identification (CLEI) Code, it displays here. CLEI Codes identify individual Central Office Telecommunications products.
Firmware Version	This field displays the version number of the device's current firmware and its creation date.
dsl driver version	This is the driver version that a DSL line card's DSL chip is using.
dsl modem version	This is the release of modem code that a DSL line card is using.
codec slc driver version	This field displays the driver version of the Codec SLIC chipset on a VOP line card.
codec slc modem version	This field displays the modem version of the Codec SLIC chipset on a VOP line card.
dsp driver version	This field displays the driver version that a VOP line card's DSP chip is using.
dsp modem version	This is the release of modem code that a VOP line card is using.
Inband MAC	This field applies to the management card. It displays the MAC address used for the inband management interface.
Outband MAC	This field applies to the management card. It displays the MAC address used for the out-of-band management interface.
Current Voltage Level	This field displays the current voltage readings at the card's sensors.

Table 29 System Info: Slot (continued)

LABEL	DESCRIPTION
Current Temperature	This field displays the current temperature at the card's sensors.
Current Fan Speed	This field applies to the management card. It displays the current fan speeds.

5.7 Enable Privilege Screen

Each Web Configurator screen requires a privilege level to access.

- Privilege level 1 access is read-only.
- Privilege level 8 access lets you view most screens and configure general features.
- Privilege level 14 access lets you view all the screens and configure all settings including creating administrator accounts, restarting the system, and resetting the factory defaults.

When the system uses a TACACS+ server to authenticate administrator logins, you automatically have the lowest privilege level (1) when you log into the Web Configurator.

When the system uses its local database to authenticate administrator logins, you automatically have your account's assigned privilege level when you log into the Web Configurator.

In either case you can use the **Enable Privilege** screen to change your privilege level for your current Web Configurator session. Click **Enable** at the top of the screen to open the **Enable Privilege** screen.

Figure 61 Enable Privilege

The following table describes the labels in this screen.

Table 30 Enable Privilege

LABEL	DESCRIPTION
Privilege	Select the access level you want to attain.
Password	Enter the password for the access level you selected.
Apply	Click Apply to have the system authenticate the password you entered.
Cancel	Click Cancel to begin configuring this screen afresh.

5.8 Enable Password Screen

Click **Enable** > **Password** at the top of the screen to open this screen where you can configure the password for each access privilege level. These passwords are the ones the system checks for if you set AAA authentication for Enable privilege to local. These passwords are separate from the login password and can be different from the login password. Only an administrator with the configuration session at privilege level 14 can configure these settings.

Figure 62 Enable > Password

The following table describes the labels in this screen.

Table 31 Enable > Password

LABEL	DESCRIPTION
Privilege	These are the access levels.
Password	Configure the password for each access level.
Retype Password	Type the configured password again.
Apply	Click Apply to save the changes in this screen to the system's volatile memory. The system loses these changes if it is turned off or loses power, so use the Config Save link on the navigation panel and then the Save button to save your changes to the non-volatile memory when you are done configuring.
New	Click New to create a new privilege entry.
Cancel	Click Cancel to begin configuring this screen afresh.
Privilege	Displays the access level.
Password	Displays the password hidden behind asterisk characters.
Select	Click Select to choose a privilege.
Modify	Click Modify to change a privilege's level and password.
Delete	Click Delete to remove a privilege.

CHAPTER 6

Access Control List Screens

This chapter describes the ACL (Access Control List) screens.

6.1 Anti-MAC Spoofing Screen

With anti-MAC spoofing enabled, a line card that detects MAC address spoofing (another device using a MAC address that is connected to another subscriber port on the system) disables the subscriber port where it detected the spoofed MAC address. The line card re-enables the port after five minutes.

Click **ACL > AntiMacspoof** to enable or disable protection against MAC address spoofing.

Note: A line card can detect MAC spoofing only when the spoofed MAC address is already in use by a device connected to another subscriber port.

Figure 63 ACL > AntiMacspoof

The following table describes the labels in this screen.

Table 32 ACL > AntiMacspoof

LABEL	DESCRIPTION
Anti Macspoof	Turn on MAC spoofing protection to have the system check for hosts with fake or duplicated MAC addresses which attempt to access the system.
Spoof Action Enable	Turn on anti-spoofing action so the IES deactivates User Network Interface (UNI) ports upon which it detects MAC address spoofing.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to begin configuring the screen again.

6.2 DHCP Transparent Screen

DHCP (Dynamic Host Configuration Protocol) allows individual clients to obtain TCP/IP configuration at start-up from a DHCP server. Click **ACL > DHCP** to configure the IES to bypass all DHCP packets

(Discover, Offer, Request, ACK) on specific VLANs. The IES does not check and record any information for DHCP packets on those VLANs.

Note: DHCP transparent and L2 Agent cannot be enabled at the same time in the same VLAN.

Figure 64 ACL > DHCP > Transparent

The screenshot shows the configuration interface for DHCP Transparent. At the top, there are two tabs: 'Transparent' (active) and 'L2 Agent'. Below the tabs, there is a 'Transparent VID' input field with a range indicator '[1 ~ 4093]' and an 'Apply' button. Below this is a table with three columns: 'Index', 'Transparent VID', and 'Select'. The table contains one entry with 'Index' 1, 'Transparent VID' 1, and a radio button in the 'Select' column. Below the table is a 'Delete' button.

The following table describes the labels in this screen.

Table 33 ACL > DHCP > Transparent

LABEL	DESCRIPTION
Transparent VID	Enter a VLAN ID (between 1 and 4093) that enables transparent DHCP packets to have the IES bypass all DHCP packets.
Apply	Click Apply to save your changes.
Index	This is the index number of an entry.
Transparent VID	This is the ID number of the VLAN group.
Select	Select an entry's Select check box and click Delete to remove the entry.
Delete	Click Delete to remove the selected entries.
Apply	Click Apply to save your changes.

6.3 DHCP L2 Agent Screen

Click **ACL > DHCP > L2 Agent** to configure DHCP L2 Agent to have the IES only accept DHCP requests from the downlink network on specific VLANs. It will drop other DHCP packets, such as DHCP Offer. This can help prevent Denial-Of-Service (DOS) attacks through DHCP.

Note: DHCP transparent and L2 Agent cannot be enabled at the same time in the same VLAN.

Figure 65 ACL > DHCP > L2 Agent

The following table describes the labels in this screen.

Table 34 ACL > DHCP > L2 Agent

LABEL	DESCRIPTION
Max-lease Overflow-mode	Select the DHCP snooping database overflow handling mode. The DHCP snooping table supports 32 entries at maximum per subscriber data port. If the table is full and a new record is observed, then Deny-new-lease: denies a new record. Remove-oldest-lease: drops the oldest record in the table, and adds the new one into the table.
Apply	Click Apply to save your changes.
L2 Agent VID	Enter a VLAN ID (between 1 and 4093) that enables DHCP L2 Agent to have the IES only accept DHCP requests from the downlink network.
Ldra	Click the check box to enable DHCP L2 Agent Lightweight DHCPv6 Relay Agent (LDRA) function on the VLAN.
Format	Select a DHCP relay agent information option.
Option-Info	Use this field to specify up to 127 English keyboard characters of additional information for the IES to add to the DHCP requests that it relays to a DHCP server.
Apply	Click Apply to save your changes.
New	Click New to create a new DHCP relay entry.
Cancel	Click Cancel to begin configuring this screen afresh.
Index	This is the index number of an entry.
L2 Agent VID	This is the ID number of the VLAN group.
Ldra	This field displays whether the LDRA is enabled or not.
Interface-ID Option18-Info	This field displays the option 18 interface ID information to add to the DHCP request packets.

Table 34 ACL > DHCP > L2 Agent

LABEL	DESCRIPTION
Remote-ID Option37-Info	This field displays the option 37 remote ID information to add to the DHCP request packets.
Circuit-ID Option82-Info	This field displays the option 82 circuit ID information to add to the DHCP request packets.
Remote-ID Option82-Info	This field displays the option 82 remote ID information to add to the DHCP request packets.
Select	Select an entry's Select check box and click Delete to remove the entry or click Modify to edit the entry.
Modify	Click Modify to change the settings of the selected entry.
Delete	Click Delete to remove the selected entries.

6.4 IEEE 802.1x

This section describes the IEEE 802.1x authentication method and RADIUS server connection setup.

IEEE 802.1x is an extended authentication protocol¹ that allows support of RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile management on a network RADIUS server.

6.4.1 General Setup

Click **ACL > 802.1x > General Setup** to enable IEEE 802.1x and select the authentication method.

Figure 66 ACL > 802.1x > General Setup

The screenshot shows the 'General Setup' configuration page for IEEE 802.1x. The page has a tabbed interface with the following tabs: '802.1x' (selected), 'Radius Server', 'User Profile', 'Port Setting', and 'Port Status'. Under the 'General Setup' tab, there is a section with two fields: 'Enable 802.1x Method' with an unchecked checkbox, and 'Authentication Method' with a dropdown menu set to 'radius'. At the bottom of the page are 'Apply' and 'Cancel' buttons.

1. Not all Windows operating systems support IEEE 802.1x (see the Microsoft web site for details). For other operating systems, see its documentation. If your operating system does not support IEEE 802.1x, then you may need to install IEEE 802.1x client software.

The following table describes the labels in this screen.

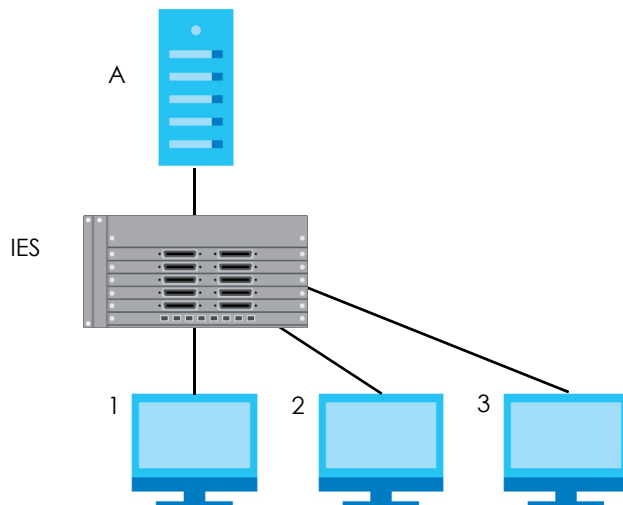
Table 35 ACL > 802.1x > General Setup

LABEL	DESCRIPTION
Enable 802.1x Method	Click the check box to enable the IEEE 802.1x.
Authentication Method	Select the IEEE 802.1x port authentication method. radius: send the authentication request to the RADIUS server. userprofile: the IES does the authentication.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to begin configuring the screen again.

6.4.2 RADIUS Server

RADIUS authentication is a popular protocol used to authenticate users by means of an external server instead of (or in addition to) an internal device user database that is limited to the memory capacity of the device. In essence, RADIUS authentication allows you to validate an unlimited number of users from a central location. In the following graphic, the RADIUS server (A) authenticates users 1, 2, and 3.

Figure 67 RADIUS Server



Click **ACL > 802.1x > RADIUS Server** to configure the authentication server's IP address and port number.

Figure 68 ACL > 802.1x > RADIUS Server

Index	IP Address	Port	Secret
1	0.0.0.0	1812	1234
2	0.0.0.0	1812	1234
3	0.0.0.0	1812	1234
4	0.0.0.0	1812	1234
5	0.0.0.0	1812	1234
6	0.0.0.0	1812	1234
7	0.0.0.0	1812	1234
8	0.0.0.0	1812	1234
9	0.0.0.0	1812	1234
10	0.0.0.0	1812	1234
11	0.0.0.0	1812	1234
12	0.0.0.0	1812	1234
13	0.0.0.0	1812	1234
14	0.0.0.0	1812	1234
15	0.0.0.0	1812	1234
16	0.0.0.0	1812	1234

Apply Cancel

The following table describes the labels in this screen.

Table 36 ACL > 802.1x > RADIUS Server

LABEL	DESCRIPTION
Index	This is the index number of a RADIUS server.
IP Address	Enter the IP address of the external RADIUS server in dotted decimal notation.
Port	The default port of the RADIUS server for authentication is 1812 . You need not change this value unless your network administrator instructs you to do so.
Secret	Specify a password (up to 31 alphanumeric characters) as the key to be shared between the external RADIUS server and the system. This key is not sent over the network. This key must be the same on the external RADIUS server and the IES.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to begin configuring the screen again.

6.4.3 User Profile

Click **ACL > 802.1x > User Profile** to configure the IEEE 802.1x user accounts.

Figure 69 ACL > 802.1x > User Profile

The following table describes the labels in this screen.

Table 37 ACL > 802.1x > User Profile

LABEL	DESCRIPTION
Name	Type an IEEE 802.1x user name for local authentication.
Password	Configure the password for the user account.
Retype Password	Type the configured password again.
Apply	Click Apply to save your changes.
New	Click New to create a new user account.
Cancel	Click Cancel to begin configuring the screen again.
Index	This is the index number of a user account.
Name	This displays the user name.
Select	Select the check box to choose a user account.
Modify	Click Modify to change the settings of the selected name.
Delete	Click Delete to remove the selected name.

6.4.4 Port Setting

Click **ACL > 802.1x > Port Setting** to configure the IEEE 802.1x port authentication.

Figure 70 ACL > 802.1x > Port Setting

Port Setting

General Setup | Radius Server | User Profile | **Port Setting** | Port Status

Slot: 3

Port	Enable Circuid ID	Control	Server Index	Auth Once	[60 ~ 65535] Reauth Period
All	☐			☐	
1	☐	auth	1	☐	3600
2	☐	auth	1	☐	3600
3	☐	auth	1	☐	3600
4	☐	auth	1	☐	3600
5	☐	auth	1	☐	3600
6	☐	auth	1	☐	3600
7	☐	auth	1	☐	3600
9	☐	auth	1	☐	3600
10	☐	auth	1	☐	3600
11	☐	auth	1	☐	3600
12	☐	auth	1	☐	3600
13	☐	auth	1	☐	3600
14	☐	auth	1	☐	3600
15	☐	auth	1	☐	3600
16	☐	auth	1	☐	3600
17	☐	auth	1	☐	3600
22	☐	auth	1	☐	3600
23	☐	auth	1	☐	3600
24	☐	auth	1	☐	3600
25	☐	auth	1	☐	3600
26	☐	auth	1	☐	3600
27	☐	auth	1	☐	3600
28	☐	auth	1	☐	3600
29	☐	auth	1	☐	3600
30	☐	auth	1	☐	3600
31	☐	auth	1	☐	3600
32	☐	auth	1	☐	3600

Apply Cancel

The following table describes the labels in this screen.

Table 38 ACL > 802.1x > Port Setting

LABEL	DESCRIPTION
Slot	Select a slot for configuring the IEEE 802.1x authentication.
Port	This is the index number of subscriber ports.
Enable	Click the check box to enable IEEE 802.1x authentication on the specified port.
Circuit ID	Type the circuit ID information to add to request packet to the RADIUS server, up to 127 characters.
Control	Select auto to authenticate all subscribers before they can access the network through this port. Select auth to allow all connected users to access the network through this port without authentication. Select unauth to deny all subscribers access to the network through this port.
Server Index	This is the index number of a RADIUS server.
Auth Once	Click the check box to stop user re-authentication for the ports.
Reauth Period	Specify how often a client has to re-enter his or her username and password to stay connected to the port.
All	Configure settings at All to set all the settings for each port at once.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to begin configuring the screen again.

6.4.5 Port Status

Click **ACL > 802.1x > Port Status** to display the IEEE 802.1x port authentication status for all ports.

Figure 71 ACL > 802.1x > Port Status

Port Status						
General Setup Radius Server User Profile Port Setting Port Status						
Slot 3						
Port	Status	Control	Reauth	Reauth Period (sec)	Authorized	Reauth Count
1	inactive	auto	V	3600	-	
2	inactive	auto	V	3600	-	
3	inactive	auto	V	3600	-	
4	inactive	auto	V	3600	-	
5	inactive	auto	V	3600	-	
6	inactive	auto	V	3600	-	
7	inactive	auto	V	3600	-	
8	inactive	auto	V	3600	-	
9	inactive	auto	V	3600	-	
10	inactive	auto	V	3600	-	
11	inactive	auto	V	3600	-	
12	inactive	auto	V	3600	-	

The following table describes the labels in this screen.

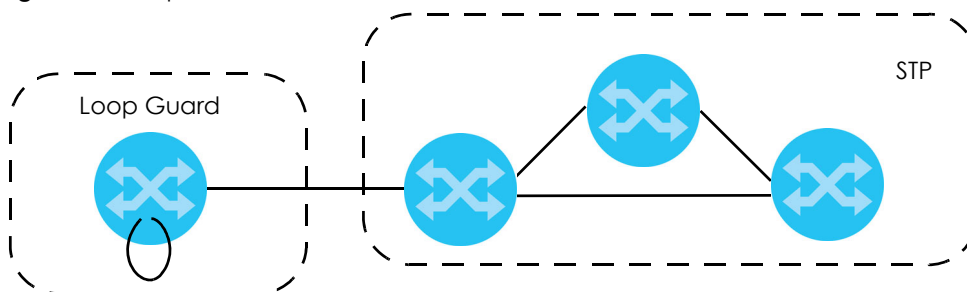
Table 39 ACL > 802.1x > User Status

LABEL	DESCRIPTION
Slot	This field displays the number of the slot.
Port	This field displays the number of the port.
Status	This field displays whether the IEEE 802.1x is enabled on the specified port. active means IEEE 802.1x is enabled on the specified port. inactive means IEEE 802.1x is disabled on the specified port.
Control	This field displays the IEEE 802.1x port authentication option for a subscriber port.
Reauth	This field displays whether the IEEE 802.1x re-authentication option is turned on or not (V for enabled, - for disabled).
Reauth Period	This field displays the IEEE 802.1x re-authentication period.
Authorized	This field displays whether the specified port has passed the IEEE 802.1x authorized process.
Reauth Count	This field displays the number of re-authentication attempts.

6.5 Loop Guard

Configure loop guard to protect against loops on the edge of your network. Loop guard allows you to configure the system to shut down a port if it detects that packets sent out on that port loop back to the system. While you can use Spanning Tree Protocol (STP) to prevent loops in the core of your network, STP cannot prevent loops that occur on the edge of your network.

Figure 72 Loop Guard vs. STP



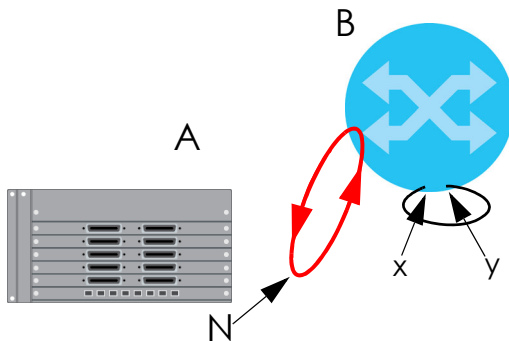
Loop guard is designed to handle loop problems on the edge of your network. This can occur when a port is connected to a switch that is in a loop state. Loop state occurs as a result of human error. It happens when two ports on a switch are connected with the same cable. When a switch in loop state sends out broadcast messages the messages loop back to the switch and are re-broadcast again and again causing a broadcast storm.

If a switch (not in loop state) connects to a switch in loop state, then it will be affected by the switch in loop state in the following way:

- It will receive broadcast messages sent out from the switch in loop state.
- It will receive its own broadcast messages that it sends out as they loop back. It will then re-broadcast those messages again.

The following figure shows port **N** on system **A** connected to another switch **B**. Switch **B** has mistakenly two ports, **x** and **y**, connected to each other. It forms a loop. When switch **B** receives broadcast or multicast frames, they will be broadcast again to senders including port **N** on system **A**.

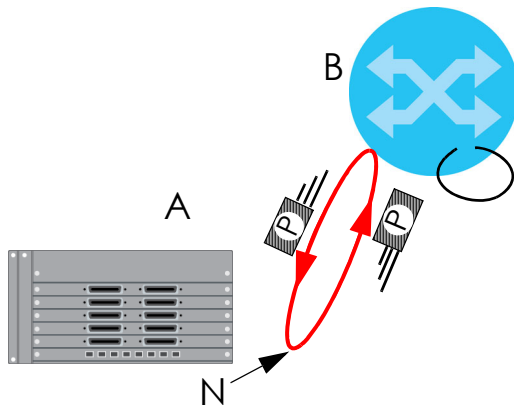
Figure 73 Switch in Loop State



The loop guard feature checks to see if a loop guard enabled port is connected to a switch in loop state. This is accomplished by periodically sending a probe packet and seeing if the packet returns on the same port. If this is the case, the system will shut down the port connected to the switch in loop state.

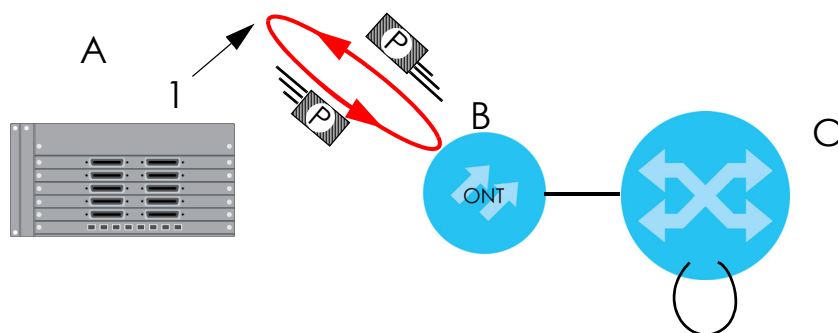
Loop guard can be enabled on both Ethernet ports or xDSL ports. In the following figure, Ethernet port **N** has loop guard enabled on the system **A** sending a probe packet **P** to switch **B**. Since switch **B** is in loop state, the probe packet **P** returns to port **N** on **A**. The system then shuts down port **N** to ensure that the rest of the network is not affected by the switch in loop state.

Figure 74 Loop Guard - Probe Packet



The system also shuts down port **N** if the probe packet returns to system **A** on any other port. In other words loop guard also protects against standard network loops.

The following figure illustrates the system **A**, a subscriber device **B** and another switch **C** forming a loop. A sample path of the loop guard probe packet is also shown. In this example, the probe packet is sent from an xDSL port **1** and returns also on port **1**. As long as loop guard is enabled on port **1**, the system will shut down port **1** if it detects that the probe packet has returned to the system.

Figure 75 Loop Guard - Network Loop

Note: After resolving the loop problem on your network you can re-activate the disabled port via the Web Configurator or via commands.

6.5.1 Loopguard Setup

Click **ACL > Loopguard > Loopguard** to configure loop guard.

Figure 76 ACL > Loopguard > Loopguard

Loopguard

Loopguard Statistics

Slot 3

Port	Status	LG Enable	Policy	[60 ~ 600] sec Recover Time	[1 ~ 4093] Uni vlan	[0 ~ 7] Pbit
All		☐				
1	inactive	☐	fix	60	-	-
2	inactive	☐	fix	60	-	-
3	inactive	☐	fix	60	-	-
4	inactive	☐	fix	60	-	-
5	inactive	☐	fix	60	-	-
6	inactive	☐	fix	60	-	-
7	inactive	☐	fix	60	-	-
8	inactive	☐	fix	60	-	-
9	inactive	☐	fix	60	-	-
10	inactive	☐	fix	60	-	-
11	inactive	☐	fix	60	-	-
12	inactive	☐	fix	60	-	-
13	inactive	☐	fix	60	-	-
14	inactive	☐	fix	60	-	-
29	inactive	☐	fix	60	-	-
30	inactive	☐	fix	60	-	-
31	inactive	☐	fix	60	-	-
32	inactive	☐	fix	60	-	-

Apply Cancel

The following table describes the labels in this screen.

Table 40 ACL > Loopguard > Loopguard

LABEL	DESCRIPTION
Slot	Select a slot to configure the subscriber ports' loop guard settings.
Port	This column lists the subscriber ports.

Table 40 ACL > Loopguard > Loopguard (continued)

LABEL	DESCRIPTION
Status	This field displays the line card's current operational status. active means the specified port is in link up state. inactive means the specified port is in link down state.
LG Enable	Enable or disable loop guard for this individual port.
Policy	Select the port mode for loop guard. If you select fix, the system shuts down the port when the system detects that packets sent out on the port loop back to the system. To activate the port again, you need to manually enable the port in the corresponding port setup screen. If you select dynamic, the system shuts down the port if the system detects that packets sent out on the port loop back to the system. The port becomes active automatically after the time you specified in the Recover Time field.
Recover Time	Enter the time (in seconds) a port in dynamic mode waits to become active again after the loop guard feature shuts it down.
Uni VLAN	Configure the unicast VLAN tag for the loop detection packets.
Pbit	Configure the IEEE 802.1p priority bit for the loop detection packets.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to begin configuring the screen again.

6.5.2 Statistics Screen

Click **ACL > Loop Guard > Statistics** to display loop guard statistics (packet counters).

Figure 77 ACL > Loop Guard > Statistics

Statistics

Loopguard Statistics

Slot 3

Refresh

Flush

Port	Status	LG Enable	Total TxPkts	Total RxPkts	Bad RxPkts	Shutdown Time
1	inactive	y	0	0	0	01/01/1970 00:00:00
2	inactive	-	0	0	0	01/01/1970 00:00:00
3	inactive	-	0	0	0	01/01/1970 00:00:00
4	inactive	-	0	0	0	01/01/1970 00:00:00
5	inactive	-	0	0	0	01/01/1970 00:00:00
6	inactive	-	0	0	0	01/01/1970 00:00:00
7	inactive	-	0	0	0	01/01/1970 00:00:00
8	inactive	-	0	0	0	01/01/1970 00:00:00
9	inactive	-	0	0	0	01/01/1970 00:00:00
10	inactive	-	0	0	0	01/01/1970 00:00:00
11	inactive	-	0	0	0	01/01/1970 00:00:00
12	inactive	-	0	0	0	01/01/1970 00:00:00
13	inactive	-	0	0	0	01/01/1970 00:00:00
14	inactive	-	0	0	0	01/01/1970 00:00:00
15	inactive	-	0	0	0	01/01/1970 00:00:00

The following table describes the labels in this screen.

Table 41 ACL > Loop Guard > Statistics

LABEL	DESCRIPTION
Slot	Select a slot number to display subscriber ports' loop guard statistics.
Refresh	Click Refresh to reload the statistics of the port.
Flush	Click Flush to remove all the statistics of the port.
Port	This field displays the number of the port.
Status	This field displays the current link status of a port. active: the port is in link up state inactive: the port is in link down state
LG Enable	This field displays whether loop guard is enabled or disabled for this individual port.
Total TxPkts	This is the total number of packets the port has sent.
Total RxPkts	This is the total number of packets the port has received.

Table 41 ACL > Loop Guard > Statistics (continued)

LABEL	DESCRIPTION
Bad RxPkts	This is the number of packets the loop guard feature has detected that looped back to the port.
Shutdown Time	If the loop guard feature detected looped back packets on this port and shut it down, the time that it did so displays here.

6.6 Packet Filter Screen

Click **ACL > Packet Filter** to set which types of packets the IES accepts on individual DSL or FE ports.

Figure 78 ACL > Packet Filter

Packet filter setup

Slot **3** Port **1** **Load**

Index	VLAN	PPPoE	Drop	Drop	Drop	Drop	Drop	Drop	Drop	Select
		Only	PPPoE	IP	ARP	NetBIOS	DHCP	EAPOL	IGMP	

Delete

VLAN [1 ~ 4093]

PPPoE Only ☒

Drop ☐

Drop Packet Type

PPPoE	Filter Out ☐	IP	Filter Out ☐
ARP	Filter Out ☐	NetBIOS	Filter Out ☐
DHCP	Filter Out ☐	EAPOL	Filter Out ☐
IGMP	Filter Out ☐		

Apply **Cancel**

ID	State	Card Type	Uptime
1	Active	MSC1002GA	114:36:05
2	Active	VOP1164A-61	114:34:52
3	Active	ALC1132A-51	114:35:17
4	Active	ELC1132A-45	114:34:35
5	Active	VLC1124A-51	114:34:17

The following table describes the labels in this screen.

Table 42 ACL > Packet Filter

LABEL	DESCRIPTION
Slot, Port	Use the drop-down list boxes to select a DSL or FE port on a line card for which you wish to configure packet type filtering.
Load	Click Load to display the port's current settings.
Index	This is the index number of an entry.
VLAN	This displays the VLAN ID.
PPPoE Only	This displays whether only PPPoE packets are allowed.

Table 42 ACL > Packet Filter (continued)

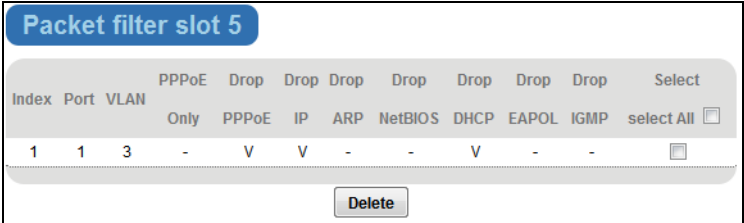
LABEL	DESCRIPTION
Drop PPPoE	This displays whether PPPoE packets are blocked (V for blocked, - for allowed).
Drop IP	This displays whether IP packets are blocked (V for blocked, - for allowed).
Drop ARP	This displays whether ARP packets are blocked (V for blocked, - for allowed).
Drop NetBIOS	This displays whether NetBIOS packets are blocked (V for blocked, - for allowed).
Drop DHCP	This displays whether DHCP packets are blocked (V for blocked, - for allowed).
Drop EAPOL	This displays whether EAPOL packets are blocked (V for blocked, - for allowed).
Drop IGMP	This displays whether IGMP packets are blocked (V for blocked, - for allowed).
Select	Click Select to choose an entry.
Delete	Click Delete to remove the selected entries.
Select the radio buttons of the types of packets to accept on the port.	
VLAN	Enter a VLAN ID (1 to 4093).
PPPoE Only	Select PPPoE Only to allow only PPPoE traffic. This will gray out the check boxes for other packet types and the switch will drop any non-PPPoE packets.
Drop	Select Drop and specify which types of packets listed below will be blocked.
PPPoE Filter Out	Point-to-Point Protocol over Ethernet relies on PPP and Ethernet. It is a specification for connecting the users on an Ethernet to the Internet through a common broadband medium, such as a single DSL line, wireless device or cable modem.
IP Filter Out	Internet Protocol. The underlying protocol for routing packets on the Internet and other TCP/IP-based networks.
ARP Filter Out	Address Resolution Protocol is a protocol for mapping an Internet Protocol address (IP address) to a physical computer address that is recognized in the local network.
NetBIOS Filter Out	NetBIOS (Network Basic Input/Output System) are TCP or UDP packets that enable a computer to find other computers.
DHCP Filter Out	Dynamic Host Configuration Protocol (DHCP) automatically assigns IP addresses to clients when they log on. DHCP centralizes IP address management on central computers that run the DHCP server program. DHCP leases addresses, for a period of time, which means that past addresses are "recycled" and made available for future reassignment to other systems.
EAPOL Filter Out	EAP (Extensible Authentication Protocol, RFC 2486) over LAN. EAP is used with IEEE 802.1x to allow additional authentication methods (besides RADIUS) to be deployed with no changes to the access point or the wireless clients.
IGMP Filter Out	Internet Group Management Protocol is used when sending packets to a specific group of hosts.
Apply	Click Apply to save your changes in this screen.
Cancel	Click Cancel to begin configuring the screen again.
ID	This is the slot number of a line card. Click an ID to view detailed packet filter settings of the specified slot as shown below. Figure 79 ACL > Packet Filter > Slot 

Table 42 ACL > Packet Filter (continued)

LABEL	DESCRIPTION
State	This field displays the line card's current operational status. Active means the line card is operating normally. init means the IES is initializing the line card. disable means a manager has disabled the line card. inactive means the specified port is in link down state.
Card Type	This field displays the type of a line card.
Up Time	This field displays how long the line card has been running since the last time it was started.

6.7 PPPoE

6.7.1 PPPoE Intermediate Agent

This section describes how the IES gives a PPPoE termination server additional information that the server can use to identify and authenticate a PPPoE client.

If the PPPoE Intermediate Agent is enabled, the IES adds a vendor-specific tag to PADI (PPPoE Active Discovery Initialization) and PADR (PPPoE Active Discovery Request) packets from PPPoE clients. This tag is defined in RFC 2516 and has the following format for this feature.

Table 43 PPPoE Intermediate Agent Vendor-specific Tag Format

Tag_Type (0x0105)	Tag_Len	Value	i1	i2

The Tag_Type is 0x0105 for vendor-specific tags, as defined in RFC 2516. The Tag_Len indicates the length of Value, i1 and i2. The Value is the 32-bit number 0x00000DE9, which stands for the "ADSL Forum" IANA entry. i1 and i2 are PPPoE intermediate agent sub-options, which contain additional information about the PPPoE client. The IES supports remote ID and circuit ID in TR-101 format for the PPPoE intermediate agent sub-options.

6.7.2 PPPoE Screen

Use the **ACL > PPPoE** screen to configure PPPoE line information setting by VLAN. The IES adds the line information to PPPoE packets for identification and security.

Figure 80 ACL > PPPoE

PPPoE

Transparent VID 1 ~ 4093

Apply

Index	Transparent VID	Select
1	1	☐

Delete

Intermediate-Agent VID 1 ~ 4093

Format

☐ Circuit ID Option-Info

☐ Remote ID Option-Info

Apply **New** **Cancel**

Index	Intermediate-Agent VID	Circuit-ID Option-Info	Remote-ID Option-Info	Select
1	4			☐

Modify **Delete**

The following table describes the labels in this screen.

Table 44 ACL > PPPoE

LABEL	DESCRIPTION
Transparent VID	Enter a VLAN ID (between 1 and 4093) for PPPoE packet transparent.
Apply	Click Apply to save your changes in this screen.
Index	This is the index number of an entry.
Transparent VID	This displays the transparent VLAN ID.
Select	Click Select to choose an entry.
Delete	Select an entry's Select button and click Delete to remove the entry.
Intermediate-Agent VID	Enter a VLAN ID (between 1 and 4093) for PPPoE intermediate agent.
Format	Configure the PPPoE intermediate agent format. Enter up to 127 ASCII characters of additional information for the IES to add to the VLAN's PPPoE packets. See Table 250 on page 391 for detailed information on Circuit ID and Remote ID option info.
Apply	Click Apply to save your changes in this screen.
New	Click New to clear the fields so you can create a new entry.
Cancel	Click Cancel to begin configuring this screen afresh.
Index	This is the index number of an entry.
Intermediate-Agent VID	This displays the intermediate agent VLAN ID.
Circuit-ID Option-Info	This displays the additional information in the Agent Circuit-ID Sub-option.
Remote-ID Option-Info	This displays the additional information in the Agent Remote-ID Sub-option.

Table 44 ACL > PPPoE (continued)

LABEL	DESCRIPTION
Select	Click Select to choose an entry.
Modify	Select an entry's Select button and click Modify to edit the entry's information.
Delete	Select an entry's Select button and click Delete to remove the entry.

6.8 ACL Rule Screen

An ACL (Access Control List) profile allows the system to classify and allow or deny upstream traffic.

- Use the **Profile > ACL** screen ([Section 13.2 on page 167](#)) to configure the ACL profiles.
- Click **ACL > Rule** to apply the ACL profiles to ports.

Figure 81 ACL > Rule

Rule

Interface Slot Port ACL Profile

Apply

Interface Slot Port

Load

Index	ACL Profile Name	Select
1		

Delete **Cancel**

Index	State	Card Type	Uptime
1	Active	MSC1002GA	114:48:32
2	Active	VOP1164A-61	114:47:19
3	Active	ALC1132A-51	114:47:44
4	Active	ELC1132A-45	114:47:02
5	Active	VLC1124A-51	114:46:44

The following table describes the labels in this screen.

Table 45 ACL > Rule

LABEL	DESCRIPTION
Interface	Use the drop-down list boxes to select an interface, a line card, and port for which to apply ACL profiles to a port.
Slot	
Port	
ACL Profile	
Apply	Click Apply to save your changes in this screen.

Table 45 ACL > Rule (continued)

LABEL	DESCRIPTION												
Interface Slot Port	Use the drop-down list boxes to select an interface, a line card, and port for which to display the applied ACL profile. Enet: display the ACL profiles applied to MSC ports. DSL: display the ACL profiles applied to DSL ports. FE: display the ACL profiles applied to FE ports. System: display the ACL profile applied system-wide.												
Load	Click Load to display the port's current settings.												
Index	This is the index number of an entry.												
ACL Profile Name	This field displays the ACL profile the system applies to the port.												
Select	Click Select to choose an entry.												
Delete	Click Delete to remove the selected entry.												
Cancel	Click Cancel to begin configuring the screen again.												
Index	This is the slot number of a line card. Click an index to view the ACL profile that the specified slot applies as shown. Figure 82 ACL > Rule > Slot Rule: slot 1 <table><thead><tr><th>Index</th><th>Port</th><th>ACL Profile</th><th>Select</th></tr></thead><tbody><tr><td>1</td><td>system</td><td>ccc</td><td>☐</td></tr><tr><td>2</td><td>system</td><td>ddd</td><td>☐</td></tr></tbody></table> Delete	Index	Port	ACL Profile	Select	1	system	ccc	☐	2	system	ddd	☐
Index	Port	ACL Profile	Select										
1	system	ccc	☐										
2	system	ddd	☐										
State	This field displays the line card's current operational status. Active means the line card is operating normally. init means the IES is initializing the line card. disable means a manager has disabled the line card. inactive means the line card is starting up or is not operating normally.												
Card Type	This field displays the type of a line card.												
Up Time	This field displays how long the line card has been running since the last time it was started.												

CHAPTER 7

Alarm Screens

This chapter describes alarm management.

7.1 Current Alarm Screen

Click **Alarm > Current** to display the screen where you can view current alarms.

Figure 83 Alarm > Current Alarm

The following table describes the labels in this screen.

Table 46 Alarm > Current Alarm

LABEL	DESCRIPTION
Severity	Select an alarm severity level (critical , major , minor , warning or all).
Alarm	Select an alarm category. All specifies every alarm category. eqpt represents equipment alarms. dsl represents Digital Subscriber Line (DSL) alarms. enet represents Ethernet alarms. sys represents system alarms. voip represents alarms related to the VoIP function. fe represents Fast Ethernet alarms.
Condition	Specify an alarm condition.

Table 46 Alarm > Current Alarm (continued)

LABEL	DESCRIPTION
Date (mm/dd/yyyy)	Select the radio button and specify a range of time in the month/day/year format to display the alarms occur during this period only.
Order	Specify the displaying order. forward : oldest entry displayed first reverse : latest entry displayed first
Load	Click Load to display current alarms.
Flush All	Click Flush All to remove all the current alarms.
Flush Selected	Click Flush Selected to remove the selected current alarms.
Index	This is the index number of the alarm.
Alarm	This is the alarm category.
Condition	This is the alarm condition.
Severity	This is the severity level (critical , major , minor , warning or all) of alarms.
Timestamp	This is the time when the alarm occurred.
Source	This is the location where the alarm occurred.
Select	Click Select to choose an entry.
Previous Next	Click Previous or Next to show the preceding or following screen if the information cannot be displayed in one screen.

7.2 History Alarm Screen

Click **Alarm > History** to display the screen where you can view historic alarms.

Figure 84 Alarm > History Alarm

The screenshot shows the 'History Alarm' interface. At the top, there's a title bar 'History Alarm'. Below it, a filter section includes dropdowns for 'Severity' (set to 'All') and 'Alarm' (set to 'All'), a text input for 'Condition', a date range selector (set to '(mm/dd/yyyy)'), and radio buttons for 'Order' (selected 'Forward', 'Reverse' is unselected). Below the filters are 'Load' and 'Flush' buttons. The main area is a table with columns: Index, Alarm, Condition, Severity, Timestamp, and Source. The table contains 7 rows of alarm data. At the bottom, there's a 'Page 1' indicator and 'Previous' and 'Next' navigation buttons.

Index	Alarm	Condition	Severity	Timestamp	Source
1	eqpt	(10011)warm_start DSLAM: System warm-starts	warning	01/04/2016 11:03:53	eqpt
2	eqpt	(10033)it_active DSLAM-3:LT is active	event	01/04/2016 11:04:32	eqpt 3
3	eqpt	(10033)it_active DSLAM-2:LT is active	event	01/04/2016 11:04:48	eqpt 2
4	eqpt	(10033)it_active DSLAM-4:LT is active	event	01/04/2016 11:05:08	eqpt 4
5	eqpt	(10033)it_active DSLAM-5:LT is active	event	01/04/2016 11:05:25	eqpt 5
6	enet	(20005)up ENET1:GbE interface is up, 100/100 Mbps, SN=1	event	01/04/2016 11:06:57	enet 1
7	enet	(20006)down ENET1:GbE interface is down	event	01/04/2016 16:30:45	enet 1

The following table describes the labels in this screen.

Table 47 Alarm > History Alarm

LABEL	DESCRIPTION
Severity	Select an alarm severity level (critical , major , minor , warning or all).
Alarm	Select an alarm category. All specifies every alarm category. eqpt represents equipment alarms. dsl represents Digital Subscriber Line (DSL) alarms. enet represents Ethernet alarms. sys represents system alarms. voip represents alarms related to the VoIP function. fe represents Fast Ethernet alarms.
Condition	Specify an alarm condition.
Date (mm/dd/yyyy)	Select the radio button and specify a range of time in the month/day/year format to display the alarms occur during this period only.
Order	Specify the displaying order. forward : oldest entry displayed first reverse : latest entry displayed first
Load	Click Load to display historic alarms.
Flush	Click Flush to remove all the historic alarms.
Index	This is the index number of the alarm.
Alarm	This is the alarm category.
Condition	This is the alarm condition.
Severity	This is the severity level (critical , major , minor , warning or all) of alarms.
Timestamp	This is the time when the alarm occurred.
Source	This is the location where the alarm occurred.
Previous Next	Click Previous or Next to show the preceding or following screen if the information cannot be displayed in one screen.

7.3 Alarm Input Screens

7.3.1 Alarm Input Screen

Click **Alarm > Input > Alarm Input** to configure names for the external alarm inputs. This makes it easier to identify the source of an alarm.

Figure 85 Alarm > Input > Alarm Input

The following table describes the labels in this screen.

Table 48 Alarm > Input > Alarm Input

LABEL	DESCRIPTION
Index 1-4 Name	Enter 1 to 31 characters for the name of the connected external alarm system.
Apply	Click Apply to save your changes in this screen.
Cancel	Click Cancel to begin configuring the screen again.

7.3.2 CPU Overload Alarm

Click **Alarm > Input > CPU Overload Alarm** to configure the settings for issuing a CPU overload alarm.

Figure 86 Alarm > Input > CPU Overload Alarm

The following table describes the labels in this screen.

Table 49 Alarm > Input > CPU Overload Alarm

LABEL	DESCRIPTION
Analytic Method	Select the method of analyzing CPU usage in monitoring for a CPU overload. continuous: issue a CPU overload alarm if all samples are above the configured Issue Threshold . average: issue a CPU overload alarm if the average of all samples is above the configured Issue Threshold . Clear the CPU overload alarm if the average of all samples is below the configured Clear Threshold .
Issue Threshold	Specify the threshold for issuing an CPU overload alarm.
Clear Threshold	Specify the threshold for clearing an CPU overload alarm.
Sample Seconds	Specify the number of sample seconds used for monitoring for a CPU overload.

Table 49 Alarm > Input > CPU Overload Alarm (continued)

LABEL	DESCRIPTION
Apply	Click Apply to save your changes in this screen.
Cancel	Click Cancel to begin configuring the screen again.

7.3.3 System Suppress

Click **Alarm > Input > System Suppress** to open the following screen. Use this screen to activate or deactivate the system suppress.

Figure 87 Alarm > Alarm Input > System Suppress

The following table describes the labels in this screen.

Table 50 Alarm > Alarm Input > System Suppress

LABEL	DESCRIPTION
Enable System Suppress	Select the check box to suppress all traps except those with the "event" severity level. The IES still records all alarms and syslog (if enabled).
Apply	Click Apply to save your changes in this screen.
Cancel	Click Cancel to begin configuring the screen again.

7.4 Alarm Definition Screen

7.4.1 DSL

Click **Alarm > Definition > DSL** to configure DSL alarm settings.

Figure 88 Alarm > Definition > DSL

DSL

DSL Eqt Sys Enet VoIP FE

No	Condition	SNMP	SYSLOG	Facility	Severity	Type
Select All		☐	☐	local1	event	
1	line_up	☒	☒	local1	event	TC
2	line_down	☒	☒	local1	event	TC
3	ad_perf_lof_thresh	☒	☒	local1	minor	TC
4	ad_perf_los_thresh	☒	☒	local1	minor	TC
5	ad_perf_lpr_thresh	☒	☒	local1	minor	TC
6	ad_perf_es_thresh	☒	☒	local1	minor	TC
7	ad_perf_ses_thresh	☒	☒	local1	minor	TC
8	ad_perf_uas_thresh	☒	☒	local1	minor	TC
9	ad_perf_fec_thresh	☒	☒	local1	minor	TC
10	ad_perf_fecc_thresh	☒	☒	local1	minor	TC
11	ad_perf_cv_thresh	☒	☒	local1	minor	TC
12	ad_atuc_loftrap	☒	☒	local1	minor	SC,CL
13	ad_atuc_lostrap	☒	☒	local1	minor	SC,CL
14	ad_atur_loftrap	☒	☒	local1	minor	SC,CL
15	ad_atur_lostrap	☒	☒	local1	minor	SC,CL
16	ad_atur_lprtrap	☒	☒	local1	minor	SC,CL
17	line_loopguard	☒	☒	local1	minor	SC,CL
18	dsp_download_fail	☒	☒	local1	critical	SC,CL
19	dsp_inoperable	☒	☒	local1	critical	TC
20	ht_port_policer	☒	☒	local1	minor	TC
21	dsl_tx_byte_th	☒	☒	local1	minor	TC
22	dsl_tx_pkt_th	☒	☒	local1	minor	TC
23	dsl_tx_uc_pkt_th	☒	☒	local1	minor	TC
24	dsl_tx_bc_pkt_th	☒	☒	local1	minor	TC
25	dsl_tx_mc_pkt_th	☒	☒	local1	minor	TC
26	dsl_tx_dc_pkt_th	☒	☒	local1	minor	TC
27	dsl_rx_byte_th	☒	☒	local1	minor	TC
28	dsl_rx_pkt_th	☒	☒	local1	minor	TC
29	dsl_rx_uc_pkt_th	☒	☒	local1	minor	TC
30	dsl_rx_bc_pkt_th	☒	☒	local1	minor	TC
31	dsl_rx_mc_pkt_th	☒	☒	local1	minor	TC
32	dsl_rx_dc_pkt_th	☒	☒	local1	minor	TC
33	dsl_gbond_up	☒	☒	local1	event	TC
34	dsl_gbond_down	☒	☒	local1	event	TC
35	dsl_gbond_port_up	☒	☒	local1	event	TC
36	dsl_gbond_port_down	☒	☒	local1	event	TC

Apply Cancel

The following table describes the labels in this screen.

Table 51 Alarm > Definition > DSL

LABEL	DESCRIPTION
No	This is the number of an individual alarm.
Condition	This identifies an individual alarm.
SNMP	Select the check box to have the IES send SNMP traps of the specified alarm condition.

Table 51 Alarm > Definition > DSL (continued)

LABEL	DESCRIPTION
SYSLOG	Select this check box to have the IES send this alarm to a syslog server.
Facility	Select the log facility (local1 ~ local7) to have the IES send a type of alarm to a specific file in the syslog server. Please refer to the documentation of your syslog program for more details.
Severity	Select the severity level from warning , minor , major and critical for the specified alarm condition.
Type	This field displays the alarm type. TC : Only alarm set (no clear) will be issued, and the alarm is only stored in the alarm history after issued. SC,CL : Both alarm set and clear will be issued. Once set, it will be put to current alarm until it is cleared. Both the set and clear events will be stored in the alarm history.
Select All	Select one of these options to automatically select that option for all entries. Clear it to clear that option for all entries. Alternatively, you may select or clear the check boxes for individual entries.
Apply	Click Apply to save your changes in this screen.
Cancel	Click Cancel to begin configuring the screen again.

7.4.2 Equipment

Click **Alarm > Definition > Eqpt** to configure equipment alarm settings.

Figure 89 Alarm > Definition > Eqpt

Eqpt

DSL **Eqpt** Sys Enet VoIP FE

No	Condition	SNMP	SYSLOG	Facility	Severity	Type
Select All		☐	☐	local1	critical	
1	vol_err	☒	☒	local1	critical	SC,CL
2	temp_err	☒	☒	local1	critical	SC,CL
3	fan_err	☒	☒	local1	critical	SC,CL
4	hw_rtc_fail	☒	☒	local1	critical	TC
5	hw_mon_fail	☒	☒	local1	critical	TC
6	cold_start	☒	☒	local1	warning	TC
7	warm_start	☒	☒	local1	warning	TC
8	alm_input1	☒	☒	local1	critical	SC,CL
9	alm_input2	☒	☒	local1	critical	SC,CL
10	alm_input3	☒	☒	local1	critical	SC,CL
11	alm_input4	☒	☒	local1	critical	SC,CL
12	lt_plug_out	☒	☒	local1	major	SC,CL
13	lt_active	☒	☒	local1	event	TC
14	lt_inactive	☒	☒	local1	event	TC
15	lt_disable	☒	☒	local1	warning	TC
16	lt_reset	☒	☒	local1	warning	TC
17	lt_mismatch	☒	☒	local1	minor	SC,CL
18	voip_battery_fail	☒	☒	local1	critical	SC,CL
19	voip_clock_fail	☒	☒	local1	critical	SC,CL

Apply Cancel

The following table describes the labels in this screen.

Table 52 Alarm > Definition > Eqpt

LABEL	DESCRIPTION
No	This is the number of an individual alarm.
Condition	This identifies an individual alarm.
SNMP	Select the check box to have the IES send SNMP traps of the specified alarm condition.
SYSLOG	Select this check box to have the IES send this alarm to a syslog server.
Facility	Select the log facility (local1 ~ local7) to have the IES send a type of alarm to a specific file in the syslog server. Please refer to the documentation of your syslog program for more details.
Severity	Select the severity level from warning , minor , major and critical for the specified alarm condition.
Type	This field displays the alarm type. TC: Only alarm set (no clear) will be issued, and the alarm is only stored in the alarm history after issued. SC,CL: Both alarm set and clear will be issued. Once set, it will be put to current alarm until it is cleared. Both the set and clear events will be stored in the alarm history.

Table 52 Alarm > Definition > Eqpt (continued)

LABEL	DESCRIPTION
Select All	Select one of these options to automatically select that option for all entries. Clear it to clear that option for all entries. Alternatively, you may select or clear the check boxes for individual entries.
Apply	Click Apply to save your changes in this screen.
Cancel	Click Cancel to begin configuring the screen again.

7.4.3 System

Click **Alarm > Definition > Sys** to configure system alarm settings.

Figure 90 Alarm > Definition > Sys

No	Condition	SNMP	SYSLOG	Facility	Severity	Type
Select All		☐	☐	local1	warning	
1	reboot	☒	☒	local1	warning	TC
2	alm_clear	☒	☒	local1	warning	TC
3	login_fail	☒	☒	local1	minor	TC
4	anti_spoofing	☒	☒	local1	minor	TC
5	cpu_overload	☒	☒	local1	minor	SC,CL
6	cfg_upload_fail	☒	☒	local1	warning	TC
7	cfg_reload_fail	☒	☒	local1	warning	TC
8	write_flash_fail	☒	☒	local1	critical	TC
9	invalid_mfg_data	☒	☒	local1	warning	TC
10	remain_pwr_alert	☒	☒	local1	critical	SC,CL
11	slot_op_pwr_exceed	☒	☒	local1	minor	TC
12	port_op_pwr_exceed	☒	☒	local1	minor	TC
13	card_bat_pwr_exceed	☒	☒	local1	minor	TC
14	rstp_topology_change	☒	☒	local1	event	TC
15	rstp_new_root	☒	☒	local1	event	TC

The following table describes the labels in this screen.

Table 53 Alarm > Definition > Sys

LABEL	DESCRIPTION
No	This is the number of an individual alarm.
Condition	This identifies an individual alarm.
SNMP	Select the check box to have the switch send SNMP traps of the specified alarm condition.
SYSLOG	Select this check box to have the IES send this alarm to a syslog server.
Facility	Select the log facility (local1 ~ local7) to have the IES send a type of alarm to a specific file in the syslog server. Please refer to the documentation of your syslog program for more details.

Table 53 Alarm > Definition > Sys (continued)

LABEL	DESCRIPTION
Severity	Select the severity level from warning , minor , major and critical for the specified alarm condition.
Type	This field displays the alarm type. TC : Only alarm set (no clear) will be issued, and the alarm is only stored in the alarm history after issued. SC,CL : Both alarm set and clear will be issued. Once set, it will be put to current alarm until it is cleared. Both the set and clear events will be stored in the alarm history.
Select All	Select one of these options to automatically select that option for all entries. Clear it to clear that option for all entries. Alternatively, you may select or clear the check boxes for individual entries.
Apply	Click Apply to save your changes in this screen.
Cancel	Click Cancel to begin configuring the screen again.

7.4.4 Ethernet

Click **Alarm > Definition > Enet** to configure Ethernet alarm settings.

Figure 91 Alarm > Definition > Enet

No	Condition	SNMP	SYSLOG	Facility	Severity	Type
Select All		☐	☐	local1	event	
1	up	☒	☒	local1	event	TC
2	down	☒	☒	local1	event	TC
3	ge_tx_byte_th	☒	☒	local1	minor	TC
4	ge_tx_pkt_th	☒	☒	local1	minor	TC
5	ge_tx_bc_pkt_th	☒	☒	local1	minor	TC
6	ge_tx_mc_pkt_th	☒	☒	local1	minor	TC
7	ge_rx_byte_th	☒	☒	local1	minor	TC
8	ge_rx_pkt_th	☒	☒	local1	minor	TC
9	ge_rx_bc_pkt_th	☒	☒	local1	minor	TC
10	ge_rx_mc_pkt_th	☒	☒	local1	minor	TC
11	ge_rx_crc_err_th	☒	☒	local1	minor	TC
12	ge_rx_under_pkt_th	☒	☒	local1	minor	TC
13	ge_rx_over_pkt_th	☒	☒	local1	minor	TC
14	ge_rx_frag_th	☒	☒	local1	minor	TC
15	ge_collision_th	☒	☒	local1	minor	TC
16	ge_pkt64_th	☒	☒	local1	minor	TC
17	ge_pkt65_127_th	☒	☒	local1	minor	TC
18	ge_pkt128_255_th	☒	☒	local1	minor	TC
19	ge_pkt256_511_th	☒	☒	local1	minor	TC
20	ge_pkt512_1023_th	☒	☒	local1	minor	TC
21	ge_pkt1024_1518_th	☒	☒	local1	minor	TC
22	ge_pkt1519_1522_th	☒	☒	local1	minor	TC
23	ge_tx_util_lv1_th	☒	☒	local1	major	SC,CL
24	ge_rx_util_lv1_th	☒	☒	local1	major	SC,CL
25	ge_tx_util_lv2_th	☒	☒	local1	critical	SC,CL
26	ge_rx_util_lv2_th	☒	☒	local1	critical	SC,CL

The following table describes the labels in this screen.

Table 54 Alarm > Definition > Enet

LABEL	DESCRIPTION
No	This is the number of an individual alarm.
Condition	This identifies an individual alarm.
SNMP	Select the check box to have the IES send SNMP traps of the specified alarm condition.
SYSLOG	Select this check box to have the IES send this alarm to a syslog server.
Facility	Select the log facility (local1 ~ local7) to have the IES send a type of alarm to a specific file in the syslog server. Please refer to the documentation of your syslog program for more details.

Table 54 Alarm > Definition > Enet (continued)

LABEL	DESCRIPTION
Severity	Select the severity level from warning , minor , major and critical for the specified alarm condition.
Type	This field displays the alarm type. TC : Only alarm set (no clear) will be issued, and the alarm is only stored in the alarm history after issued. SC,CL : Both alarm set and clear will be issued. Once set, it will be put to current alarm until it is cleared. Both set and clear event will be stored in the alarm history.
Select All	Select one of these options to automatically select that option for all entries. Clear it to clear that option for all entries. Alternatively, you may select or clear the check boxes for individual entries.
Apply	Click Apply to save your changes in this screen.
Cancel	Click Cancel to begin configuring the screen again.

7.4.5 VoIP

Click **Alarm > Definition > VoIP** to configure VoIP alarm settings. The version of the screen depends on whether the IES is using H.248 or SIP firmware.

Figure 92 Alarm > Definition > VoIP (H.248)

VoIP

DSL Eqpt Sys Enet **VoIP** FE

No	Condition	SNMP	SYSLOG	Facility	Severity	Type
Select All		☐	☐			
1	voip_temp_error	☒	☒	local1 ▼	critical ▼	SC,CL
2	voip_dc_power_fail	☒	☒	local1 ▼	critical ▼	SC,CL
3	voip_ac_power_fail	☒	☒	local1 ▼	critical ▼	SC,CL
4	voip_ring_timer_fail	☒	☒	local1 ▼	warning ▼	TC
5	voip_ring_rsce_fail	☒	☒	local1 ▼	warning ▼	TC
6	voip_no_free_dsp_ch	☒	☒	local1 ▼	warning ▼	TC
7	voip_service_up	☒	☒	local1 ▼	event ▼	TC
8	voip_service_down	☒	☒	local1 ▼	event ▼	TC
9	voip_mgc_up	☒	☒	local1 ▼	event ▼	TC
10	voip_mgc_down	☒	☒	local1 ▼	event ▼	TC
11	rtp_elaps_th	☒	☒	local1 ▼	minor ▼	TC
12	rtp_tx_byte_th	☒	☒	local1 ▼	minor ▼	TC
13	rtp_rx_byte_th	☒	☒	local1 ▼	minor ▼	TC
14	rtp_tx_pkt_th	☒	☒	local1 ▼	minor ▼	TC
15	rtp_rx_pkt_th	☒	☒	local1 ▼	minor ▼	TC
16	rtp_tx_los_pkt_th	☒	☒	local1 ▼	minor ▼	TC
17	rtp_rx_los_pkt_th	☒	☒	local1 ▼	minor ▼	TC

Apply Cancel

Figure 93 Alarm > Definition > VoIP (SIP)

VoIP

DSL Eqpt Sys Enet **VoIP** FE

No	Condition	SNMP	SYSLOG	Facility	Severity	Type
Select All		☐	☐	local1	critical	
1	voip_temp_error	☒	☒	local1	critical	SC,CL
2	voip_dc_power_fail	☒	☒	local1	critical	SC,CL
3	voip_ac_power_fail	☒	☒	local1	critical	SC,CL
4	voip_ring_timer_fail	☒	☒	local1	warning	TC
5	voip_ring_rsrce_fail	☒	☒	local1	warning	TC
6	voip_no_free_dsp_ch	☒	☒	local1	warning	TC
7	voip_service_up	☒	☒	local1	event	TC
8	voip_service_down	☒	☒	local1	event	TC
9	voip_sip_svr_up	☒	☒	local1	event	TC
10	voip_sip_svr_down	☒	☒	local1	event	TC
11	rtp_elaps_th	☒	☒	local1	minor	TC
12	rtp_tx_byte_th	☒	☒	local1	minor	TC
13	rtp_rx_byte_th	☒	☒	local1	minor	TC
14	rtp_tx_pkt_th	☒	☒	local1	minor	TC
15	rtp_rx_pkt_th	☒	☒	local1	minor	TC
16	rtp_tx_los_pkt_th	☒	☒	local1	minor	TC
17	rtp_rx_los_pkt_th	☒	☒	local1	minor	TC

Apply Cancel

The following table describes the labels in this screen.

Table 55 Alarm > Definition > VoIP

LABEL	DESCRIPTION
No	This is the number of an individual alarm.
Condition	This identifies an individual alarm.
SNMP	Select the check box to have the IES send SNMP traps of the specified alarm condition.
SYSLOG	Select this check box to have the IES send this alarm to a syslog server.
Facility	Select the log facility (local1 ~ local7) to have the IES send a type of alarm to a specific file in the syslog server. Please refer to the documentation of your syslog program for more details.
Severity	Select the severity level from warning , minor , major and critical for the specified alarm condition.
Type	This field displays the alarm type. TC: Only alarm set (no clear) will be issued, and the alarm is only stored in the alarm history after issued. SC,CL: Both alarm set and clear will be issued. Once set, it will be put to current alarm until it is cleared. Both set and clear event will be stored in the alarm history.
Select All	Select one of these options to automatically select that option for all entries. Clear it to clear that option for all entries. Alternatively, you may select or clear the check boxes for individual entries.

Table 55 Alarm > Definition > VoIP (continued)

LABEL	DESCRIPTION
Apply	Click Apply to save your changes in this screen.
Cancel	Click Cancel to begin configuring the screen again.

7.4.6 FE

Click **Alarm > Definition > FE** to configure Fast Ethernet alarm settings.

Figure 94 Alarm > Definition > FE

The screenshot shows the 'FE' configuration screen for alarms. At the top, there are tabs for DSL, Eqpt, Sys, Enet, VoIP, and FE, with 'FE' being the active tab. Below the tabs is a table with 7 columns: No, Condition, SNMP, SYSLOG, Facility, Severity, and Type. The table contains 21 rows of alarm conditions. Each row has a checkbox for SNMP and SYSLOG, a dropdown for Facility (all set to 'local1'), a dropdown for Severity (most set to 'minor', two to 'event'), and a Type (all set to 'TC').

No	Condition	SNMP	SYSLOG	Facility	Severity	Type
Select All		☐	☐			
1	fe_tx_byte_th	☒	☒	local1	minor	TC
2	fe_tx_pkt_th	☒	☒	local1	minor	TC
3	fe_tx_bc_pkt_th	☒	☒	local1	minor	TC
4	fe_tx_mc_pkt_th	☒	☒	local1	minor	TC
5	fe_rx_byte_th	☒	☒	local1	minor	TC
6	fe_rx_pkt_th	☒	☒	local1	minor	TC
7	fe_rx_bc_pkt_th	☒	☒	local1	minor	TC
8	fe_rx_mc_pkt_th	☒	☒	local1	minor	TC
9	fe_rx_crc_err_th	☒	☒	local1	minor	TC
10	fe_rx_under_pkt_th	☒	☒	local1	minor	TC
11	fe_rx_over_pkt_th	☒	☒	local1	minor	TC
12	fe_rx_frag_th	☒	☒	local1	minor	TC
13	fe_collision_th	☒	☒	local1	minor	TC
14	fe_pkt64_th	☒	☒	local1	minor	TC
15	fe_pkt65_127_th	☒	☒	local1	minor	TC
16	fe_pkt128_255_th	☒	☒	local1	minor	TC
17	fe_pkt256_511_th	☒	☒	local1	minor	TC
18	fe_pkt512_1023_th	☒	☒	local1	minor	TC
19	fe_pkt1024_1518_th	☒	☒	local1	minor	TC
20	fe_up	☒	☒	local1	event	TC
21	fe_down	☒	☒	local1	event	TC

The following table describes the labels in this screen.

Table 56 Alarm > Definition > FE

LABEL	DESCRIPTION
No	This is the number of an individual alarm.
Condition	This identifies an individual alarm.
SNMP	Select the check box to have the IES send SNMP traps of the specified alarm condition.
SYSLOG	Select this check box to have the IES send this alarm to a syslog server.

Table 56 Alarm > Definition > FE (continued)

LABEL	DESCRIPTION
Facility	Select the log facility (local1 ~ local7) to have the IES send a type of alarm to a specific file in the syslog server. Please refer to the documentation of your syslog program for more details.
Severity	Select the severity level from warning , minor , major and critical for the specified alarm condition.
Type	This field displays the alarm type. TC: Only alarm set (no clear) will be issued, and the alarm is only stored in the alarm history after issued. SC,CL: Both alarm set and clear will be issued. Once set, it will be put to current alarm until it is cleared. Both set and clear event will be stored in the alarm history.
Select All	Select one of these options to automatically select that option for all entries. Clear it to clear that option for all entries. Alternatively, you may select or clear the check boxes for individual entries.
Apply	Click Apply to save your changes in this screen.
Cancel	Click Cancel to begin configuring the screen again.

CHAPTER 8

Diagnostic Screens

This chapter explains the **Diagnostic** screens.

8.1 DELT Test Screen

Click **Diagnostic > DELT** to display this screen. Use this screen to perform the DSL Dual End Loop Test (DELT) on an ADSL2, ADSL2+ or VDSL port. A DELT provides details about the line condition. The subscriber device must also support DELT in order to perform this. See ITU-T G933.2 for more information. This feature is applicable for DSL line cards only.

Figure 95 Diagnostic > DELT

DELT

Slot 3 Port 1 Items set_DELT

Apply

The following table describes the labels in this screen.

Table 57 Diagnostic > DELT

LABEL	DESCRIPTION
Slot, Port	Select the DSL port to perform loop diagnostics upon. The port must have a connection. It takes about one minute for the loop diagnostics to finish.
Items	set_DELT: Starts DELT test on a specified port. get_result: Displays the basic loop diagnostic mode test results. get_hlin: Displays the channel characteristics function represented in linear format by a scale factor and a complex number. These are the maximum upstream and downstream scale factors used in producing the channel characteristics function. get_hlog: Displays channel characteristics. The format provides magnitude values in a logarithmic scale. This can be used in analyzing the physical condition of the ADSL or VDSL line. get_qln: Displays the Quiet Line Noise for a DMT tone is the rms (root mean square) level of the noise present on the line, when no ADSL or VDSL signals are present. It is measured in dBm/Hz. The QLN can be used in analyzing crosstalk. get_snr: Displays the upstream and downstream Signal to Noise Ratio (in dB). A DMT tone's SNR is the ratio between the received signal power and the received noise power. The SNR can be used in analyzing time dependent changes in crosstalk levels and line attenuation (such as those caused by temperature variations and moisture).
Apply	Click Apply to save your changes and to display diagnostics results in this screen.

8.2 IP Ping Screen

Click **Diagnostic > IP Ping** to display this screen. Use this screen to ping IP addresses.

Figure 96 Diagnostic > IP Ping

The following table describes the labels in this screen.

Table 58 Diagnostic > IP Ping

LABEL	DESCRIPTION
IPv4/IPv6 Address	Type the IP address of a device that you want to ping in order to test a connection.
Bytes	Specify the ping packet size.
Times	Specify the number of times that you want to ping the IP address.
IPv4/IPv6 Option	Select which interface you want to send ping packets through.
IPv4/IPv6 Ping	Click IPv4 or IPv6 Ping to ping the IP address that you specified.

8.3 MLT Screen

Use this screen to perform a variety of standard Metallic Line Tests (MLT) on the lines connected to VoIP ports. Click **Diagnostic > MLT** to display the following screen. The version of the screen depends on whether the IES is using H.248 or SIP firmware.

Figure 97 Diagnostic > MLT (H.248)

Figure 98 Diagnostic > MLT (SIP)

The following table describes the labels in this screen.

Table 59 Diagnostic > MLT

LABEL	DESCRIPTION
Slot, Port	Use the Slot and Port drop-down list boxes to select the port on an active VoIP line card you want to configure.
Termination-Id	This displays when using H.248 firmware. Type an existing termination ID.
Tel	This displays when using SIP firmware. Type an existing telephone number.
Account	This displays when using SIP firmware. Type an existing account name.

Table 59 Diagnostic > MLT

LABEL	DESCRIPTION
Option	Select which test to perform on the line. all: perform all the MLT tests vac: test the line's AC voltage only vdc: test the line's DC voltage only rload: test the line's load resistance only riso: test the line's isolation resistance only cap: test the line's capacitance only ren: test the line's ringer equivalent number only ring: test the line's ring voltage only metering: test the line's metering voltage only dialtone: test the line's dialtone only digit: test if the line circuit accepts dialed digits and switches the call to its destination roh: test if the receiver is off hook only loop: test loop condition including feeding voltage battery high and low, loop resistance, loop current, and voltage between TIP/RING rrev: test loop condition in battery reversal condition
Force	Select Enable to perform the tests immediately even if the port is in use. If you don't need the port to perform the tests immediately, then select Disable.
Set MLT	Click Set MLT to save your changes in this screen.
Get MLT Data	Click Get MLT Data to see the results of the latest MLT test performed on the specified line card and port.

8.4 SELT Test Screen

Click **Diagnostic > SELT** to display this screen. Use this screen to perform a SELT (Single End Loop Test) on a port to check the distance to the subscriber's location. Not all line cards support the SELT test.

Note: The port must have an open loop. There cannot be a DSL device, phone, fax machine or other device connected to the subscriber's end of the telephone line.

Figure 99 Diagnostic > SELT

SELT

Slot 3 Port 1

Set SELT Port Get SELT Data

The following table describes the labels in this screen.

Table 60 Diagnostic > SELT

LABEL	DESCRIPTION
Slot Port	Select slot and port numbers from the Slot (not all cards support the SELT test) and Port drop-down list boxes.
Set SELT Port	Click Set SELT Port to perform a Single End Loop Test (SELT) on the specified port. This test checks the distance to the subscriber's location.
Get SELT Data	The SELT takes at least fifteen seconds. To check the status of the SELT or to look at the results when the SELT is complete, select a port number from the Port drop-down list box and click Get SELT Data . The results tell you what gauge of telephone wire is connected to the port and the approximate length of the line.

CHAPTER 9

Line Card

This chapter explains how to enable, disable, reset, or display status information about line cards.

9.1 Line Card

Click **Line Card** > **Line Card** to activate, reset, or display line cards' status.

Figure 100 Line Card > Line Card

ID	State	Card Type	Provision Type	Uptime	Heat	Vol	Mon
1	Active	MSC1002GA	-	5:16:32:58	-	-	-
2	Active	VOP1164A-61	VOP1164A-61	5:16:31:45	-	-	-
3	Active	ALC1132A-51	ALC1132A-51	5:16:32:10	-	-	-
4	Active	ELC1132A-45	ELC1132A-45	5:16:31:28	-	-	-
5	Active	VLC1124A-51	VLC1124A-51	5:16:31:10	-	-	-

The following table describes the labels in this screen.

Table 61 Line Card > Line Card

LABEL	DESCRIPTION
Lcman	Use this column to enable, disable, or reset the line card on the specified slot.
Action Slot	
Apply	Click Apply to save your changes.
Provision	Use this column to provision the specified slot for a type of line card.
Type Slot	alc : card type ADSL vlc : card type VDSL vop : card type VoIP lef : card type Fast Ethernet

Table 61 Line Card > Line Card (continued)

LABEL	DESCRIPTION
Apply	Click Apply to save your changes.
ID	This column lists the slot numbers of the cards.
State	This field displays the line card's current operational status. active means the line card is operating normally. init means the IES is initializing the line card. disable means a manager has disabled the line card. inactive means the line card is starting up or is not operating normally.
Card Type	This field displays the type of a card.
Provision Type	This field displays the provision type of a slot.
Uptime	This field displays how long the card has been running since the last time it was started.
Heat	This field indicates whether the temperature of the line card is too high.
Vol	This field indicates whether the voltage on the line card is out of the tolerance range.
Mon	This field indicates if there is any abnormal voltage or temperature value.

CHAPTER 10

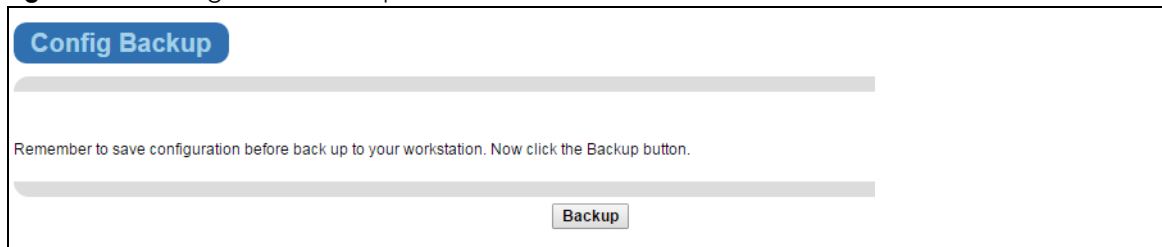
Maintenance Screens

This chapter explains how to use the maintenance screens.

10.1 Configuration Backup Screen

Click **Maintenance** > **Config Backup** to open the following screen. Use this screen to back up your system configuration. This allows you to create various “snap shots” of your device from which you may restore at a later date.

Figure 101 Configuration Backup



- 1 Click **Backup** to save your device's configuration to your computer.
- 2 In the **Save As** screen, choose a location to save the file on your computer from the **Save in** drop-down list box and type a descriptive name for it in the **File name** list box. Click **Save** to save the configuration file to your computer.

Note: You can change the “.dat” file to a “.txt” file and still upload it to the system. See the chapters on commands to edit the configuration text file.

10.2 Configuration Restore Screen

Click **Maintenance** > **Config Restore** to open the following screen. Use this screen to load a configuration file from your computer to the system.

Figure 102 Configuration Restore

Config Restore

To restore the device's configuration from a file, browse to the location of the configuration file and click Restore button.
Restoring a configuration file will reboot system automatically!

File Path : No file chosen

Click **Choose File** to display a **Choose File** screen from which you can locate it. After you have specified the file, click **Restore**. "conf-0" is the name of the configuration file on the system, so your backup configuration file is automatically renamed when you restore using this screen.

10.3 Configuration Reset Screen

Click **Maintenance** > **Config Reset** to open the following screen. Use this screen to clear all system configuration information that you have configured and return to the factory defaults.

Figure 103 Configuration Reset

Config Reset

This page allows you to reset the device's current configuration to default setting. After resetting the device, you need to re-login. Now click the Reset button.

Click **Reset** to return the system to the factory default settings.

10.4 Firmware Upgrade Screen

Click **Maintenance** > **Firmware Upgrade** to open the following screen. Use this screen to view your current firmware version number and upload firmware to cards in the system. Make sure you have downloaded (and unzipped) the correct model firmware and version to your computer before uploading to the card.

Be sure to upload the correct model firmware as uploading the wrong model firmware may damage a card.

Figure 104 FW Upgrade

FW Upgrade

Current Image	ras-0
Boot Image	ras-0 (V3.60(ABIZ.0)b2) ▼
File Path :	Choose File No file chosen

The IES supports dual firmware images, ras-0 and ras-1. You can switch them from one to the other by selecting the **Boot Image**. The system doesn't reboot after it completes a firmware upgrade.

Click **Browse...** in the **File Path** field to select the firmware file you wish to upload. The selected file's name will display on this screen. After you have specified the file, click **Upgrade**.

10.5 Reboot Screen

Click **Maintenance > Reboot** to open the following screen. Use this screen to restart the system without physically turning the power off.

Figure 105 Reboot

Reboot

This page allows you to reboot the system. Now click the Reboot button.

Boot Image: ras-0 (V3.60(ABIZ.0)b2) ▼

Current Image: ras-0

Scheduled Latency: 0 (0 or 5 ~ 86400 in seconds)

Reboot

The IES supports dual firmware images, ras-0 and ras-1. You can switch them from one to the other by selecting the **Boot Image**. Then, click the **Reboot** button to return the system to the configuration that was last saved to nonvolatile memory.

Use the **Scheduled Latency** field if you want to set a delay before the IES restarts. The IES counts down the time till the restart in the **Scheduled Latency** field. Click **Cancel Reboot** if you want to stop the IES from restarting.

Figure 106 Reboot

Reboot

This page allows you to reboot the system. Now click the Reboot button.

Boot Image: ras-1 (V3.60(ABJK.0)b2) ▼

Current Image: ras-1

Scheduled Latency: 27 (0 or 5 ~ 86400 in seconds)

Cancel Reboot

CHAPTER 11

Multicast Screens

This chapter describes the **Multicast** screens.

11.1 IGMP Introduction

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender to 1 recipient) or Broadcast (1 sender to everybody on the network). Multicast delivers IP packets to just a group of hosts on the network.

IGMP (Internet Group Management Protocol) is a network-layer protocol used to establish membership in a multicast group - it is not used to carry user data. Refer to RFCs 1112, 2236 and 3376 for information on IGMP versions 1, 2, and 3 respectively.

11.1.1 IP Multicast Addresses

In IPv4, a multicast address allows a device to send packets to a specific group of hosts (multicast group) in a different sub-network. A multicast IP address represents a traffic receiving group, not individual receiving devices. IP addresses in the Class D range (224.0.0.0 to 239.255.255.255) are used for IP multicasting. Certain IP multicast numbers are reserved by IANA for special purposes (see the IANA web site for more information).

In IPv6, multicast addresses provide the same functionality as IPv4 broadcast addresses. Broadcasting is not supported in IPv6.

11.1.2 IGMP Snooping

A layer-2 switch can passively snoop on IGMP Query, Report and Leave (IGMP versions 2 and 3) packets transferred between IP multicast routers/switches and IP multicast hosts to learn the IP multicast group membership. It checks IGMP packets passing through it, picks out the group registration information, and configures multicasting accordingly. IGMP snooping allows the system to learn multicast groups without you having to manually configure them.

The system forwards multicast traffic destined for multicast groups (that it has learned from IGMP snooping or that you have manually configured) to ports that are members of that group. The system discards multicast traffic destined for multicast groups that it does not know. IGMP snooping generates no additional network traffic, allowing you to significantly reduce multicast traffic passing through your device.

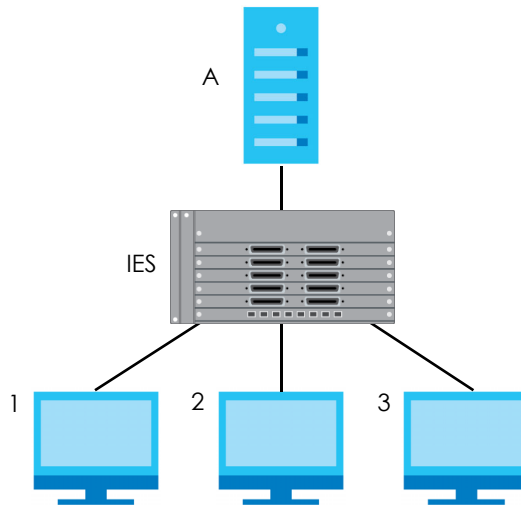
11.1.3 IGMP Proxy

To allow better network performance, you can use IGMP proxy instead of a multicast routing protocol in a simple tree network topology.

In IGMP proxy, an upstream interface is the port that is closer to the source (or the root of the multicast tree) and is able to receive multicast traffic. There should only be one upstream interface (also known as the query port) on the system to limit bandwidth use. A downstream interface is a port that connects to a host (such as a computer). A query VLAN determines which ports are downstream interfaces.

The following figure shows a network example where A is the multicast source while computers 1, 2 and 3 are the receivers. In the figure A is connected to the upstream interface and 1, 2 and 3 are connected to the downstream interface.

Figure 107 IGMP Proxy Network Example



The system will not respond to IGMP join and leave messages on the upstream interface. The system only responds to IGMP query messages on the upstream interface. The system sends IGMP query messages to the hosts that are members of the query VLAN.

The system only sends an IGMP leave messages via the upstream interface when the last host leaves a multicast group.

One of the Ethernet ports acts as the upstream interface. By default, the DSL ports are set as the downstream interfaces.

Note: The switch does not allow a subscriber port to send multicast traffic (except static multicast traffic) to an uplink port. Only the uplink port can forward multicast traffic to the subscriber ports.

11.1.4 IGMP Snooping and Proxy Note

The IES acts as an IGMPv3 client host for an edge IGMPv3 multicast router and as a IGMPv2/v3 router for IGMPv2/v3 client hosts (subscribers). The IES can recognize IGMPv3 protocol messages and forward them towards the IGMP multicast router. It does not support full-featured IGMPv3 functions like source IP address control specified in RFC 3376.

11.1.5 IGMP Fast Leave

When a host leaves a multicast group (224.1.1.1), it sends an IGMP leave message to inform all routers (224.0.0.2) in the multicast group. When a router receives the leave message, it sends a specific query message to all multicast group (224.1.1.1) members to check if any other hosts are still in the group. Then the router deletes the host's information.

With the IGMP fast leave feature enabled, the router (DSLAM) removes the host's information from the group member list once it receives a leave message from a host and the fast leave timer expires.

11.1.6 Multicast Listener Discovery

The Multicast Listener Discovery (MLD) protocol (defined in RFC 2710) is derived from IPv4's Internet Group Management Protocol version 2 (IGMPv2). MLD uses ICMPv6 message types, rather than IGMP message types. MLDv1 is equivalent to IGMPv2 and MLDv2 is equivalent to IGMPv3.

- MLD allows an IPv6 switch or router to discover the presence of MLD hosts who wish to receive multicast packets and the IP addresses of multicast groups the hosts want to join on its network.
- MLD snooping and MLD proxy are analogous to IGMP snooping and IGMP proxy in IPv4.
- MLD filtering controls which multicast groups a port can join.
- An MLD Report message is equivalent to an IGMP Report message, and a MLD Done message is equivalent to an IGMP Leave message.

11.2 IGMP Setup Screens

11.2.1 IGMP Setup Screen

Click **Multicast > IGMP > IGMP Setup** to display the screen shown next. Use this screen to configure your IGMP settings.

Figure 108 Multicast > IGMP > IGMP Setup

The screenshot shows the 'IGMP-MLD Setup' window with three tabs: 'IGMP Setup' (selected), 'Port Setup', and 'Port MVLAN Setup'. The 'IGMP Setup' tab contains the following configuration options:

- Mode:** A dropdown menu set to 'disable'.
- Version:** A dropdown menu set to 'igmpv2'.
- Leave Mode:** A dropdown menu set to 'last-member-query'.
- Pbit:** A dropdown menu set to '7'.
- General Query Timer:** A section with three fields:
 - interval:** A text box with '125' and a range '[10 ~ 300] seconds'.
 - robustness:** A text box with '2' and a range '[1 ~ 5]'.
 - max-response-time:** A text box with '10' and a range '[1 ~ 10] seconds'.
- Last Member Query Timer:** A section with two fields:
 - interval:** A text box with '1000' and a range '[100 ~ 1000] in ms, in step of 100'.
 - robustness:** A text box with '2' and a range '[1 ~ 5]'.

At the bottom of the window are 'Apply' and 'Cancel' buttons.

The following table describes the labels in this screen.

Table 62 Multicast > IGMP > IGMP Setup

LABEL	DESCRIPTION
Mode	Select snooping to have the system passively learn multicast groups. Select proxy to have the system proxy multicast traffic. Select transparent to enable transparent IGMP message transmission. Select proxy-reporting to limit the number of packets being transmitted. Select disable to have the system not use either IGMP proxy or snooping.
Version	Select which version of IGMP you want the system to support. With IPv4, select igmpv2 or igmpv3. If you select IGMPv2, the system discards IGMPv3 packets. This provides better security if none of the devices in the network use IGMPv3. If you select IGMPv3, the system recognizes both IGMPv2 and IGMPv3. With IPv6, select mldv1 or mldv2. If you select MLDv1, the system discards MLDv2 packets. This provides better security if none of the devices in the network use MLDv2. If you select MLDv2, the system recognizes both MLDv1 and MLDv2. igmpv2+mldv1: IGMP version 2 plus MLD version 1 igmpv2+mldv2: IGMP version 2 plus LMD version 1 and version 2 igmpv3+mldv1: IGMP version 2 and version 3 plus MLD version 1 igmpv3+mldv2: IGMP version 2 and version 3 plus MLD version 1 and version 2
Leave Mode	Select the IGMP/MLD leave message handling mode. fast-leave: leave the joined group immediately last-member-query: send a specific query to check if any hosts are still members
Pbit	Select the priority bit in proxy mode.
General Query Timer	
A group will be timeout and removed if the IES doesn't receive any IGMP report for the group in (Robustness)* (Interval) + (Max response time).	
interval	Specify the interval for the IGMP snooping queries sent by the switch.
robustness	Specify the general query robustness. Possible values are 1-5. 5 is the most robust. Robustness is the maximum number of IGMP query intervals that the IES will wait to receive at an IGMP report for an IGMP group.
max-response-time	Specify the general query maximum response time. Possible values are 1-10 in seconds. Maximum response time is the maximum time within which the IGMP client should send out an IGMP report after it receives an IGMP query.
Last Member Query Timer	
interval	Specify the interval for the IGMP specific queries sent by the switch. If fast-leave is disabled, the IES sends out specific queries every (interval) to check if there are any IGMP client request for the group after a leave message.
robustness	Specify the last member query robustness. Possible values are 1-5. 5 is the most robust. When fast-leave is disabled, an IGMP group will be removed if the IES doesn't get any IGMP report for the group in (Robustness)*(Interval) after a leave message is received.
Apply	Click Apply to save your changes in this screen.
Cancel	Click Cancel to begin configuring the screen again.

11.2.2 Port Setup Screen

Click **Multicast > IGMP > Port Setup** to display the screen shown next. Use this screen to configure multicast related settings for a port, including multicast CAC, maximum concurrent joined multicast group and group privilege control.

Figure 109 Multicast > IGMP > Port Setup

The screenshot shows the 'IGMP-MLD Setup' window with the 'Port Setup' tab selected. At the top, there are dropdowns for 'Slot 2' and 'Port 1', followed by a 'Load' button. Below this is a 'CAC control' section with a checkbox. Underneath are input fields for 'Bandwidth' (with a range of [0 ~ 100] in Mbps) and 'Max Group' (with a range of [1 ~ 16]). There is another checkbox for 'Group Privilege'. Below these is a 'Group Privilege Profile' section containing two large list boxes, one labeled 'Apply' and one labeled 'Remove', with '<<' and '>>' buttons between them. At the bottom of the window are 'Apply' and 'Cancel' buttons.

The following table describes the labels in this screen.

Table 63 Multicast > IGMP > Port Setup

LABEL	DESCRIPTION
Slot, Port, Load	Use the Slot and Port drop-down list boxes to select a subscriber port on an active line card. Click Load to display it's settings.
CAC control	Click the check box to enable the Call Admission Control (CAC). CAC Control is used to prevent oversubscription of a VoIP network.
Bandwidth	Specify the maximum multicast bandwidth.
Max Group	Specify the maximum group counts on the specified DSL port.
Group Privilege	Click the check box to enable group privilege checking on the specified DSL port.
Group Privilege Profile	Select groups to be applied or removed on the specified DSL port. Go to Section 11.3 on page 128 to configure the group privilege profile.
Apply	Click Apply to save your changes in this screen.
Cancel	Click Cancel to begin configuring the screen again.

11.2.3 Port MVLAN Setup Screen

Click **Multicast > IGMP > Port MVLAN Setup** to display the screen shown next. Use this screen to add line cards' ports into a MVLAN group.

Figure 110 Multicast > IGMP > Port MVLAN Setup

IGMP-MLD Setup

IGMP Setup Port Setup **Port MVLAN Setup**

Slot **3** Port **1** **Load**

Index	MVLAN	Type	uni-vid	Select
Delete				

MVLAN **None**

Type **None**

uni-vid **[1 ~ 4093]**

Apply **Cancel**

ID	State	Card Type	Uptime
1	Active	MSC1002GA	136:51:53
2	Active	VOP1164A-61	136:50:40
3	Active	ALC1132A-51	136:51:05
4	Active	ELC1132A-45	136:50:23
5	Active	VLC1124A-51	136:50:05

The following table describes the labels in this screen.

Table 64 Multicast > IGMP > Port MVLAN Setup

LABEL	DESCRIPTION
Slot, Port, Load	Use the Slot and Port drop-down list boxes to select a subscriber port on an active line card. Click Load to display it's settings.
Index	This is the number of the port MVLAN entry.
MVLAN	This displays the port's MVLAN ID.
Type	This displays the type of the port's MVLAN.
uni-vid	This displays the uni-VLAN's ID.
Select	Click Select to choose a port MVLAN entry.
Delete	Click Delete to remove a port MVLAN entry.
MVLAN	Select an existing MVLAN to add in the specified DSL port.
Type	Select the type (none , transparent , uni-vlan , untag) of the MVLAN.
uni-vid	Specify the uni-VLAN's ID.
Apply	Click Apply to save your changes in this screen.
Cancel	Click Cancel to begin configuring the screen again.
ID	This is the slot number of a line card. Click an ID to view the MVLAN settings of ports on the specified slot. Interface MVLAN setup slot 5 Index Port MVLAN Type uni-vid Select select All ☐ Delete

Table 64 Multicast > IGMP > Port MVLAN Setup (continued)

LABEL	DESCRIPTION
State	This field displays the line card's current operational status. Active means the line card is operating normally. init means the IES is initializing the line card. disable means a manager has disabled the line card. inactive means the line card is starting up or is not operating normally.
Card Type	This field displays the type of a line card.
Uptime	This field displays how long the card has been running since the last time it was started.

11.3 IGMP Privilege Profile Screen

Click **Multicast > IGMP Privilege Profile** to display the screen shown next. Use this screen to configure IGMP profiles to determine whether IGMP packets should be discarded or transmitted to the IGMP group.

Figure 111 Multicast > IGMP Privilege Profile

The following table describes the labels in this screen.

Table 65 Multicast > IGMP Privilege Profile

LABEL	DESCRIPTION
Profile Name	Enter the name for a group privilege profile.
Index	Specify the specified group privilege profile's entry.
Active	Click the check box to enable the specified group privilege profile.
Bandwidth	Specify the channel bandwidth for the IGMP group.

Table 65 Multicast > IGMP Privilege Profile (continued)

LABEL	DESCRIPTION
Group Range	
Start Address	Type the start and end IP address to specify the group range.
End Address	
Privilege	Select the privilege of the group. forbid: the IGMP profile denies access to the group. preview: the IGMP profile allows preview to the group. • Length: Specify the lifetime of preview entries in seconds. • Interval: Specify the number of seconds to wait before the device can accept a port's Join request to this group again after the last Join request expired. • Count: Specify the total number of times a port can join this group. Once it reaches this count number, the device refuses the port's Join request to this group until this count number is reset. • Reset: Specify the number of seconds to wait before the device resets the Count number. permit: the IGMP profile allows access to the group.
Apply	Click Apply to save your changes in this screen.
New	Click New to set the screen to configure a new entry.
Cancel	Click Cancel to begin configuring the screen again.
Index	This is the number of the privilege profile's entry.
Name	This displays the profile's name.
Select	Select the radio button of a privilege profile's entry.
Modify	Click Modify to edit the profile's parameters.
Delete	Click Delete to remove the specified entry.

11.4 IGMP Status Screens

11.4.1 IGMP Status

Click **Multicast > IGMP Status > IGMP Status** to display the screen shown next. This screen displays IGMP status and statistics for the whole system and per multicast group.

Figure 112 Multicast > IGMP Status > IGMP Status

The following table describes the labels in this screen.

Table 66 Multicast > IGMP Status > IGMP Status

LABEL	DESCRIPTION
Refresh	Click this button to refresh the statistics.
Current Multicast Group Count	This displays the number of the current IGMP groups.
Rx / Tx	
Query	This displays the number of IGMP query packets received and transmitted.
Report	This displays the number of IGMP report packets received and transmitted.
Flush	Click Flush to remove the statistics.
IGMP / MLD	
Uplink in Older Version Compatible Mode	If the IGMP/MLD version is configured as IGMPv3 or MLDv2, this field displays whether the uplink port is in IGMPv2 or MLDv1.
Total	This field displays the total number of joined multicast groups.
Index	This is the number of the MVLAN group entry.
MVLAN	This displays the MVLAN ID.
Group Addr	This displays the IP address of the MVLAN group.
Group Member Count	This displays the number of members of the MVLAN group.
New Joined Member Count	This displays the number of new members of the MVLAN group.
Left Member Count	This displays the number of members left of the MVLAN group.
Joined Port	This displays the number of ports that join the MVLAN group.

Table 66 Multicast > IGMP Status > IGMP Status (continued)

LABEL	DESCRIPTION
Previous	Click this button to go to the previous page.
Next	Click this button to go to the next page.
Go to Page	Select the specified page you want to go to.

11.4.2 IGMP Port Group

Click **Multicast > IGMP Status > IGMP Port Group** to display the screen shown next. This screen displays port status for multicast function.

Figure 113 Multicast > IGMP Status > IGMP Port Group

The following table describes the labels in this screen.

Table 67 Multicast > IGMP Status > IGMP Port Group

LABEL	DESCRIPTION
Port	Select Enet to select an MSC Gigabit Ethernet port or use the drop-down list boxes to select a DSL or FE port on a line card.
Refresh	Click this button to refresh the statistics.
IGMP / MLD	
In Older Version Compatible Mode	If the IGMP/MLD version is configured as IGMPv3 or MLDv2, this field displays whether the port is in IGMPv2 or MLDv1.
Total	This field displays the total number of multicast groups the specified port has joined.
Index	This is the number of the MVLAN group entry.
MVLAN	This displays the MVLAN ID.
Group Addr	This displays the IP address of the MVLAN group.
Create Time	This displays when the group is created.
Bandwidth	This displays the group's bandwidth.
Privilege	This displays the group's privilege.
State	This displays the group's current status.
Previous	Click this button to go to the previous page.

Table 67 Multicast > IGMP Status > IGMP Port Group (continued)

LABEL	DESCRIPTION
Next	Click this button to go to the next page.
Go to Page	Select the specified page you want to go to.

11.4.3 IGMP Port Statistics

Click **Multicast > IGMP Status > IGMP Port Statistics** to display the screen shown next. This screen displays port and group statistics.

Figure 114 Multicast > IGMP Status > IGMP Port Statistics

IGMP Port Statistics

IGMP Status | IGMP Port Group | **IGMP Port Statistics** | IGMP Port Log

Port: ☐ Enet 1 ☒ Slot 2 Port 1

Current Group Count	0		
Create Channel Group Success	0	Create Channel Group Fail	0
Remove Channel Group Leave	0	Remove Channel Group Timeout	0
Query Rx	0	Query Tx	0
Report Rx	0	Report Tx	0

IGMP

Query			
General Query IGMPv2	0	General Query IGMPv3	0
Specific Query IGMPv2	0	Specific Query IGMPv3	0
IGMP Drop	0		
Report			
IGMPv2 Join	0	IGMPv2 Leave	0
IGMPv3	0	Drop	0

MLD

Query			
General Query MLDv1	-	General Query Mldv2	-
Specific Query MLDv1	-	Specific Query MLDv2	-
MLD Drop	-		
Report			
MLDv1 Join	-	MLDv1 Leave	-
MLDv2	-	Drop	-

Total: 0

Index	Group Addr	Privilege	Event	Log Time	J/L counter
Page 0 of 0					

The following table describes the labels in this screen.

Table 68 Multicast > IGMP Status > IGMP Statistics

LABEL	DESCRIPTION
Port	Select Enet to select an MSC Gigabit Ethernet port or use the drop-down list boxes to select a DSL or FE port on a line card.
Refresh	Click this button to refresh the statistics.
Flush	Click this button to remove all the statistics.
Current Group Count	This displays the current number of port groups.
Create Channel Group Success	This field displays the number of groups successfully created.
Create Channel Group Fail	This field displays the number of groups that failed to be created.
Remove Channel Group Leave	This field displays the number of groups removed due to leave messages received.
Remove Channel Group Timeout	This field displays the number of groups removed due to life timeout.
Query Rx	This displays the number of query packets the specified port has received.
Query Tx	This displays the number of query packets the specified port has transmitted.
Report Rx	This displays the number of report packets the specified port has received.
Report Tx	This displays the number of report packets the specified port has transmitted.
IGMP-Query	
General Query IGMP v2	This displays the number of IGMP v2 general query packets.
General Query IGMP v3	This displays the number of IGMP v3 general query packets.
Specific Query IGMP v2	This displays the number of IGMP v2 specific query packets.
Specific Query IGMP v3	This displays the number of IGMP v3 specific query packets.
IGMP Drop	This displays the number of IGMP packets that are dropped.
IGMP-Report	
IGMP v2 Join	This displays the number of IGMP v2 groups the specified port includes.
IGMP v2 Leave	This displays the number of IGMP v2 groups that has left the specified port.
IGMP v3	This displays the number of IGMP v3 groups the specified port includes.
Drop	This displays the number of IGMP packets that are dropped.
MLD Query	
General Query MLD v1	This displays the number of MLD v1 general query packets.
General Query MLD v2	This displays the number of MLD v2 general query packets.
Specific Query MLD v1	This displays the number of MLD v1 specific query packets.
Specific Query MLD v2	This displays the number of MLD v2 specific query packets.

Table 68 Multicast > IGMP Status > IGMP Statistics (continued)

LABEL	DESCRIPTION
MLD Drop	This displays the number of MLD packets that are dropped.
MLD-Report	
MLD v1 Join	This displays the number of MLD v1 groups the specified port includes.
MLD v1 Leave	This displays the number of MLD v1 groups that has left the specified port.
MLD v2	This displays the number of MLD v2 groups the specified port includes.
Drop	This displays the number of MLD packets that are dropped.
Total	This displays the total number of groups a port joins.
Index	This is the number of the port group entry.
Group Addr	This displays the IP address of the specified port group.
Privilege	This displays the port group's privilege.
Event	This displays the most recent event.
Log Time	This displays the log time of the last logged event.
J/L counter	This displays the total number of join and leave messages.
Previous	Click this button to go to the previous page.
Next	Click this button to go to the next page.
Go to Page	Select the specified page you want to go to.

11.4.4 IGMP Port Log

Click **Multicast > IGMP Status > IGMP Port Log** to display the screen shown next. This screen displays the IGMP log information of the specified DSL port.

Figure 115 Multicast > IGMP Status > IGMP Port Log

The following table describes the labels in this screen.

Table 69 Multicast > IGMP Status > IGMP Port Log

LABEL	DESCRIPTION
Port	Use the drop-down list boxes to select a DSL or FE port on a line card.
Refresh	Click this button to refresh the statistics.
Flush	Click this button to remove all the data.
Total	This displays the number of log events.
Index	This is the number of the log entry.
Time	This displays the time the event happens.

Table 69 Multicast > IGMP Status > IGMP Port Log (continued)

LABEL	DESCRIPTION
Event	This displays the event name.
Group Addr	This displays the IP address of the port group.

11.5 MVLAN Setup Screens

11.5.1 MVLAN Setup Screen

Multicast VLAN allows one single multicast VLAN to be shared among different subscriber VLANs on the network. This improves bandwidth utilization by reducing multicast traffic in the subscriber VLANs and simplifies multicast group management.

Click **Multicast** > **MVLAN** to display the screen shown next. Use this screen to configure MVLAN groups in this screen.

Figure 116 Multicast > MVLAN

The following table describes the labels in this screen.

Table 70 Multicast > MVLAN

LABEL	DESCRIPTION
MVLAN	Enter the VLAN ID (VLAN Identifier) for this MVLAN; the valid range is between 1 and 4093.
tr101-fw	Click the check box to enable transparent forwarding of IGMP/MLD messages on this MVLAN.
Apply	Click Apply to save your changes in this screen.
Cancel	Click Cancel to start configuring the screen again.
Index	This is the number of a MVLAN entry.
MVLAN	This displays the MVLAN ID.
tr101-fw	This displays whether tr101-fw is enabled or not.
Select	Select a MVLAN's Select radio button and click Delete to remove the MVLAN.
Delete	

11.5.2 MVLAN Table Screen

Click **Multicast > MVLAN Table** to display the screen shown next. Use this screen to configure the group ranges for the MVLANs.

Note: The MVLAN table is not editable when **tr101-fw** is specified for the MVLAN.

Figure 117 Multicast > MVLAN Table

The screenshot shows the 'Multicast > MVLAN Table' configuration screen. At the top, there are two tabs: 'MVLAN' and 'MVLAN Table'. Below the tabs, there are two input fields for IP ranges: 'IPv4 range: [224.0.0.0 ~ 239.255.255.255]' and 'IPv6 range: [#00:: ~ ffff:ffff:ffff:ffff:ffff:ffff]'. The main area is a table with columns 'Index', 'Start Address', and 'End Address'. The 'Index' column contains numbers 1 through 16. The 'Start Address' and 'End Address' columns contain input fields. At the bottom, there are 'Apply' and 'Cancel' buttons, and a 'Modify' button below a row of 'Index', 'MVLAN', and 'Select' labels.

The following table describes the labels in this screen.

Table 71 Multicast > MVLAN Table

LABEL	DESCRIPTION
MVLAN	This displays the MVLAN ID.
Index	This is the number of a group entry.
Start / End Address	Type the start and end IP address of the group.
Apply	Click Apply to save your changes in this screen.
Cancel	Click Cancel to start configuring the screen again.
Index	This is the number of a MVLAN entry.

Table 71 Multicast > MVLAN Table (continued)

LABEL	DESCRIPTION
MVLAN	This displays the MVLAN ID.
Select	Select a MVLAN's Select radio button and click Modify to edit the MVLAN.
Modify	

11.6 Static Multicast Screen

Click **Multicast > Static Multicast** to display the screen shown next. Use static multicast to allow incoming frames based on the VID and multicast MAC addresses. This feature can be used in conjunction with IGMP snooping to allow multicast MAC addresses that are not learned by IGMP snooping or IGMP proxy and would otherwise be dropped. Use static multicast to pass routing protocols, such as RIP and OSPF.

Figure 118 Multicast > Static Multicast

Index	State	Card Type	Uptime
1	Active	MSC1002GA	139:06:25
2	Active	VOP1164A-61	139:05:12
3	Active	ALC1132A-51	139:05:37
4	Active	ELC1132A-45	139:04:55
5	Active	VLC1124A-51	139:04:37

The following table describes the related labels in this screen.

Table 72 Multicast > Static Multicast

LABEL	DESCRIPTION
Slot port	Use the Slot and Port drop-down list boxes to select the port on an active line card.
Load	Click Load to save your changes.
Index	The is the number of a multicast group entry.
MAC Address	This displays a static multicast MAC address.
UNI VLAN	This displays the VLAN ID on the specified UNI port.
Select Delete	Select an entry and click Delete to remove the entry.
MAC Address	Type a static multicast MAC address which identifies the multicast group.

Table 72 Multicast > Static Multicast (continued)

LABEL	DESCRIPTION
UNI VLAN	Untag: multicast packets will be forwarded to the specified port without VLAN tag. A VLAN trunk untagged mode must be configured first. Vid: multicast packets with the UNI vid will be forwarded to the specified port with VLAN tag. any VLAN mode that has the UNI vid must be configured first.
Apply	Click Apply to save your changes in this screen.
Cancel	Click Cancel to start configuring the screen again.
Index	This is the slot number of a line card. Click the index number to view the multicast group information of the ports on the specified slot. 
State	This field displays the line card's current operational status. Active means the line card is operating normally. init means the IES is initializing the line card. disable means a manager has disabled the line card. inactive means the line card is starting up or is not operating normally.
Card Type	This field displays the type of a line card.
Uptime	This field displays how long the card has been running since the last time it was started.

CHAPTER 12

Port Setup Screens

This chapter explains how to configure settings for individual subscriber ports. It also covers how to configure permanent virtual circuits.

12.1 Alarm Port Setup Screen

Click **Port > Alarm** to display the screen shown next. Use this screen to set the severity level and profile of alarms to record on the system or specific ports.

Figure 119 Port > Alarm

Index	State	Card Type	Uptime
1	Active	MSC1002GA	139:08:18
2	Active	VOP1164A-61	139:07:05
3	Active	ALC1132A-51	139:07:30
4	Active	ELC1132A-45	139:06:48
5	Active	VLC1124A-51	139:06:30

The following table describes the fields in this screen.

Table 73 Port > Alarm

LABEL	DESCRIPTION
Interface Setup	Select an interface and use the drop-down list boxes to select a port on a line card, and then click Setup to configure the alarm severity and alarm profile.
Index	This is the slot number of a line card.
State	This field displays the line card's current operational status. Active means the line card is operating normally. init means the IES is initializing the line card. disable means a manager has disabled the line card. inactive means the line card is starting up or is not operating normally.
Card Type	This field displays the type of a line card.
Uptime	This field displays how long the card has been running since the last time it was started.

If you select **System** for the interface, the screen is shown as below.

Figure 120 Port > Alarm: System

The following table describes the fields in this screen.

Table 74 Port > Alarm: System

LABEL	DESCRIPTION
Interface	This displays the selected interface.
Load	Click this to display the alarm configuration of the specified port.
Severity	Use the drop-down list to select an alarm severity level. It is the alarm severity threshold that triggers the IES to send out SNMP traps.
Apply	Click Apply to save your changes in this screen.
Cancel	Click Cancel to begin configuring the screen again.

If you select **Enet** for the interface, the screen is shown as below.

Figure 121 Port > Alarm: Enet

The following table describes the fields in this screen.

Table 75 Port > Alarm: Enet

LABEL	DESCRIPTION
Interface	This displays the selected interface.
Load	Click this to display the alarm configuration of the specified port.
Severity	Use the drop-down list to select an alarm severity level. It is the alarm severity threshold that triggers the IES to send out SNMP traps.

Table 75 Port > Alarm: Enet (continued)

LABEL	DESCRIPTION
Alarm Profile	Use the drop-down list to select an Enet alarm profile.
Alarm Utilization Setup	
Sample Seconds	Specify the sample seconds for the following thresholds. Ethernet utilization alarm will be triggered if the utilization surpasses the following thresholds for sample seconds.
rx-level1-threshold	Specify the utilization threshold for RX utilization level 1 alarm.
rx-level2-threshold	Specify the utilization threshold for RX utilization level 2 alarm.
tx-level1-threshold	Specify the utilization threshold for TX utilization level 1 alarm.
tx-level2-threshold	Specify the utilization threshold for TX utilization level 2 alarm.
Apply	Click Apply to save your changes in this screen.
Cancel	Click Cancel to begin configuring the screen again.

Select **DSL**, **FE**, or **VoIP** for the interface to display a screen like the following (DSL shown).

Figure 122 Port > Alarm: DSL

The following table describes the fields in this screen.

Table 76 Port > Alarm: DSL, FE, or VoIP

LABEL	DESCRIPTION
Interface	This displays the selected interface.
Load	Click this to display the alarm configuration of the specified port.
Severity	Use the drop-down list to select an alarm severity level. It is the alarm severity threshold that triggers the IES to send out SNMP traps.
Alarm Profile	Use the drop-down list to select an alarm profile.
Apply	Click Apply to save your changes in this screen.
Cancel	Click Cancel to begin configuring the screen again.

12.2 Port Copy Screen

Click **Port > Copy** to open the following screen. Use this screen to copy all subscriber port settings from one port to other ports.

Figure 123 Port > Copy

The following table describes the fields in this screen.

Table 77 Port > Copy

LABEL	DESCRIPTION
Interface	Select Enet to select an MSC Gigabit Ethernet port. Select DSL , FE , or VoIP to be able to select a port on a line card.
Source	Select the number of a line card's slot and the number of a port on the line card.
Destination	Specify a port on the line card to where you want to copy settings.
Copy	Click this button to copy settings from one port to another.

12.3 Port Default Screen

Click **Port > Default** to open the following screen. Use this screen to reset the subscriber port's settings to the defaults.

Figure 124 Port > Default

The following table describes the fields in this screen.

Table 78 Port > Default

LABEL	DESCRIPTION
Interface	Select Ene t and use the Port field to select an MSC Gigabit Ethernet port. Select DSL , FE , or VoIP and use the Slot and Port fields to select a port on a line card. Use * to select all ports on a line card. Select System to select system-wide interface settings.
Apply	Click Apply to reset the specified port's settings to the defaults.

12.4 DHCP Screen

Click **Port > DHCP** to open the following screen. Use this screen to configure the DHCP snooping settings of the specified port.

Figure 125 Port > DHCP

The following table describes the fields in this screen.

Table 79 Port > DHCP

LABEL	DESCRIPTION
Slot, Port, Load	Use the Slot and Port drop-down list boxes to select the port on an active line card. Click Load to display the port's settings in the editing fields.
Max-lease	Specify the DHCP Snooping database max lease count for the specified port.
Ip-mac-binding	Use the drop-down list to enable or disable IP-MAC binding on the specified port.
Apply	Click Apply to save your changes in this screen.
Cancel	Click Cancel to begin configuring the screen again.

12.5 DSL

Click **Port > DSL** to open the following screen. Click the index number to configure the DSL settings of ports of the specified slot.

Figure 126 Port > DSL

DSL Port Setup

Slot **3** Port **1** **Setup**

Index	State	Card Type	Uptime
1	Active	MSC1002GA	144:11:37
2	Active	VOP1164A-61	144:10:24
3	Active	ALC1132A-51	144:10:49
4	Active	ELC1132A-45	144:10:07
5	Active	VLC1124A-51	144:09:49

Figure 127 Port > DSL Port Setup - Slot

DSL Port Setup: Slot 5

Index	Active	Name	Line Template	Fallback Template	Alarm Template	Transmission Type
1	☐		DEFVAL	DEFVAL	DEFVAL	auto
2	☐		DEFVAL	DEFVAL	DEFVAL	auto
3	☐		DEFVAL	DEFVAL	DEFVAL	auto
4	☐		DEFVAL	DEFVAL	DEFVAL	auto
5	☐		DEFVAL	DEFVAL	DEFVAL	auto
6	☐		DEFVAL	DEFVAL	DEFVAL	auto
7	☐		DEFVAL	DEFVAL	DEFVAL	auto
8	☐		DEFVAL	DEFVAL	DEFVAL	auto
9	☐		DEFVAL	DEFVAL	DEFVAL	auto
10	☐		DEFVAL	DEFVAL	DEFVAL	auto
11	☐		DEFVAL	DEFVAL	DEFVAL	auto
12	☐		DEFVAL	DEFVAL	DEFVAL	auto
13	☐		DEFVAL	DEFVAL	DEFVAL	auto
14	☐		DEFVAL	DEFVAL	DEFVAL	auto
15	☐		DEFVAL	DEFVAL	DEFVAL	auto
16	☐		DEFVAL	DEFVAL	DEFVAL	auto
17	☐		DEFVAL	DEFVAL	DEFVAL	auto
18	☐		DEFVAL	DEFVAL	DEFVAL	auto
19	☐		DEFVAL	DEFVAL	DEFVAL	auto
20	☐		DEFVAL	DEFVAL	DEFVAL	auto
21	☐		DEFVAL	DEFVAL	DEFVAL	auto
22	☐		DEFVAL	DEFVAL	DEFVAL	auto
23	☐		DEFVAL	DEFVAL	DEFVAL	auto
24	☐		DEFVAL	DEFVAL	DEFVAL	auto

Apply **Cancel**

The following table describes the fields in this screen.

Table 80 Port > DSL Port Setup - Slot

LABEL	DESCRIPTION
Index	This field displays the index number of a port. Click the index number to go to the screen as shown in the following figure.
Active	Select the check box to enable the specified port on the line card.
Name	Type the name of up to 31 printable characters for the specified port.

Table 80 Port > DSL Port Setup - Slot (continued)

LABEL	DESCRIPTION
Line Template	Select a DSL line template for the specified DSL port to reference.
Fallback Template	Select a DSL line template for the DSL port to use for fallback.
Alarm Template	Select a DSL alarm template for the specified DSL port to reference.
Transmission Type	Use the drop-down list box to select the allowed transmission type. auto : select the transmission type automatically. vdsl2/adsl2+/adsl2/gdmt/glite/t1413 : allow the specified protocol only. profile : adopt the DSL line/channel profile settings.
Apply	Click Apply to save your changes in this screen.
Cancel	Click Cancel to begin configuring the screen again.

Use the **Slot** and **Port** drop-down list boxes to select a subscriber port, and click **Setup** to configure the DSL port settings of the specified port.

Figure 128 Port > DSL Port Setup

DSL Port Setup: DSL 3/1

Slot 3 Port 1 Load

Active ☐

Name

Line Template DEFVAL

Alarm Template DEFVAL

Transmission Type auto

Annex I disable

Annex J disable

Annex L disable

Annex M disable

Pm mode disable

L0 time 255 [0 ~ 255] seconds

L2 time 255 [0 ~ 255] seconds

L2 power down step 1 [0 ~ 15] dB

L2 power down max 6 [0 ~ 15] dB

Tx power mode rate

Max US Tx power 130 [-130 ~ 200] 0.1 dBm

Max DS Tx power 200 [-50 ~ 200] 0.1 dBm

Max US Rx power 130 [-255 ~ 255] 0.1 dBm

Min INP downstream 5 [0 ~ 32]

Min INP upstream 5 [0 ~ 32]

Apply Cancel

The following table describes the fields in this screen.

Table 81 Port > DSL

LABEL	DESCRIPTION
Slot, Port, Load	Use the Slot and Port drop-down list boxes to select the port on an active line card. Click Load to display the port's settings in the editing fields.
Active	Select the check box to enable the DSL port.
Name	Type the name of up to 31 printable characters for the DSL port.
Line Template	Select the DSL line template to apply to the DSL port.
Alarm Template	Select the DSL alarm template to apply to the DSL port.
Transmission Type	Use the drop-down list box to select the transmission type allowed on the port. auto : select the transmission type automatically. vdsl2/adsl2+/adsl2/gdmt/glite/t1413 : allow the specified protocol only. profile : adopt the DSL line/channel profile settings and cannot configure Annex I to Min INP upstream settings in the screen above.
Annex I/J/L/M	Select Enable or Disable to activate or deactivate Annex I/J/L/M.
Pm mode	Specify the power management operating mode (used for ADSL2 and ADSL2+ protocols only). allow-I3 : DSL can automatically change to Idle (I3) state. allow-I2 : DSL can automatically change to low power (L2) state. allow-both : DSL can automatically change to Idle (I3) and low power (L2) state.
L0 time	Specify the time to stay in L0 (full power) mode.
L2 time	Specify the time to wait before performing another power trim in L2 mode.
L2 power down step	Specify the maximum total aggregate power reduction in dB per power trim in L2 mode.
L2 power down max	Specify the maximum total aggregate power reduction in dB in L2 mode.
Tx power mode	Select the Tx power mode. fix : fix to the maximum rate rate : priority to rate power : priority to power
Max US Tx power	Specify the maximum upstream allowed transmit power.
Max DS Tx power	Specify the maximum downstream allowed transmit power.
Max US Rx power	Specify the maximum aggregate receive power at the ATU-C.
Min INP downstream	Specify the downstream minimum INP for 4.3125 KHz carrier space DSL link.
Min INP upstream	Specify the upstream minimum INP for 4.3125 KHz carrier space DSL link.
Apply	Click Apply to save your changes in this screen.
Cancel	Click Cancel to begin configuring the screen again.

12.6 DSL Status

Click **Port > DSL Status** to open the following screen. This screen displays DSL line status.

Figure 129 Port > DSL Status

The following table describes the fields in this screen.

Table 82 Port > DSL Status

LABEL	DESCRIPTION
Slot	Use the Slot and Port drop-down list boxes to select the port on an active line card.
Port	
Load	Click Load to display the port's current status.
Line	This field displays the first part of DSL line parameters used for the DSL line.
line info	This field displays the second part of DSL line parameters used for the DSL line.
line rate	This field displays the line rate related information of a DSL line.
channel	This field displays the channel related information of a DSL line.
band	This field displays the band related information of a DSL line.
medleypsd	This field displays Medley PSD of a line card.
qln	This field displays per tone quiet line noise of a DSL line.
snr	This field displays per tone signal to noise ratio of a DSL line.
hlog	This field displays loop characteristics of a DSL line.
bitalloc	This field displays per tone Background Intelligent Transfer Service (BITS) allocation information of a DSL line.

12.7 FDB

Click **Port > FDB** to open the following screen. Use this screen to configure the forwarding database settings and display the forwarding database address table.

Figure 130 Port > FDB

FDB Port Setup

Slot **3** Port **1** **Load**

Static Only ☐

Max Count **32** [1 ~ 32]

Apply **Cancel**

Index	VLAN	Max Count	Select
New			Apply
Delete			

Index	MAC Address	VLAN	Select
New		☐	Apply
Delete			

Index	State	Card Type	Uptime
1	Active	MSC1002GA	144:32:17
2	Active	VOP1164A-61	144:31:04
3	Active	ALC1132A-51	144:31:29
4	Active	ELC1132A-45	144:30:47
5	Active	VLC1124A-51	144:30:29

The following table describes the fields in this screen.

Table 83 Port > FDB

LABEL	DESCRIPTION
Slot, Port, Load	Use the Slot and Port drop-down list boxes to select the port on an active line card. Click Load to display the port's settings in the editing fields.
Static Only	Select the check box to allow static MAC addresses only. If not, both static and dynamic MAC addresses are allowed.
Max Count	Specify the maximum number of forwarding database MAC entries for the specified port.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to begin the configuration again.
Index	This is the number of the forwarding database entry.
VLAN	Specify and display the VLAN ID on the specified port.
Max Count	Specify and display the maximum number of forwarding database MAC entries for the specified VLAN on the specified port.
Select	Click Apply to create a new entry, or click an entry's Select check box.
Delete	Click Delete to remove the specified entry.
Index	This is the number of the forwarding database entry.
MAC Address	Type an unicast MAC address to configure a static MAC entry on the specified port.
VLAN	Click the check box and type a VLAN ID to specify the VLAN if necessary.
Select	Click Apply to create a new entry, or click an entry's Select check box.
Delete	Click Delete to remove the specified entry.

Table 83 Port > FDB (continued)

LABEL	DESCRIPTION																																																																																																																																																																					
Index	This is the slot number of a line card. Click an index number to view the forwarding database address table of ports of the specified slot. FDB Port Config List <table><tr><th>Port</th><th>Static Only</th><th>Max Count</th><th>Max Count per VLAN</th><th>Static MAC</th></tr><tr><td>1</td><td>-</td><td>32</td><td>--</td><td>--</td></tr><tr><td>2</td><td>-</td><td>32</td><td>--</td><td>--</td></tr><tr><td>3</td><td>-</td><td>32</td><td>--</td><td>--</td></tr><tr><td>4</td><td>-</td><td>32</td><td>--</td><td>--</td></tr><tr><td>5</td><td>-</td><td>32</td><td>--</td><td>--</td></tr><tr><td>6</td><td>-</td><td>32</td><td>--</td><td>--</td></tr><tr><td>7</td><td>-</td><td>32</td><td>--</td><td>--</td></tr><tr><td>8</td><td>-</td><td>32</td><td>--</td><td>--</td></tr><tr><td>9</td><td>-</td><td>32</td><td>--</td><td>--</td></tr><tr><td>10</td><td>-</td><td>32</td><td>--</td><td>--</td></tr><tr><td>11</td><td>-</td><td>32</td><td>--</td><td>--</td></tr><tr><td>12</td><td>-</td><td>32</td><td>--</td><td>--</td></tr><tr><td>13</td><td>-</td><td>32</td><td>--</td><td>--</td></tr><tr><td>14</td><td>-</td><td>32</td><td>--</td><td>--</td></tr><tr><td>15</td><td>-</td><td>32</td><td>--</td><td>--</td></tr><tr><td>16</td><td>-</td><td>32</td><td>--</td><td>--</td></tr><tr><td>17</td><td>-</td><td>32</td><td>--</td><td>--</td></tr><tr><td>18</td><td>-</td><td>32</td><td>--</td><td>--</td></tr><tr><td>19</td><td>-</td><td>32</td><td>--</td><td>--</td></tr><tr><td>20</td><td>-</td><td>32</td><td>--</td><td>--</td></tr><tr><td>21</td><td>-</td><td>32</td><td>--</td><td>--</td></tr><tr><td>22</td><td>-</td><td>32</td><td>--</td><td>--</td></tr><tr><td>23</td><td>-</td><td>32</td><td>--</td><td>--</td></tr><tr><td>24</td><td>-</td><td>32</td><td>--</td><td>--</td></tr><tr><td>25</td><td>-</td><td>32</td><td>--</td><td>--</td></tr><tr><td>26</td><td>-</td><td>32</td><td>--</td><td>--</td></tr><tr><td>27</td><td>-</td><td>32</td><td>--</td><td>--</td></tr><tr><td>28</td><td>-</td><td>32</td><td>--</td><td>--</td></tr><tr><td>29</td><td>-</td><td>32</td><td>--</td><td>--</td></tr><tr><td>30</td><td>-</td><td>32</td><td>--</td><td>--</td></tr><tr><td>31</td><td>-</td><td>32</td><td>--</td><td>--</td></tr><tr><td>32</td><td>-</td><td>32</td><td>--</td><td>--</td></tr></table>	Port	Static Only	Max Count	Max Count per VLAN	Static MAC	1	-	32	--	--	2	-	32	--	--	3	-	32	--	--	4	-	32	--	--	5	-	32	--	--	6	-	32	--	--	7	-	32	--	--	8	-	32	--	--	9	-	32	--	--	10	-	32	--	--	11	-	32	--	--	12	-	32	--	--	13	-	32	--	--	14	-	32	--	--	15	-	32	--	--	16	-	32	--	--	17	-	32	--	--	18	-	32	--	--	19	-	32	--	--	20	-	32	--	--	21	-	32	--	--	22	-	32	--	--	23	-	32	--	--	24	-	32	--	--	25	-	32	--	--	26	-	32	--	--	27	-	32	--	--	28	-	32	--	--	29	-	32	--	--	30	-	32	--	--	31	-	32	--	--	32	-	32	--	--
Port	Static Only	Max Count	Max Count per VLAN	Static MAC																																																																																																																																																																		
1	-	32	--	--																																																																																																																																																																		
2	-	32	--	--																																																																																																																																																																		
3	-	32	--	--																																																																																																																																																																		
4	-	32	--	--																																																																																																																																																																		
5	-	32	--	--																																																																																																																																																																		
6	-	32	--	--																																																																																																																																																																		
7	-	32	--	--																																																																																																																																																																		
8	-	32	--	--																																																																																																																																																																		
9	-	32	--	--																																																																																																																																																																		
10	-	32	--	--																																																																																																																																																																		
11	-	32	--	--																																																																																																																																																																		
12	-	32	--	--																																																																																																																																																																		
13	-	32	--	--																																																																																																																																																																		
14	-	32	--	--																																																																																																																																																																		
15	-	32	--	--																																																																																																																																																																		
16	-	32	--	--																																																																																																																																																																		
17	-	32	--	--																																																																																																																																																																		
18	-	32	--	--																																																																																																																																																																		
19	-	32	--	--																																																																																																																																																																		
20	-	32	--	--																																																																																																																																																																		
21	-	32	--	--																																																																																																																																																																		
22	-	32	--	--																																																																																																																																																																		
23	-	32	--	--																																																																																																																																																																		
24	-	32	--	--																																																																																																																																																																		
25	-	32	--	--																																																																																																																																																																		
26	-	32	--	--																																																																																																																																																																		
27	-	32	--	--																																																																																																																																																																		
28	-	32	--	--																																																																																																																																																																		
29	-	32	--	--																																																																																																																																																																		
30	-	32	--	--																																																																																																																																																																		
31	-	32	--	--																																																																																																																																																																		
32	-	32	--	--																																																																																																																																																																		
State	This field displays the line card's current operational status. Active means the line card is operating normally. init means the IES is initializing the line card. disable means a manager has disabled the line card. inactive means the line card is starting up or is not operating normally.																																																																																																																																																																					
Card Type	This field displays the type of a line card.																																																																																																																																																																					
Uptime	This field displays how long the card has been running since the last time it was started.																																																																																																																																																																					

12.8 Permanent Virtual Circuits

A Permanent Virtual Circuit (PVC) is a logical point-to-point circuit between sites. PVCs are low-delay circuits because routing decisions do not need to be made along the way. Permanent means that the circuit is pre-programmed by the carrier as a path through the network. It does not need to be set up or torn down for each session. PVCs are also called virtual channels.

The system can handle multiple IEEE 802.1p priority queues on a single PVC. You can also define up to eight PVCs on a DSL port and use them for different services or levels of service. You set the PVID that is assigned to untagged frames received on each channel. You also set an IEEE 802.1p priority for each of the PVIDs. In this way you can assign different priorities to different channels (and consequently the services that get carried on them or the subscribers that use them).

For example, you want to give high priority to voice service on one of the ADSL ports. First configure a static VLAN on the system for voice on the port. Then do the following:

- Configure a channel on the port for voice service.
- Set the channel to use the PVID of the static VLAN you configured.
- Assign the channel a high priority.

12.8.1 LLC

LLC is a type of encapsulation where one VC (Virtual Circuit) carries multiple protocols with each packet header containing protocol identifying information. Despite the extra bandwidth and processing overhead, this method may be advantageous if it is not practical to have a separate VC for each carried protocol, for example, if charging heavily depends on the number of simultaneous VCs.

12.8.2 VC Mux

VC Mux is a type of encapsulation where, by prior mutual agreement, each protocol is assigned to a specific virtual circuit, for example, VC1 carries IP, VC2 carries IPX, and so on. VC-based multiplexing may be dominant in environments where dynamic creation of large numbers of ATM VCs is fast and economical.

12.8.3 PVC Setup Screen

Click **Port > PVC** to open the following screen. Use this screen to view and configure permanent virtual circuit settings for individual ports.

Figure 131 Port > PVC

PVC Setup: DSL 3/1

Slot **3** Port **1** **Load**

Index	VPI/VCI	Encapsulation	Priority	Pvid	Pbit	MVLAN	Select
1	0/33	Ilc	0	1	0	-	☒

Delete

VPI/VCI: /

Encapsulation: **Ilc** ▼

Priority: **0** ▼

Pvid:

Pbit:

MVLAN: ☐

Apply **Cancel**

Index	State	Card Type	Uptime
1	Active	MSC1002GA	159:50:36
2	Active	VOP1164A-61	159:49:23
3	Active	ALC1132A-51	159:49:48
4	Active	ELC1132A-45	159:49:06
5	Active	VLC1124A-51	159:48:48

The following table describes the fields in this screen.

Table 84 Port > PVC

LABEL	DESCRIPTION
Slot	Select the number of a line card's slot.
Port	Select the number of a DSL port on the line card.
Load	Click Load to display the port's PVC settings in the PVC Table .
Index	This is the number of the PVC on this port.
VPI/VCI	This field displays the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI). The VPI and VCI identify a channel on this port.
Encapsulation	This displays the encapsulation type this PVC uses.
Priority	This field displays QoS priority between PVCs in the specified port.
Pvid	This field displays the PVID (Port VLAN ID) to assign to untagged frames received on this channel.
Pbit	This field displays the priority bit value (0 to 7) that the line card adds to frames that come in on this PVC.
MVLAN	This field displays the PVC's current multicast VLAN setting. "-" indicates the multicast VLAN is not active while "V" indicates the multicast VLAN is active.
Select	Select a PVC's radio button and click the Delete button to remove an entry.
Delete	
VPI/VCI	Type the Virtual Path Identifier and Virtual Circuit Identifier for a channel on this port.

Table 84 Port > PVC (continued)

LABEL	DESCRIPTION																																																																																																																																																																																																																																																																																																									
Encapsulation	Select the encapsulation type this PVC uses. llc: LLC encapsulation vc: VC-MUX encapsulation																																																																																																																																																																																																																																																																																																									
Priority	Type the QoS priority between PVCs in the specified port.																																																																																																																																																																																																																																																																																																									
Pvid	Type a Port VLAN ID (PVID) to assign to untagged frames received on this channel.																																																																																																																																																																																																																																																																																																									
Pbit	Type the priority bit value to add to incoming frames.																																																																																																																																																																																																																																																																																																									
MVLAN	Select this option to turn on multicast VLAN for this PVC.																																																																																																																																																																																																																																																																																																									
Apply	Click Apply to save your changes in this screen.																																																																																																																																																																																																																																																																																																									
Cancel	Click Cancel to begin configuring this screen again.																																																																																																																																																																																																																																																																																																									
Index	This is the slot number of a line card. Click an index number to view the PVC settings of ports of the specified slot. PVC Setup: Slot 5 <table><thead><tr><th>Index</th><th>Port</th><th>PVC</th><th>Encapsulation</th><th>Priority</th><th>Pvid</th><th>Pbit</th><th>MVLAN</th><th>Select</th></tr></thead><tbody><tr><td>1</td><td>1</td><td>0/33</td><td>llc</td><td>0</td><td>1</td><td>0</td><td>-</td><td>☐</td></tr><tr><td>2</td><td>2</td><td>0/33</td><td>llc</td><td>0</td><td>1</td><td>0</td><td>-</td><td>☐</td></tr><tr><td>3</td><td>3</td><td>0/33</td><td>llc</td><td>0</td><td>1</td><td>0</td><td>-</td><td>☐</td></tr><tr><td>4</td><td>4</td><td>0/33</td><td>llc</td><td>0</td><td>1</td><td>0</td><td>-</td><td>☐</td></tr><tr><td>5</td><td>5</td><td>0/33</td><td>llc</td><td>0</td><td>1</td><td>0</td><td>-</td><td>☐</td></tr><tr><td>6</td><td>6</td><td>0/33</td><td>llc</td><td>0</td><td>1</td><td>0</td><td>-</td><td>☐</td></tr><tr><td>7</td><td>7</td><td>0/33</td><td>llc</td><td>0</td><td>1</td><td>0</td><td>-</td><td>☐</td></tr><tr><td>8</td><td>8</td><td>0/33</td><td>llc</td><td>0</td><td>1</td><td>0</td><td>-</td><td>☐</td></tr><tr><td>9</td><td>9</td><td>0/33</td><td>llc</td><td>0</td><td>1</td><td>0</td><td>-</td><td>☐</td></tr><tr><td>10</td><td>10</td><td>0/33</td><td>llc</td><td>0</td><td>1</td><td>0</td><td>-</td><td>☐</td></tr><tr><td>11</td><td>11</td><td>0/33</td><td>llc</td><td>0</td><td>1</td><td>0</td><td>-</td><td>☐</td></tr><tr><td>12</td><td>12</td><td>0/33</td><td>llc</td><td>0</td><td>1</td><td>0</td><td>-</td><td>☐</td></tr><tr><td>13</td><td>13</td><td>0/33</td><td>llc</td><td>0</td><td>1</td><td>0</td><td>-</td><td>☐</td></tr><tr><td>14</td><td>14</td><td>0/33</td><td>llc</td><td>0</td><td>1</td><td>0</td><td>-</td><td>☐</td></tr><tr><td>15</td><td>15</td><td>0/33</td><td>llc</td><td>0</td><td>1</td><td>0</td><td>-</td><td>☐</td></tr><tr><td>16</td><td>16</td><td>0/33</td><td>llc</td><td>0</td><td>1</td><td>0</td><td>-</td><td>☐</td></tr><tr><td>17</td><td>17</td><td>0/33</td><td>llc</td><td>0</td><td>1</td><td>0</td><td>-</td><td>☐</td></tr><tr><td>18</td><td>18</td><td>0/33</td><td>llc</td><td>0</td><td>1</td><td>0</td><td>-</td><td>☐</td></tr><tr><td>19</td><td>19</td><td>0/33</td><td>llc</td><td>0</td><td>1</td><td>0</td><td>-</td><td>☐</td></tr><tr><td>20</td><td>20</td><td>0/33</td><td>llc</td><td>0</td><td>1</td><td>0</td><td>-</td><td>☐</td></tr><tr><td>21</td><td>21</td><td>0/33</td><td>llc</td><td>0</td><td>1</td><td>0</td><td>-</td><td>☐</td></tr><tr><td>22</td><td>22</td><td>0/33</td><td>llc</td><td>0</td><td>1</td><td>0</td><td>-</td><td>☐</td></tr><tr><td>23</td><td>23</td><td>0/33</td><td>llc</td><td>0</td><td>1</td><td>0</td><td>-</td><td>☐</td></tr><tr><td>24</td><td>24</td><td>0/33</td><td>llc</td><td>0</td><td>1</td><td>0</td><td>-</td><td>☐</td></tr><tr><td>25</td><td>25</td><td>0/33</td><td>llc</td><td>0</td><td>1</td><td>0</td><td>-</td><td>☐</td></tr><tr><td>26</td><td>26</td><td>0/33</td><td>llc</td><td>0</td><td>1</td><td>0</td><td>-</td><td>☐</td></tr><tr><td>27</td><td>27</td><td>0/33</td><td>llc</td><td>0</td><td>1</td><td>0</td><td>-</td><td>☐</td></tr><tr><td>28</td><td>28</td><td>0/33</td><td>llc</td><td>0</td><td>1</td><td>0</td><td>-</td><td>☐</td></tr><tr><td>29</td><td>29</td><td>0/33</td><td>llc</td><td>0</td><td>1</td><td>0</td><td>-</td><td>☐</td></tr><tr><td>30</td><td>30</td><td>0/33</td><td>llc</td><td>0</td><td>1</td><td>0</td><td>-</td><td>☐</td></tr><tr><td>31</td><td>31</td><td>0/33</td><td>llc</td><td>0</td><td>1</td><td>0</td><td>-</td><td>☐</td></tr><tr><td>32</td><td>32</td><td>0/33</td><td>llc</td><td>0</td><td>1</td><td>0</td><td>-</td><td>☐</td></tr></tbody></table> Delete	Index	Port	PVC	Encapsulation	Priority	Pvid	Pbit	MVLAN	Select	1	1	0/33	llc	0	1	0	-	☐	2	2	0/33	llc	0	1	0	-	☐	3	3	0/33	llc	0	1	0	-	☐	4	4	0/33	llc	0	1	0	-	☐	5	5	0/33	llc	0	1	0	-	☐	6	6	0/33	llc	0	1	0	-	☐	7	7	0/33	llc	0	1	0	-	☐	8	8	0/33	llc	0	1	0	-	☐	9	9	0/33	llc	0	1	0	-	☐	10	10	0/33	llc	0	1	0	-	☐	11	11	0/33	llc	0	1	0	-	☐	12	12	0/33	llc	0	1	0	-	☐	13	13	0/33	llc	0	1	0	-	☐	14	14	0/33	llc	0	1	0	-	☐	15	15	0/33	llc	0	1	0	-	☐	16	16	0/33	llc	0	1	0	-	☐	17	17	0/33	llc	0	1	0	-	☐	18	18	0/33	llc	0	1	0	-	☐	19	19	0/33	llc	0	1	0	-	☐	20	20	0/33	llc	0	1	0	-	☐	21	21	0/33	llc	0	1	0	-	☐	22	22	0/33	llc	0	1	0	-	☐	23	23	0/33	llc	0	1	0	-	☐	24	24	0/33	llc	0	1	0	-	☐	25	25	0/33	llc	0	1	0	-	☐	26	26	0/33	llc	0	1	0	-	☐	27	27	0/33	llc	0	1	0	-	☐	28	28	0/33	llc	0	1	0	-	☐	29	29	0/33	llc	0	1	0	-	☐	30	30	0/33	llc	0	1	0	-	☐	31	31	0/33	llc	0	1	0	-	☐	32	32	0/33	llc	0	1	0	-	☐
Index	Port	PVC	Encapsulation	Priority	Pvid	Pbit	MVLAN	Select																																																																																																																																																																																																																																																																																																		
1	1	0/33	llc	0	1	0	-	☐																																																																																																																																																																																																																																																																																																		
2	2	0/33	llc	0	1	0	-	☐																																																																																																																																																																																																																																																																																																		
3	3	0/33	llc	0	1	0	-	☐																																																																																																																																																																																																																																																																																																		
4	4	0/33	llc	0	1	0	-	☐																																																																																																																																																																																																																																																																																																		
5	5	0/33	llc	0	1	0	-	☐																																																																																																																																																																																																																																																																																																		
6	6	0/33	llc	0	1	0	-	☐																																																																																																																																																																																																																																																																																																		
7	7	0/33	llc	0	1	0	-	☐																																																																																																																																																																																																																																																																																																		
8	8	0/33	llc	0	1	0	-	☐																																																																																																																																																																																																																																																																																																		
9	9	0/33	llc	0	1	0	-	☐																																																																																																																																																																																																																																																																																																		
10	10	0/33	llc	0	1	0	-	☐																																																																																																																																																																																																																																																																																																		
11	11	0/33	llc	0	1	0	-	☐																																																																																																																																																																																																																																																																																																		
12	12	0/33	llc	0	1	0	-	☐																																																																																																																																																																																																																																																																																																		
13	13	0/33	llc	0	1	0	-	☐																																																																																																																																																																																																																																																																																																		
14	14	0/33	llc	0	1	0	-	☐																																																																																																																																																																																																																																																																																																		
15	15	0/33	llc	0	1	0	-	☐																																																																																																																																																																																																																																																																																																		
16	16	0/33	llc	0	1	0	-	☐																																																																																																																																																																																																																																																																																																		
17	17	0/33	llc	0	1	0	-	☐																																																																																																																																																																																																																																																																																																		
18	18	0/33	llc	0	1	0	-	☐																																																																																																																																																																																																																																																																																																		
19	19	0/33	llc	0	1	0	-	☐																																																																																																																																																																																																																																																																																																		
20	20	0/33	llc	0	1	0	-	☐																																																																																																																																																																																																																																																																																																		
21	21	0/33	llc	0	1	0	-	☐																																																																																																																																																																																																																																																																																																		
22	22	0/33	llc	0	1	0	-	☐																																																																																																																																																																																																																																																																																																		
23	23	0/33	llc	0	1	0	-	☐																																																																																																																																																																																																																																																																																																		
24	24	0/33	llc	0	1	0	-	☐																																																																																																																																																																																																																																																																																																		
25	25	0/33	llc	0	1	0	-	☐																																																																																																																																																																																																																																																																																																		
26	26	0/33	llc	0	1	0	-	☐																																																																																																																																																																																																																																																																																																		
27	27	0/33	llc	0	1	0	-	☐																																																																																																																																																																																																																																																																																																		
28	28	0/33	llc	0	1	0	-	☐																																																																																																																																																																																																																																																																																																		
29	29	0/33	llc	0	1	0	-	☐																																																																																																																																																																																																																																																																																																		
30	30	0/33	llc	0	1	0	-	☐																																																																																																																																																																																																																																																																																																		
31	31	0/33	llc	0	1	0	-	☐																																																																																																																																																																																																																																																																																																		
32	32	0/33	llc	0	1	0	-	☐																																																																																																																																																																																																																																																																																																		
State	This field displays the line card's current operational status. Active means the line card is operating normally. init means the IES is initializing the line card. disable means a manager has disabled the line card. inactive means the line card is starting up or is not operating normally.																																																																																																																																																																																																																																																																																																									
Card Type	This field displays the type of a line card.																																																																																																																																																																																																																																																																																																									
Uptime	This field displays how long the card has been running since the last time it was started.																																																																																																																																																																																																																																																																																																									

12.9 QoS

Click **Port > QoS** to open the following screen. Click an index number to configure QoS settings for ports of the specified slot.

Figure 132 Port > QoS

QoS Port Setup

Slot **3** Port **1** **Setup**

Index	State	Card Type	Uptime
1	Active	MSC1002GA	159:51:40
2	Active	VOP1164A-61	159:50:27
3	Active	ALC1132A-51	159:50:52
4	Active	ELC1132A-45	159:50:10
5	Active	VLC1124A-51	159:49:52

Figure 133 Port > QoS Port Setup - Slot

QoS Port Setup: Slot 3

Index	Max Rate [32 ~ 100000] kbps	Algorithm	Shaping Profile	Weight Profile
1	100000	sp	DEFVAL	DEFVAL
2	100000	sp	DEFVAL	DEFVAL
3	100000	sp	DEFVAL	DEFVAL
4	100000	sp	DEFVAL	DEFVAL
5	100000	sp	DEFVAL	DEFVAL
6	100000	sp	DEFVAL	DEFVAL
7	100000	sp	DEFVAL	DEFVAL
8	100000	sp	DEFVAL	DEFVAL
9	100000	sp	DEFVAL	DEFVAL
10	100000	sp	DEFVAL	DEFVAL
11	100000	sp	DEFVAL	DEFVAL
12	100000	sp	DEFVAL	DEFVAL
13	100000	sp	DEFVAL	DEFVAL
14	100000	sp	DEFVAL	DEFVAL
15	100000	sp	DEFVAL	DEFVAL
16	100000	sp	DEFVAL	DEFVAL
17	100000	sp	DEFVAL	DEFVAL
18	100000	sp	DEFVAL	DEFVAL
19	100000	sp	DEFVAL	DEFVAL
20	100000	sp	DEFVAL	DEFVAL
21	100000	sp	DEFVAL	DEFVAL
22	100000	sp	DEFVAL	DEFVAL
23	100000	sp	DEFVAL	DEFVAL
24	100000	sp	DEFVAL	DEFVAL
25	100000	sp	DEFVAL	DEFVAL
26	100000	sp	DEFVAL	DEFVAL
27	100000	sp	DEFVAL	DEFVAL
28	100000	sp	DEFVAL	DEFVAL
29	100000	sp	DEFVAL	DEFVAL
30	100000	sp	DEFVAL	DEFVAL
31	100000	sp	DEFVAL	DEFVAL
32	100000	sp	DEFVAL	DEFVAL

Apply **Cancel**

The following table describes the fields in this screen.

Table 85 Port > QoS Port Setup - Slot

LABEL	DESCRIPTION
Index	This field displays the index number of a port on the specified slot. Click the index number to configure the QoS settings of the specified port as shown in the figure below.
Max Rate	Specify the maximum transmission rate.
Algorithm	Select which QoS algorithm to use on the specified DSL port. sp : Strict Priority, queue 7 has the highest priority wfq : Weighted Fair Queueing sp+wfq : Strict Priority + Weighted Fair Queueing. Queue 5-0 are scheduled by WFQ first, and the output of WFQ, queue 7, and queue 6 are scheduled by Strict Priority. Queue 7 has the highest priority, and the output of WFQ has the lowest priority. shaping : Strict Priority + shaping. Every queue has its own shaping rate. After shaping, every queue is scheduled by Strict Priority. Queue 7 has the highest priority.
Shaping Profile	Select a shaping profile to apply to the specified port.
Weight Profile	Select a Weighted Round Robin or Weight Fair Queueing profile on the specified port.
Apply	Click Apply to save your changes in this screen.
Cancel	Click Cancel to begin configuring the screen again.

Use the **Slot** and **Port** drop-down list boxes in **QoS Port Setup** screen to select a subscriber port, and click **Setup** to configure the Quality of Service (QoS) settings of the specified port.

Figure 134 Port > QoS Setup

The following table describes the fields in this screen.

Table 86 Port > QoS

LABEL	DESCRIPTION
Slot	Use the Slot and Port drop-down list boxes to select the port on an active line card.
Port	
Load	Click Load to save your changes.
Max Rate	Specify the maximum transmission rate.

Table 86 Port > QoS (continued)

LABEL	DESCRIPTION
Algorithm	Select which QoS algorithm to use on the specified DSL port. sp: Strict Priority, queue 7 has the highest priority wfq: Weighted Fair Queueing sp+wfq: Strict Priority + Weighted Fair Queueing. Queue 5-0 are scheduled by WFQ first, and the output of WFQ, queue 7, and queue 6 are scheduled by Strict Priority. Queue 7 has the highest priority, and the output of WFQ has the lowest priority. shaping: Strict Priority + shaping. Every queue has its own shaping rate. After shaping, every queue is scheduled by Strict Priority. Queue 7 has the highest priority.
Shaping Profile	Select a shaping profile on the specified port.
Weight Profile	Select a Weighted Round Robin or Weight Fair Queueing profile on the specified port.
VC-Shaping Profile	Select a VC shaping profile to apply to the specified port.
Apply	Click Apply to save your changes in this screen.
Cancel	Click Cancel to begin configuring the screen again.

12.10 H.248 Port Setup

This is available when using H.248 firmware. Click **Port > H.248** to manage and configure subscriber H.248 VoIP port settings. Click an index number to configure settings for ports on the specified slot.

Figure 135 Port > H.248

H248 Port Setup			
Slot	2 ▼	Port	1 ▼
Setup			
Index	State	Card Type	Uptime
1	Active	MSC1002GA	159:56:04
<u>2</u>	Active	VOP1164A-61	159:54:51
3	Active	ALC1132A-51	159:55:16
4	Active	ELC1132A-45	159:54:34
5	Active	VLC1124A-51	159:54:16

Figure 136 Port > H.248 Port Setup - Slot

Index	Active ☐	DSP Profile
1	☒	DEFVAL ▼
2	☒	DEFVAL ▼
3	☒	DEFVAL ▼
4	☒	DEFVAL ▼
5	☒	DEFVAL ▼
6	☒	DEFVAL ▼
7	☒	DEFVAL ▼
8	☒	DEFVAL ▼
9	☒	DEFVAL ▼
10	☒	DEFVAL ▼
11	☒	DEFVAL ▼
12	☒	DEFVAL ▼
13	☒	DEFVAL ▼
14	☒	DEFVAL ▼

58	☐	DEFVAL ▼
59	☐	DEFVAL ▼
60	☐	DEFVAL ▼
61	☐	DEFVAL ▼
62	☐	DEFVAL ▼
63	☐	DEFVAL ▼
64	☐	DEFVAL ▼

The following table describes the labels in this screen.

Table 87 Port > H.248 Port Setup - Slot

LABEL	DESCRIPTION
Index	This field displays the index number of a port on the specified slot. Click the index number to configure the VoIP settings of the specified port as shown in the following figure.
Active	Select the check box to enable the VoIP port.
DSP Profile	Select the digital sound processing profile the port uses for voice traffic. If you have not configured any profiles, you can only select the default profile DEFVAL .
Apply	Click Apply to save your changes.
Cancel	Click Cancel to begin configuring the screen again.

Use the **Slot** and **Port** drop-down list boxes on **H.248 Port Setup** screen to select a subscriber port, and click **Setup** to manage and configure the VoIP settings of each port on your H.248 line cards.

Figure 137 Port > H.248 Setup

H248 Port Setup: VoIP 2/1

Slot **2** Port **1** **Load**

VoIP

Active ☐

DSP Profile **DEFVAL**

VBD DSP Profile **DEFVAL**

Impedance **270ohm_750ohm_150nf**

Apply **Cancel**

POTS

Battery **Low**

Data Gain TX **0** RX **-3** [-20 ~ 20] in unit of 1dB

Voice Gain TX **0** RX **-3** [-20 ~ 20] in unit of 1dB

Loopcurrent **25** [10 ~ 30] in unit of mA

Loopresistance **2600** [2600 or 3200] in unit of ohm

CID Type AS Type **DEFVAL** Payload Type **DEFVAL**

Hook Flash Detection **DEFVAL** ☒

Minimum Time **90** 20 ~ 1500 ms

Maximum Time **500** Minimum Time ~ 1500 ms

Apply **Cancel**

H248

Termination ID

Apply **Cancel**

The following table describes the labels in this screen.

Table 88 Port > H.248

LABEL	DESCRIPTION
Slot	Use the drop-down list boxes to select the port on an active VoIP line card you want to configure.
Port	
Load	Click this to display the port's current settings.
VoIP	
Active	Click the check box to enable the VoIP Port.
DSP Profile	Select the digital sound processing profile the port uses for voice traffic. If you have not configured any profiles, you can only select the default profile DEFVAL .
VBD DSP Profile	Select the digital sound processing profile the port uses for voice band data service. If you have not configured any profiles, you can only select the default profile DEFVAL .
Impedance	Select the POTS impedance value on the specified subscriber port.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to begin configuring the screen again.
POTS	

Table 88 Port > H.248 (continued)

LABEL	DESCRIPTION
Battery	Select the battery supply of a port. low: for short loop high: for long loop boost: for even more power for an even longer loop.
Data Gain	Specify the amount of gain (increase in volume) to apply to the voice band data service the subscriber transmits (tx) or receives (rx). A negative value decreases the volume.
Voice Gain	Specify the amount of gain (increase in volume) to apply to the voice signal the subscriber transmits (tx) or receives (rx). A negative value decrease the volume.
Loopcurrent	Specify the supplied line current in milliamps.
Loopresistance	Specify the port's loop resistance in ohm.
CID Type	Specify the port's Caller ID type. as-type: the AS (Alerting Signal) type of CID, 0-6 DEFVAL: (determine the setting based on the country code) CID during ring DTAS (Dual Tone Alerting Signal) CID before ring RPAS (Ringing Pulse Alerting Signal) CID before ring LR Line Reversal DTAS CID before ring LR CID before ring CID before ring
Payload Type	Specify the port's payload type of CID. DEFVAL (determine the setting based on the country code) MDMF (Multiple Data Message Format) which transmits caller name, number, date and time. SDMF (Single Data Message Format) which transmits caller number, date and time. ETSI MDMF ETSI SDMF DTMF UK MDMF UK SDMF Japanese MDMF
Hook Flash Detection	Specify how long (in milliseconds) a user has to press the flash key to register its use. DEFVAL: Not specified (use the value defined in the current selected country code).
Apply	Click Apply to save your changes.
Cancel	Click Cancel to begin configuring the screen again.
H.248	
Termination ID	Enter the name for this port's H.248 Termination. By default, the port's Termination name is "termX", where X is the port number. Enter up to 31 alphanumeric characters. Spaces are not allowed.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to begin configuring the screen again.

12.11 SIP Port Setup

This is available when using SIP firmware. Click **Port > SIP** to manage and configure subscriber SIP VoIP port settings. Click an index number to configure settings for ports on the specified slot.

Figure 138 Port > SIP

Index	State	Card Type	Uptime
1	Active	MSC1002GA	1:57:46
2	Active	VOP1164A-61	1:55:48
3	Active	ALC1132A-51	1:56:46
4	Active	ELC1132A-45	1:56:25
5	Active	VLC1124A-51	1:55:45

Figure 139 Port > SIP Port Setup - Slot

Index	Active ☐	Tel Number	SIP Profile	SVC Profile	DSP Profile
1	☐		DEFVAL ▼	DEFVAL ▼	DEFVAL ▼
2	☐		DEFVAL ▼	DEFVAL ▼	DEFVAL ▼
3	☐		DEFVAL ▼	DEFVAL ▼	DEFVAL ▼
4	☐		DEFVAL ▼	DEFVAL ▼	DEFVAL ▼
5	☐		DEFVAL ▼	DEFVAL ▼	DEFVAL ▼
6	☐		DEFVAL ▼	DEFVAL ▼	DEFVAL ▼
7	☐		DEFVAL ▼	DEFVAL ▼	DEFVAL ▼
8	☐		DEFVAL ▼	DEFVAL ▼	DEFVAL ▼
9	☐		DEFVAL ▼	DEFVAL ▼	DEFVAL ▼
10	☐		DEFVAL ▼	DEFVAL ▼	DEFVAL ▼
11	☐		DEFVAL ▼	DEFVAL ▼	DEFVAL ▼
12	☐		DEFVAL ▼	DEFVAL ▼	DEFVAL ▼
13	☐		DEFVAL ▼	DEFVAL ▼	DEFVAL ▼
14	☐		DEFVAL ▼	DEFVAL ▼	DEFVAL ▼
15	☐		DEFVAL ▼	DEFVAL ▼	DEFVAL ▼
16	☐		DEFVAL ▼	DEFVAL ▼	DEFVAL ▼
~~					
58	☐		DEFVAL ▼	DEFVAL ▼	DEFVAL ▼
59	☐		DEFVAL ▼	DEFVAL ▼	DEFVAL ▼
60	☐		DEFVAL ▼	DEFVAL ▼	DEFVAL ▼
61	☐		DEFVAL ▼	DEFVAL ▼	DEFVAL ▼
62	☐		DEFVAL ▼	DEFVAL ▼	DEFVAL ▼
63	☐		DEFVAL ▼	DEFVAL ▼	DEFVAL ▼
64	☐		DEFVAL ▼	DEFVAL ▼	DEFVAL ▼

Apply Cancel

The following table describes the labels in this screen.

Table 89 Port > SIP Port Setup - Slot

LABEL	DESCRIPTION
Up	Click this to go to the next higher screen.
Index	This field displays the index number of a port on the specified slot. Click the index number to configure the VoIP settings of the specified port as shown in the following figure.
Active	Select the check box to enable the VoIP port.
Tel Number	Specify the telephone number of the specified index in the specified local help table. Up to 15 characters. Only alphanumeric characters and '+' are allowed or use two quotation marks (") to clear the field. Note: '+' is only allowed as the first character.
SIP Profile	Select the SIP settings profile the port uses for voice traffic.
SVC Profile	Select the VoIP SIP Service profile for settings of SIP call services for the port.
DSP Profile	Select the digital sound processing profile the port uses for voice traffic.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to begin configuring the screen again.

Use the **Slot** and **Port** drop-down list boxes on **SIP Port Setup** screen to select a subscriber port, and click **Setup** to manage and configure the VoIP settings of each port on your SIP line cards.

Figure 140 Port > SIP Setup

SIP Port Setup: VoIP 2/1

Up

Slot 2 ▼ Port 1 ▼

Load

VoIP

Active

☐

DSP Profile

DEFVAL ▼

VBD DSP Profile

DEFVAL ▼

Impedance

200ohm_680ohm_100nf ▼

Apply

Cancel

POTS

Battery

Low ▼

Data Gain

TX 0

RX -3

[-20 ~ 20] in unit of 1dB

Voice Gain

TX 0

RX -3

[-20 ~ 20] in unit of 1dB

Loopcurrent

25 [10 ~ 30] in unit of mA

Loopresistance

2600 [2600 or 3200] in unit of ohm

VMWI Format

FSK ▼

CID Type

AS Type DEFVAL ▼

Payload Type DEFVAL ▼

Hook Flash Detection

DEFVAL ☒

Minimum Time

90 20 ~ 1500 ms

Maximum Time

500 Minimum Time ~ 1500 ms

Apply

Cancel

SIP

Account

Password

Hotline

☐ Hotline-no

Hotline timeout

[0 ~ 255] seconds

Name

Polarity-Reverse

☐

Tel Number

SIP Profile

DEFVAL ▼

SVC Profile

DEFVAL ▼

Apply

Cancel

The following table describes the labels in this screen.

Table 90 Port > SIP

LABEL	DESCRIPTION
Up	Click this to go to the next higher screen.
Slot	Use the drop-down list boxes to select the port on an active VoIP line card you want to configure.
Port	
Load	Click this to display the port's current settings.
VoIP	

Table 90 Port > SIP (continued)

LABEL	DESCRIPTION
Active	Select the check box to enable the VoIP Port.
DSP Profile	Select the digital sound processing profile the port uses for voice traffic.
VBD DSP Profile	Select the digital sound processing profile the port uses for voice band data service.
Impedance	Select the POTS impedance value on the specified subscriber port.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to begin configuring the screen again.
POTS	
Battery	Select the battery supply of the port. low: for short loop high: for long loop
Data Gain	Specify the amount of gain (increase in volume) to apply to the voice band data service the subscriber transmits (tx) or receives (rx). A negative value decreases the volume.
Voice Gain	Specify the amount of gain (increase in volume) to apply to the voice signal the subscriber transmits (tx) or receives (rx). A negative value decreases the volume.
Loopcurrent	Specify the supplied line current in milliamps.
Loopresistance	Specify the port's loop resistance in ohm.
VMWI Format	Configure the Visual Message Waiting Indicator (VMWI) format for the port. FSK: Frequency shift keying Voltage: send a higher voltage to the user port periodically
CID Type	Specify the port's Caller ID type. as-type: the AS (Alerting Signal) type of CID, 0-6 DEFVAL: (determine the setting based on the country code) CID during ring DTAS (Dual Tone Alerting Signal) CID before ring RPAS (Ringing Pulse Alerting Signal) CID before ring LR Line Reversal DTAS CID before ring LR CID before ring CID before ring
Payload Type	Specify the port's payload type of CID. DEFVAL (determine the setting based on the country code) MDMF (Multiple Data Message Format) which transmits caller name, number, date and time. SDMF (Single Data Message Format) which transmits caller number, date and time. ETSI MDMF ETSI SDMF DTMF UK MDMF UK SDMF Japanese MDMF

Table 90 Port > SIP (continued)

LABEL	DESCRIPTION
Hook Flash Detection	Specify how long (in milliseconds) a user has to press the flash key to register its use. DEFVAL: Not specified (use the value defined in the currently selected country code).
Apply	Click Apply to save your changes.
Cancel	Click Cancel to begin configuring the screen again.
SIP	
Account	Specify the account for SIP registration.
Password	Set the password for authorization of SIP messages. Use up to 31 printable characters.
Hotline	Select the check box to have the IES automatically dial a number when someone picks up the phone connected to the selected port. Hotline-no: Specify the telephone number to call. Use up to 31 characters. Only alphanumeric characters and '+' are allowed. Note: '+' is only allowed as the first character. Hotline timeout: the number of seconds the IES waits before dialing the hotline number. 0 means dial immediately.
Name	Specify the name for SIP registration.
Polarity-Reverse	Turn polarity reversal on or off. Turn on polarity reversal to reverse the tip and ring after a call is established and again after it terminates. This is used for example, as a charging signal for some types of payphone.
Tel Number	Specify a telephone number of up to 16 digits for the VoIP port. Note: The telephone number must be unique.
SIP Profile	Select the SIP settings profile the port uses for voice traffic.
SVC Profile	Select the VoIP SIP Service profile of SIP Call service settings for the port.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to begin configuring the screen again.

12.12 FE

Click **Port > FE** to open the following screen. Click the index number to configure the Fast Ethernet settings of ports of the specified slot.

Figure 141 Port > FE

Index	State	Card Type	Uptime
1	Active	MSC1002GA	160:05:45
2	Active	VOP1164A-61	160:04:32
3	Active	ALC1132A-51	160:04:57
<u>4</u>	Active	ELC1132A-45	160:04:15
5	Active	VLC1124A-51	160:03:57

Figure 142 Port > FE Port Setup - Slot

FE Port Setup: Slot 4

Index	Active ☐	Name	speed-duplex	flow control	Alarm Profile
1	☐		auto ▼	inactive ▼	DEFVAL ▼
2	☐		auto ▼	inactive ▼	DEFVAL ▼
3	☐		auto ▼	inactive ▼	DEFVAL ▼
4	☐		auto ▼	inactive ▼	DEFVAL ▼
5	☐		auto ▼	inactive ▼	DEFVAL ▼
6	☐		auto ▼	inactive ▼	DEFVAL ▼
7	☐		auto ▼	inactive ▼	DEFVAL ▼
8	☐		auto ▼	inactive ▼	DEFVAL ▼
9	☐		auto ▼	inactive ▼	DEFVAL ▼
10	☐		auto ▼	inactive ▼	DEFVAL ▼
11	☐		auto ▼	inactive ▼	DEFVAL ▼
12	☐		auto ▼	inactive ▼	DEFVAL ▼
13	☐		auto ▼	inactive ▼	DEFVAL ▼
14	☐		auto ▼	inactive ▼	DEFVAL ▼
15	☐		auto ▼	inactive ▼	DEFVAL ▼
16	☐		auto ▼	inactive ▼	DEFVAL ▼
17	☐		auto ▼	inactive ▼	DEFVAL ▼
18	☐		auto ▼	inactive ▼	DEFVAL ▼
19	☐		auto ▼	inactive ▼	DEFVAL ▼
20	☐		auto ▼	inactive ▼	DEFVAL ▼
21	☐		auto ▼	inactive ▼	DEFVAL ▼
22	☐		auto ▼	inactive ▼	DEFVAL ▼
23	☐		auto ▼	inactive ▼	DEFVAL ▼
24	☐		auto ▼	inactive ▼	DEFVAL ▼
25	☐		auto ▼	inactive ▼	DEFVAL ▼
26	☐		auto ▼	inactive ▼	DEFVAL ▼
27	☐		auto ▼	inactive ▼	DEFVAL ▼
28	☐		auto ▼	inactive ▼	DEFVAL ▼
29	☐		auto ▼	inactive ▼	DEFVAL ▼
30	☐		auto ▼	inactive ▼	DEFVAL ▼
31	☐		auto ▼	inactive ▼	DEFVAL ▼
32	☐		auto ▼	inactive ▼	DEFVAL ▼

Apply Cancel

The following table describes the fields in this screen.

Table 91 Port > FE Port Setup - Slot

LABEL	DESCRIPTION
Index	This field displays the index number of a port. Click the index number to go to the screen as shown in the following figure.
Active	Select the check box to enable the specified port on the line card.
Name	Type the name of up to 31 printable characters for the specified port.

Table 91 Port > FE Port Setup - Slot (continued)

LABEL	DESCRIPTION
speed-duplex	Configures the Fast Ethernet port's speed and duplex mode. The default is auto. auto: auto negotiation 10M-Half: fixed to 10Base-T half duplex 10M-Full: fixed to 10Base-T full duplex 100M-Half: fixed to 100Base-TX half duplex 100M-Full: fixed to 100Base-TX full duplex
flow control	Turn the Fast Ethernet port's flow control on or off.
Alarm Profile	Select an FE alarm profile for the specified FE port to reference.
Apply	Click Apply to save your changes in this screen.
Cancel	Click Cancel to begin configuring the screen again.

Use the **Slot** and **Port** drop-down list boxes to select a subscriber port, and click **Setup** to configure the FE port settings of the specified port.

Figure 143 Port > FE Port Setup

The following table describes the fields in this screen.

Table 92 Port > FE

LABEL	DESCRIPTION
Slot	Use the drop-down list boxes to select the port on an active FE line card you want to configure.
Port	
Load	Click this to display the port's current settings.
Active	Select the check box to enable the specified port on the line card.
Name	Type the name of up to 31 printable characters for the specified port.

Table 92 Port > FE (continued)

LABEL	DESCRIPTION
speed-duplex	Configures the Fast Ethernet port's speed and duplex mode. The default is auto. auto: auto negotiation 10M-Half: fixed to 10Base-T half duplex 10M-Full: fixed to 10Base-T full duplex 100M-Half: fixed to 100Base-TX half duplex 100M-Full: fixed to 100Base-TX full duplex
flow control	Turn the Fast Ethernet port's flow control on or off.
Alarm Profile	Select an FE alarm profile for the specified FE port to reference.
Apply	Click Apply to save your changes in this screen.
Cancel	Click Cancel to begin configuring the screen again.

CHAPTER 13

Profile Screens

This chapter describes how to configure profiles to use in assigning settings to the subscriber ports.

13.1 Profiles Overview

A profile is a list of settings that you define. Then you can use them to configure one or more individual ports or PVCs. You cannot delete or modify the DEFVAL profiles.

13.2 Access Control List (ACL) Screen

An ACL (Access Control List) profile allows the system to classify and perform actions on the upstream traffic. Each ACL profile consists of a rule and an action.

Use this screen to set up ACL profiles. Click **Profile** > **ACL** to display the following screen.

Figure 144 Profile > ACL

ACL Profile

Name

Rule

☐ Source MAC/OUI

☐ Destination MAC/OUI

☐ Source IP IPv4 / IPv4+mask / IPv6

☐ Destination IP IPv4 / IPv4+mask / IPv6

☐ IP Precedence

☐ DSCP [0 ~ 63]

☐ Traffic Class [0 ~ 255]

☐ Next Header [1 ~ 255]

☐ Source L4 Port ~ [0 ~ 65535]

☐ Destination L4 Port ~ [0 ~ 65535]

☐ Ethertype [0x0000 ~ 0xFFFF]

☐ Inner VID [1~4093]

☐ Inner Pbit

☐ Outer VID [1~4093]

☐ Outer Pbit

☐ Protocol [0 ~ 255]

Action

☐ Drop

☐ Change DSCP [0 ~ 63]

☐ Change Traffic Class [0 ~ 255]

☐ Change Inner Pbit

☐ Change Outer Pbit

☐ Change QoS Level

☐ Rate limit [32 ~ 100000] in kbps

Apply

New

Cancel

Index

Name

Select

Modify

Delete

The following table describes the labels in this screen.

Table 93 Profile > ACL

LABEL	DESCRIPTION
Name	Enter a descriptive name for the ACL profile. The name can be 1-31 printable ASCII characters long. Spaces are not allowed.
Rule	
Source/Destination MAC/OUI	Select the check boxes to type the source/destination MAC address or MAC Organization Unit Identifier (OUI).
Source/Destination IP	Select the check boxes to type the source/destination IP address.
IP Precedence	Select the check box to specify the IP precedence (0-7).
DSCP	Select the check box to specify the IP DSCP (0-63).
Traffic Class	Select the check box to specify the IPv6 traffic class (0-255).

IES4105 User's Guide

168

Table 93 Profile > ACL (continued)

LABEL	DESCRIPTION
Next Header	Select the check box to specify the IPv6 next header (0-255).
Source/Destination L4 Port	Select the check box to specify the layer 4 source/destination port.
Ethertype	Select the check box to specify the Ethernet type in hexadecimal.
Inner VID	Select the check box to specify an inner VLAN ID.
Inner Pbit	Select the check box to specify an inner VLAN priority bit.
Outer VID	Select the check box to specify an outer VLAN ID.
Outer Pbit	Select the check box to specify an outer VLAN priority bit.
Protocol	Select the check box to specify an IP protocol.
Action	
Drop	Select the check box if you want to discard packets that match the profiles.
Change DSCP	Select the check box to change the IP DSCP of matching packets to the specified one.
Change Traffic Class	Select the check box to change the IPv6 traffic class of matching packets.
Change Inner Pbit	Select the check box to change the inner VLAN priority bit of matching packets to the specified one.
Change Outer Pbit	Select the check box to change the outer VLAN priority bit of matching packets to the specified one.
Change QoS Level	Select the check box to change the QoS level of matched packets.
Rate limit	Select the check box if you want to limit the receiving rate for packets that match the profile.
Apply	Select Apply to save your changes in this screen.
New	While you are modifying a profile, you can click New to start configuring a fresh profile without saving your changes.
Cancel	Select Cancel to start configuring the screen again.
Index	This is an incremental number indicating the order in which the profiles were created.
Name	This is the name of the profile.
Select	Select the profile you wish to load or delete.
Modify	Select a profile and click this in order to edit its configuration.
Delete	Select a profile and click this to delete the profile. Once deleted, information cannot be retrieved.

13.3 Enet Alarm Profile Screens

Click **Profile > Enet Alarm Profile** to configure alarm profiles for the Gigabit Ethernet ports. These define Ethernet port alarm thresholds. The system sends an alarm trap and generates a syslog entry when the thresholds of the alarm profile are exceeded.

Figure 145 Profile > Enet Alarm Profile

Enet Alarm Profile

Name

15min-collision-threshold

15min-64Octets-threshold

15min-127Octets-threshold

15min-255Octets-threshold

15min-511Octets-threshold

15min-1023Octets-threshold

15min-1518Octets-threshold

15min-1522Octets-threshold

	RX	TX
15min-Octets-threshold	0	0
15min-Pkts-threshold	0	0
15min-BcastPkts-threshold	0	0
15min-McastPkts-threshold	0	0
15min-Crc-threshold	0	
15min-Under-threshold	0	
15min-Over-threshold	0	
15min-Frag-threshold	0	

threshold range: [0 ~ 18446744073709551615]

Index	Name	Select
1	DEFVAL	☐

The following table describes the fields in this screen.

Table 94 Profile > Enet Alarm Profile

LABEL	DESCRIPTION
Name	Enter a descriptive name for identification purposes.
15min-collision-threshold	Specify the number of frames for which transmission failed due to excessive collisions allowed to receive or transmit in any 15-minute period. Excessive collision is defined as the number of maximum collisions before the retransmission count is reset.
15min-64octets-threshold	Specify the number of frames 64 octets or less in length allowed to receive or transmit in any 15-minute period.
15min-127octets-threshold	Specify the number of frames 65 to 127 octets in length allowed to receive or transmit in any 15-minute period.
15min-255octets-threshold	Specify the number of frames 128 to 255 octets in length allowed to receive or transmit in any 15-minute period.
15min-511octets-threshold	Specify the number of frames 256 to 511 octets in length allowed to receive or transmit in any 15-minute period.

Table 94 Profile > Enet Alarm Profile (continued)

LABEL	DESCRIPTION
15min-1023octets-threshold	Specify the number of frames 512 to 1023 octets in length allowed to receive or transmit in any 15-minute period.
15min-1518octets-threshold	Specify the number of frames 1024 to 1518 octets in length allowed to receive or transmit in any 15-minute period.
15min-1522octets-threshold	Specify the number of frames 1519 to 1522 octets in length allowed to receive or transmit in any 15-minute period.
RX/TX	Received and transmitted thresholds.
15min-Octets-threshold	Specify the number of octets of Ethernet frames allowed to receive or transmit in any 15-minute period.
15min-Pkts-threshold	Specify the number of packets allowed to receive or transmit in any 15-minute period.
15min-BcastPkts-threshold	Specify the number of broadcast packets allowed to receive or transmit in any 15-minute period.
15min-McastPkts-threshold	Specify the number of multicast packets allowed to receive or transmit in any 15-minute period.
15min-Crc-threshold	Specify the number of CRC (Cyclical Redundancy Check) alignment errors allowed to be received in any 15-minute period.
15min-Under-threshold	Specify the number of packets that were too small allowed to be received in any 15-minute period.
15min-Over-threshold	Specify the number of packets that were too big allowed to receive in any 15-minute period.
15min-Frag-threshold	Specify the number of fragmented frames allowed to receive in any 15-minute period.
Apply	Click Apply to save your changes in this screen.
New	While you are modifying a profile, you can click New to start configuring a fresh profile without saving your changes.
Cancel	Click Cancel to start configuring this screen again.
Index	This is the number of an Enet alarm profile.
Name	This field displays the descriptive name of a profile.
Modify	Select a profile's Select radio button and click Modify to edit the profile.
Delete	Select a profile's Select radio button and click Delete to remove the profile.

13.4 DSL Screens

Click **Profile > DSL** to open the following screens. Use these screens to configure DSL line profiles, channel profiles, and template profiles.

13.4.1 Line Profile Screen

Click **Profile > DSL > Line Profile** to open the screen as shown next. Use the screen to add, edit, or delete a DSL line profile.

Figure 146 Profile > DSL > Line Profile

Line Profile

Line Profile Channel Profile Template Profile

Profile Name

Line

Template Using Counter

0

VDSL2 Profile

☒ 8a
 ☒ 8b
 ☒ 8c
 ☒ 8d
 ☒ 12a
 ☒ 12b
 ☒ 17a

Transmission Type

☒ vdsl2
 ☒ adsl2+
 ☒ adsl2
 ☒ gdmr
 ☐ t1413
 ☐ glite
 ☐ annex-m
 ☐ annex-l
 ☐ annex-j
 ☐ annex-i

XDSL2 Mode

g9932annexa

Class Mask

998or997-m1c

Limit Mask

d32

US0 Band

Enable

US0 Mask

eu32

Bit Swap

Downstream

Enable

Upstream

Enable

Rate Mode

Downstream

rainit

Upstream

rainit

Up Shift SNR [0 ~ 310] 0.1dB

Downstream

90

Upstream

90

Down Shift SNR [0 ~ 310] 0.1dB

Downstream

30

Upstream

30

Up Shift Time [0 ~ 16383] sec

Downstream

30

Upstream

30

Down Shift Time [0 ~ 16383] sec

Downstream

30

Upstream

30

Target SNR [0 ~ 310] 0.1dB

Downstream

60

Upstream

60

Max SNR [0 ~ 310] 0.1dB

Downstream

310

Upstream

310

Min SNR [0 ~ 310] 0.1dB

Downstream

0

Upstream

0

Min Overhead Rate [4 ~ 236] kbps

Downstream

4

Upstream

4

Max Tx Power [0 ~ 255] 0.1dBm

Downstream

200

Upstream

130

Max Rx Power [-255 ~ 255] 0.1dBm

Downstream

Upstream

130

Power Management

Modify

RFI Band

Modify

DPBO

Modify

UPBO

Modify

EPSP

Modify

PSD MASK

Modify

Virtual Noise

Modify

Apply

New

Cancel

Index	Name	VDSL2 Profile	Select
1	DEFVAL	8a 8b 8c 8d 12a 12b 17a	☒
2	Line	8a 8b 8c 8d 12a 12b 17a	☐

Modify

Delete

The following table describes the labels in this screen.

Table 95 Profile > DSL > Line Profile

LABEL	DESCRIPTION
Profile Name	Enter a descriptive name for identification purposes.
Template Using Counter	This field displays the number of line templates related to the line profile.
VDSL2 Profile	Specify the VDSL2 profiles you want to apply to this line profile. See page 405 for detailed information on VDSL2 profile.
Transmission Type	Specify the transmission standard for this profile.
XDSL2 Mode	This displays the transmission standard for this profile.
Class Mask	A class mask is a combination of several PSD masks according to the PSD mask types. The available options vary depending on the selection in the Transmission Type field.
Limit Mask	Select a PSD limit mask you want the system to use.
US0 Band	Specify whether you want the system to automatically activate the upstream band (Enable) or not (Disable) when necessary. Select Enable to have CPE and the system use the upstream band 0 for upstream traffic over long distances. If you select Disable , the CPE may not be able to transmit data over long distances.
US0 Mask	Select a limit mask you want the system to use for the upstream band 0.
Downstream / Upstream	
Bit Swap	Select Enable to allow on-line bits and power reallocation among the allowed sub-carriers without service interruption or errors. This helps to keep transmission data rates on a high Signal-to-Noise Ratio (SNR) VDSL2 line. Select Disable to deactivate it.
Rate Mode	Specify the downstream rate adaption mode. manual: the system fixes the transmission rate as the maximum net data rate and disables transmission rate adjustment. rainit: the system keeps the transmission rate negotiated between the system and CPE devices. It ranges from the configured minimum to the maximum net data rate based on the initial line condition. dynamicra: if the system dynamically changes the transmission rate negotiated between the system and CPE devices during initialization as well as during SHOWTIME status.
Up Shift SNR	Enter the number of decibels (in 0.1 dB) for the line's up-shift SNR margin threshold. When the line's signal-to-noise margin goes above this number, the system attempts to use a higher transmission rate.
Down Shift SNR	Enter the number of decibels (in 0.1 dB) for the line's down-shift SNR margin threshold. When the line's signal-to-noise margin goes below this number, the system attempts to use a lower transmission rate.
Up Shift Time	Enter the number of seconds to wait before using a higher transmission rate when the line's SNR margin is over the up-shift SNR margin threshold.
Down Shift Time	Enter the number of seconds to wait before using a lower transmission rate when the line's SNR margin is less than the down-shift SNR margin threshold.
Target SNR	Enter the target downstream and downstream SNR margin.
Max SNR	Enter the maximum SNR margin allowed on the line.
Min SNR	Enter the minimum downstream and upstream SNR margin accepted on the line to which this profile applies.
Min Overhead Rate	Enter the minimum transmission rate reserved for a line's overhead channel. Both the system and CPE device use the overhead channel of a line to get transmission statistics with each other.

Table 95 Profile > DSL > Line Profile (continued)

LABEL	DESCRIPTION
Max Tx Power	Enter the maximum transmission power in dBm the system uses for Downstream traffic. Enter the maximum transmission power the CPE uses for Upstream traffic.
Max Rx Power	Enter the maximum receiving power in dB for Upstream traffic.
Power Management	Click the Modify link to take you to a screen where you can configure power management settings. See Section 13.4.1.1 on page 174 for details.
RFI Band	Click the Modify link to take you to a screen where you can configure RFI band settings. See Section 13.4.1.2 on page 175 for details.
DPBO	Click the Modify link to take you to a screen where you can configure DPBO settings. See Section 13.4.1.3 on page 176 for details.
UPBO	Click the Modify link to take you to a screen where you can configure UPBO settings. See Section 13.4.1.4 on page 177 for details.
EPSP	Click the Modify link to take you to a screen where you can configure EPSP settings. See Section 13.4.1.5 on page 178 for details.
PSD Mask	Click the Modify link to take you to a screen where you can configure PSD mask settings. See Section 13.4.1.6 on page 179 for details.
Virtual Noise	Click the Modify link to take you to a screen where you can configure virtual noise settings. See Section 13.4.1.7 on page 181 for details.
Apply	Click Apply to save your changes in this screen.
New	While you are modifying a profile, you can click New to start configuring a fresh profile without saving your changes.
Cancel	Click Cancel to start configuring the screen again.
Index	This is an incremental number indicating the order in which the line profiles were created.
Name	This is the name of the line profile.
VDSL2 Profile	This displays the VDSL2 profiles applied to a line profile.
Select	Select the line profile you wish to load or delete.
Modify	Select a line profile and click this in order to edit its configuration.
Delete	Select a line profile and click this to delete the profile. Once deleted, information cannot be retrieved.

13.4.1.1 Line Profile > Power Management

Click the **Modify** link next to the **Power Management** field in the **Line Profile** screen to open the screen as shown next. Use the screen to configure the power management settings.

Figure 147 Profile > DSL > Line Profile > Power Management

Power Management

Profile Name: Line

Mode: disable

I0-time: 255 [0 ~ 255] sec

I2-time: 255 [0 ~ 255] sec

I2 Power Down Step: 1 [0 ~ 15] dB

I2 Power Down Max: 6 [0 ~ 15] dB

Apply Cancel

The following table describes the fields in this screen.

Table 96 Profile > DSL > Line Profile > Power Management

LABEL	DESCRIPTION
Profile Name	This displays the specified profile name.
Mode	Specify the power management operating mode. disable : disable power management mode. allow-l3 : DSL can automatically change to Idle (L3) state. allow-l2 : DSL can automatically change to low power (L2) state. allow-both : DSL can automatically change to Idle (L3) and low power (L2) state.
L0-time	Specify the time to stay in L0 (full power) mode.
L2-time	Specify the time to wait before performing another power trim in L2 mode.
L2 Power Down Step	Specify the maximum total aggregate power reduction in dB per power trim in L2 mode.
L2 Power Down Max	Specify the maximum total aggregate power reduction in dB in L2 mode.
Apply	Click Apply to save your changes in this screen.
Cancel	Click Cancel to start configuring the screen again.

13.4.1.2 Line Profile > RFI Band

Click the **Modify** link next to the **RFI Band** field in the **Line Profile** screen to open the screen as shown next. Use this screen to specify the RFI bands through which the system and VDSL CPE devices should avoid transmitting data according to your location. See [RFI \(Radio Frequency Interference\) on page 407](#).

Figure 148 Profile > DSL > Line Profile > RFI Band

Break Point	start		stop	
	Start Carrier[0 ~ 4095]	Frequency (kHz)	End Carrier[0 ~ 4095]	Frequency (kHz)
1	5	21.56	190	819.38
2		0		0
3		0		0
4		0		0
5		0		0
6		0		0
7		0		0
8		0		0
9		0		0
10		0		0
11		0		0
12		0		0
13		0		0
14		0		0
15		0		0
16		0		0

The following table describes the fields in this screen.

Table 97 Profile > DSL > Line Profile > RFI Band

LABEL	DESCRIPTION
Profile Name	This displays the specified profile name.
Start / Stop	Use these columns below the field to specify the starting/ending frequencies for each RFI band.
Break Point	This index number identifies each RFI band.
Start/End Carrier	This is a sub-channel of a VDSL band. Enter an increased number (than previous row) from 0 to 4095.
Frequency	This read-only field displays a frequency that equals the carrier index multiple 4.3125 dBm/Hz. This field automatically calculates after a carrier value is entered.
Apply	Click Apply to save your changes in this screen.
Cancel	Click Cancel to start configuring the screen again.

13.4.1.3 Line Profile > DPBO

Click the **Modify** link next to the **DPBO** field in the **Line Profile** screen to open the screen as shown next. Use this screen to configure Downstream Power Back-Off (DPBO) settings. See [DPBO on page 406](#).

Figure 149 Profile > DSL > Line Profile > DPBO

Parameter	Value	Range/Step
ESEL	0	[0 ~ 511], 0: 0dB, 511: 255.5dB in step of 0.5 dB
ESCMA	256	[0 ~ 640], scalar value -1~1.5 in step of 1/256
ESCMB	512	[0 ~ 640], scalar value -1~1.5 in step of 1/256
ESCMC	256	[0 ~ 640], scalar value -1~1.5 in step of 1/256
MUS	180	[0 ~ 255], 0: 0dBm/Hz, 255: -127.5dBm/Hz in step of 0.5 dBm/Hz
FMAX	512	[32 ~ 6956], 32: 138KHz, 6956: 29997.75KHz in step of 4.3125KHz
FMIN	32	[0 ~ 2048], 0: 0KHz, 2048: 8832KHz in step of 4.3125KHz
EPSP PSDID	psd_co	

The following table describes the fields in this screen.

Table 98 Profile > DSL > Line Profile > DPBO

LABEL	DESCRIPTION
Profile Name	This displays the specified profile name.
ESEL	Specify the electrical length of the cable between the system and CPE devices.
ESCMA, ESCMB, ESCMC	These parameters define a cable model that is used to describe the frequency dependent loss of exchange-side cables.
MUS	This defines the assumed minimum usable received PSD mask (in dBm/Hz) for exchange based services, used to modify parameter FMAX defined below. Enter from 0 to 255 to set the PSD to 0~-127.5 dBm/Hz in steps of -0.5 dBm.
FMAX	This defines the maximum frequency at which DPBO may be applied. Enter from 138 kHz to 29997.75 kHz in steps of 4.3125 kHz.
FMIN	This defines the minimum frequency from which the DPBO shall be applied. Enter from 0 kHz to 8832 kHz in steps of 4.3125 kHz.
EPSP PSDID	Specify the DPBO standard PSD mask. EPSP PSDID defines the PSD mask that is assumed to be exchanged at CO.
Apply	Click Apply to save your changes in this screen.
Cancel	Click Cancel to start configuring the screen again.

13.4.1.4 Line Profile > UPBO

Click the **Modify** link next to the **UPBO** field in the **Line Profile** screen to open the screen as shown next. Use this screen to configure Upstream Power Back-Off (UPBO) settings. See [UPBO on page 405](#).

Figure 150 Profile > DSL > Line Profile > UPBO

	A [4000 ~ 8095] in 0.01 dBm/Hz	B [0 ~ 4095] in 0.01 dBm/Hz
UpStream Band 0	5650	1019
UpStream Band 1	5650	614
UpStream Band 2	4000	0
UpStream Band 3	4000	0

The following table describes the fields in this screen.

Table 99 Profile > DSL > Line Profile > UPBO

LABEL	DESCRIPTION
Profile Name	This displays the specified profile name.
Force Mode	Select Disable to turn UPBO off. Select Auto to enable UPBO and CPE devices' PSD adjustment based on the negotiation result with the IES. Select Override to force CPE devices to use the electrical length defined by the IES (in the UPBOKL field below) to compute their UPBO.
UPBOKL	Specify the electrical length (0-128 dB) of the cable between the system and CPE devices.
Upstream Band 0-3	Specify 4000-8095 (0.01 dBm/Hz) for parameter A which defines the original band shape. Specify 0-4095 (0.01 dBm/Hz) for parameter B which defines the power back-off degree.
Apply	Click Apply to save your changes in this screen.
Cancel	Click Cancel to start configuring the screen again.

13.4.1.5 Line Profile > EPSD

Click the **Modify** link next to the **EPSD** field in the **Line Profile** screen to open the screen as shown next. Use this screen to configure EPSD settings: the PSD mask that is assumed to be permitted at the exchange.

Figure 151 Profile > DSL > Line Profile > EPSD

Break Point	PointSD	Tone Index[0 ~ 4095]	PSD[0 ~ 190]	PSD (dBm)
1		1	120	-60.0
2		32	120	-60.0
3		33	80	-40.0
4		255	80	-40.0
5		376	100	-50.0
6		511	103	-51.5
7		512	160	-80.0
8				0
9				0
10				0
11				0
12				0
13				0
14				0
15				0
16				0

Apply Cancel

The following table describes the fields in this screen.

Table 100 Profile > DSL > Line Profile > EPSD

LABEL	DESCRIPTION
Profile Name	This displays the specified profile name.
Break Point Point SD	This index number identifies each incremental break point.
Tone Index	A tone is a sub-channel of VDSL band. DMT divides VDSL bands into many 4.3125 kHz tones. Enter an increased number (than previous row) from 0 to 4095 in this field.
PSD	Enter 0-190 to represent 0~-95 dBm/Hz in steps of -0.5 dBm/Hz to set the PSD level for specific tones. This sets the highest transmit PSD level permitted for individual tones.
PSD (dBm/Hz)	This field displays the corresponding PSD value in units of dBm/Hz.
Apply	Click Apply to save your changes in this screen.
Cancel	Click Cancel to start configuring the screen again.

13.4.1.6 Line Profile > PSD Mask

Click the **Modify** link next to the **PSD Mask** field in the **Line Profile** screen to open the screen as shown next. Power Spectral Density (PSD) defines the distribution of a VDSL line's power in the frequency domain. A PSD mask is a template that specifies the maximum allowable PSD for a line. Use this screen to adjust PSD levels for tones based on the scope down the limit PSD masks.

Figure 152 Profile > DSL > Line Profile > PSD Mask

PSD Mask

Profile Name

Line

Upstream	Break Point	Tone Index[0 ~ 4095]	Frequency (kHz)	PSD[0 ~ 190]	PSD (dBm/Hz)
	1		0		0
	2		0		0
	3		0		0
	4		0		0
	5		0		0
	6		0		0
	7		0		0
	8		0		0
	9		0		0
	10		0		0
	11		0		0
	12		0		0
	13		0		0
	14		0		0
	15		0		0
	16		0		0
Downstream					
	1		0		0
	2		0		0
	3		0		0
	4		0		0
	5		0		0
	6		0		0
	7		0		0
	8		0		0
	9		0		0
	10		0		0
	11		0		0
	12		0		0
	13		0		0
	14		0		0
	15		0		0
	16		0		0
	17		0		0
	18		0		0
	19		0		0
	20		0		0
	21		0		0
	22		0		0
	23		0		0
	24		0		0
	25		0		0
	26		0		0
	27		0		0
	28		0		0
	29		0		0
	30		0		0
	31		0		0
	32		0		0

Apply

Cancel

The following table describes the fields in this screen.

Table 101 Profile > DSL > Line Profile > PSD Mask

LABEL	DESCRIPTION
Profile Name	This displays the specified profile name.
Upstream	Configure the following settings for the CPEs-to-the-IES direction.
Downstream	Configure the following settings for the IES-to-CPEs direction.

Table 101 Profile > DSL > Line Profile > PSD Mask (continued)

LABEL	DESCRIPTION
Break Point	This index number identifies each incremental break point.
Tone Index	A tone is a sub-channel of DSL band. DMT divides VDSL bands into many 4.3125 kHz tones. Enter an increased number (than previous row) from 0 to 4095 in this field.
Frequency (kHz)	This read-only field displays a frequency that equals the tone index multiple 4.3125 dBm/Hz. This field automatically calculates after a Tone index value is entered.
PSD	Enter 0-190 to represent 0~-95 dBm/Hz in steps of -0.5 dBm/Hz to set the PSD level for specific tones. This sets the highest transmit PSD level permitted for individual tones.
PSD (dBm/Hz)	This field displays the corresponding PSD value in units of dBm/Hz.
Apply	Click Apply to save your changes in this screen.
Cancel	Click Cancel to start configuring the screen again.

13.4.1.7 Line Profile > Virtual Noise

Click the **Modify** link next to the **Virtual Noise** field in the **Line Profile** screen to open the screen as shown next. Use this screen to configure virtual noise settings for a VDSL2 line profile.

Figure 153 Profile > DSL > Line Profile > Virtual Noise

Virtual Noise

Profile Name
Line

SNR Mode US
Disable

SNR Mode DS
Disable

Upstream	Break Point	Tone Index [0 ~ 4095]	Frequency (kHz)	PSD [0 ~ 200 or 255]	PSD (dBm/Hz)
	1		0		0
	2		0		0
	3		0		0
	4		0		0
	5		0		0
	6		0		0
	7		0		0
	8		0		0
	9		0		0
	10		0		0
	11		0		0
	12		0		0
	13		0		0
	14		0		0
	15		0		0
	16		0		0
Downstream					
	1		0		0
	2		0		0
	3		0		0
	4		0		0
	5		0		0
	6		0		0
	7		0		0
	8		0		0
	9		0		0
	10		0		0
	11		0		0
	12		0		0
	13		0		0
	14		0		0
	15		0		0
	16		0		0
	17		0		0
	18		0		0
	19		0		0
	20		0		0
	21		0		0
	22		0		0
	23		0		0
	24		0		0
	25		0		0
	26		0		0
	27		0		0
	28		0		0
	29		0		0
	30		0		0
	31		0		0
	32		0		0

Apply
Cancel

The following table describes the fields in this screen.

Table 102 Profile > DSL > Line Profile > Virtual Noise

LABEL	DESCRIPTION
Profile Name	This displays the specified profile name.
SNR Mode US/ SNR Mode DS	Select whether you want to enable virtual noise (Enable) or not (Disable) for downstream and upstream transmission. Note: For a poor quality subscriber line, you should enable this and configure virtual noise on tones where noise may occur. Note: The higher the virtual noise, the lower the line speed.
Upstream	Configure the following settings for the CPEs-to-the-IES direction.
Downstream	Configure the following settings for the IES-to-CPEs direction.
Break Point	This index number identifies each incremental break point.
Tone Index	A tone is a sub-channel of DSL band. DMT divides VDSL bands into many 4.3125 kHz tones. Enter an increased number (than previous row) from 0 to 4095 in this field.
Frequency (kHz)	This read-only field displays a frequency that equals the tone index multiple 4.3125 dBm/Hz. This field automatically calculates after a Tone index value is entered.
PSD	Enter 0-190 to represent 0~-95 dBm/Hz in steps of -0.5 dBm/Hz to set the PSD level for specific tones. This sets the highest transmit PSD level permitted for individual tones.
PSD (dBm/Hz)	This field displays the corresponding PSD value in units of dBm/Hz.
Apply	Click Apply to save your changes in this screen.
Cancel	Click Cancel to start configuring the screen again.

13.4.2 Channel Profile Screen

Click **Profile > DSL > Channel Profile** to open the screen as shown next. Use the screen to view, add, edit, or delete channel profiles.

Figure 154 Profile > DSL > Channel Profile

Channel Profile

Line Profile **Channel Profile** Template Profile

Name

Template Using Counter

	Downstream	Upstream
PhyR Mode	Auto	Auto
Max Latency Delay	8 [0 ~ 63] ms	8 [0 ~ 63] ms
Min Rate	192 [32 ~ 128000] kbps	192 [32 ~ 128000] kbps
Max Rate	100032 [64 ~ 128000] kbps	100032 [64 ~ 128000] kbps
Min INP for 4.3125KHz	4 [0 ~ 32] 0.5symbols	4 [0 ~ 32] 0.5symbols
Min INP for 8.625KHz	4 [0 ~ 32] 0.5symbols	4 [0 ~ 32] 0.5symbols

Apply New Cancel

Index	Name	Select
1	DEFVAL	☐

Modify Delete

The following table describes the fields in this screen.

Table 103 Profile > DSL > Channel Profile

LABEL	DESCRIPTION
Name	Enter a descriptive name for identification purposes.
Template Using Counter	This field displays the number of line templates related to the channel profile.
Downstream	The parameters in this column relate to downstream transmissions.
Upstream	The parameters in this column relate to upstream transmissions.
PhyR Mode	Select Enable to use the DSL physical layer for data re-transmission when impulse noise occurs. This helps to get better link connection quality. Select Disable to turn this feature off. Select Auto to have the system enable this feature when there is no impact to the data rate.
Max Latency Delay	Type the number of milliseconds of delays used for downstream and upstream transmissions. It is recommended that you configure the same latency delays for both upstream and downstream.
Min / Max Rate	Type the minimum and maximum upstream/downstream transmission rates in kbps for this profile.
Min INP for 4.3125 KHz	Configure the upstream/downstream minimum Impulse Noise Protection (INP) for a 4.3125 kHz carrier space DSL look.
Min INP for 8.625 KHz	Configure the upstream/downstream minimum Impulse Noise Protection (INP) for a 8.625 kHz carrier space DSL look.
Apply	Click Apply to save your changes in this screen.
New	While you are modifying a profile, you can click New to start configuring a fresh profile without saving your changes.
Cancel	Click Cancel to start configuring this screen again.
Index	This is the number of a DSL channel profile.
Name	This field displays the descriptive name of a profile.
Modify	Select a profile's Select radio button and click Modify to edit the profile.
Delete	Select a profile's Select radio button and click Delete to remove the profile.

13.4.3 Template Profile Screen

DSL templates each use one line profile and one channel profile. Use this screen to add, modify or delete a DSL template. To configure or view DSL templates, click **Profile > DSL > Template Profile** to open the screen as shown next.

Figure 155 Profile > DSL > Template Profile

The following table describes the fields in this screen.

Table 104 Profile > DSL > Template Profile

LABEL	DESCRIPTION
Name	Enter a descriptive name for identification purposes.
Line Profile Name	Select a line profile for this DSL profile.
Channel Profile Name	Select a channel profile for this DSL profile.
Apply	Click Apply to save your changes in this screen.
New	While you are modifying a profile, you can click New to start configuring a fresh profile without saving your changes.
Cancel	Click Cancel to start configuring this screen again.
Index	This is the number of a DSL template profile.
Name	This field displays the descriptive name of a profile.
VDSL2 Line Profile	This field displays the line profile name configured in each DSL template.
VDSL2 Channel Profile	This field displays the channel profile name configured in each DSL template.
Modify	Select a profile's Select radio button and click Modify to edit the profile.
Delete	Select a profile's Select radio button and click Delete to remove the profile.

13.5 DSL Alarm Profile Screens

Click **Profile > DSL Alarm Profile** to open the following screens. Use these screens to configure alarm profiles for the DSL ports.

13.5.1 Alarm Profile Screen

DSL alarm profiles define DSL port alarm thresholds. The system sends an alarm trap and generates a syslog entry when the thresholds of the alarm profile are exceeded. Click **Profile > DSL Alarm Profile > Alarm Profile** to open the following screen.

Figure 156 Profile > DSL Alarm Profile > Alarm Profile

Alarm Profile

Alarm Profile Alarm line Profile Alarm Channel Profile Alarm Template Profile

Name

	TX	RX
15min-Bytes-threshold	0	0
15min-Pkts-threshold	0	0
15min-UnicastPkts-threshold	0	0
15min-BroadcastPkts-threshold	0	0
15min-MulticastPkts-threshold	0	0
15min-DiscardPkts-threshold	0	0

threshold range: [0 ~ 18446744073709551615]

Apply New Cancel

Index	Name	Select
1	DEFVAL	☐

Modify Delete

The following table describes the fields in this screen.

Table 105 Profile > DSL Alarm Profile > Alarm Profile

LABEL	DESCRIPTION
Name	Enter a descriptive name for identification purposes.
15min-Bytes-threshold	Specify the number of bytes allowed to transmit/receive in any 15-minute period.
15min-Pkts-threshold	Specify the number of packets allowed to transmit/receive in any 15-minute period.
15min-UnicastPkts-threshold	Specify the number of unicast packets allowed to transmit/receive in any 15-minute period.
15min-BroadcastPkts-threshold	Specify the number of broadcast packets allowed to transmit/receive in any 15-minute period.
15min-MulticastPkts-threshold	Specify the number of multicast packets allowed to transmit/receive in any 15-minute period.
15min-DiscardPkts-threshold	Specify the number of packets dropped when transmitting/receiving packets in any 15-minute period.
Apply	Click Apply to save your changes in this screen.
New	While you are modifying a profile, you can click New to start configuring a fresh profile without saving your changes.
Cancel	Click Cancel to start configuring this screen again.
Index	This is the number of a DSL template profile.
Name	This field displays the descriptive name of a profile.
Modify	Select a profile's Select radio button and click Modify to edit the profile.
Delete	Select a profile's Select radio button and click Delete to remove the profile.

13.5.2 Alarm Line Profile Screen

Click **Profile > DSL Alarm Profile > Alarm Line Profile** to open the following screen. Use this screen to view, add, edit, or delete a DSL line alarm profile. The device sends an alarm trap and generates a syslog entry when the thresholds of the alarm profile are exceeded.

Figure 157 Profile > DSL Alarm Profile > Alarm Line Profile

The following table describes the fields in this screen.

Table 106 Profile > DSL Alarm Profile > Alarm Line Profile

LABEL	DESCRIPTION
Name	Enter a descriptive name for identification purposes.
Thresh15MinFailedFullInt	Enter the number of times of a full initialization is allowed to fail within 15 minutes.
Template Using Counter	This field displays the number of alarm line templates related to the alarm line profile.
Xtur	Configure the thresholds in this column for CPE devices.
Xtuc	Configure the thresholds in this column for the system.
Thresh15MinFecs	Enter the number of Forward Error Correction Seconds (FECS) that are permitted to occur within 15 minutes.
Thresh15MinEs	Enter the number of Errored Seconds (ES) that are permitted to occur within 15 minutes.
Thresh15MinSes	Enter the number of Severely Errored Seconds (SES) that are permitted to occur within 15 minutes.
Thresh15MinLoss	Enter the number of Loss of Signals Seconds (LOSS) that are permitted to occur within 15 minutes.
Thresh15MinLofs	Enter the number of Loss of Framing Seconds (LOFS) that are permitted to occur within 15 minutes.

Table 106 Profile > DSL Alarm Profile > Alarm Line Profile (continued)

LABEL	DESCRIPTION
Thresh15MinUas	Enter the number of Unavailable Seconds (UAS) that are permitted to occur within 15 minutes.
Thresh15MinLprs	Enter the number of times of Loss of Power Seconds (LPRS) is permitted to occur within 15 minutes.
Apply	Click Apply to save your changes in this screen.
New	While you are modifying a profile, you can click New to start configuring a fresh profile without saving your changes.
Cancel	Click Cancel to start configuring this screen again.
Index	This is the number of a DSL template profile.
Name	This field displays the descriptive name of a profile.
Modify	Select a profile's Select radio button and click Modify to edit the profile.
Delete	Select a profile's Select radio button and click Delete to remove the profile.

13.5.3 Alarm Channel Profile Screen

Click **Profile > DSL Alarm Profile > Alarm Channel Profile** to open the following screen. Use this screen to view, add, edit, or delete a DSL channel alarm profile. The device sends an alarm trap and generates a syslog entry when the thresholds of the alarm profile are exceeded.

Figure 158 Profile > DSL Alarm Profile > Alarm Channel Profile

The following table describes the fields in this screen.

Table 107 Profile > DSL Alarm Profile > Alarm Channel Profile

LABEL	DESCRIPTION
Name	Enter a descriptive name for identification purposes.
Template Using Counter	This field displays the number of alarm line templates related to the alarm channel profile.
Xtur	Configure the thresholds in this column for CPE devices.
Xtuc	Configure the thresholds in this column for the system.

Table 107 Profile > DSL Alarm Profile > Alarm Channel Profile (continued)

LABEL	DESCRIPTION
Thresh15MinCoding Violations	Enter the number of Code Violation (incorrect cyclic redundancy check) that are permitted to occur within 15 minutes.
Thresh15MinCorrected	Enter the number of error blocks that can be corrected within 15 minutes.
Apply	Click Apply to save your changes in this screen.
New	While you are modifying a profile, you can click New to start configuring a fresh profile without saving your changes.
Cancel	Click Cancel to start configuring this screen again.
Index	This is the number of a DSL template profile.
Name	This field displays the descriptive name of a profile.
Modify	Select a profile's Select radio button and click Modify to edit the profile.
Delete	Select a profile's Select radio button and click Delete to remove the profile.

13.5.4 Alarm Template Profile Screen

DSL alarm templates each use one line alarm profile and one channel alarm profile. Use this screen to add, modify or delete a DSL alarm template. To configure or view DSL alarm templates, click **Profile > DSL Alarm Profile > Alarm Template Profile** to open the screen as shown next.

Figure 159 Profile > DSL Alarm Profile > Alarm Template Profile

The following table describes the fields in this screen.

Table 108 Profile > DSL Alarm Profile > Alarm Template Profile

LABEL	DESCRIPTION
Name	Enter a descriptive name for identification purposes.
Line Alarm Profile Name	Select a line alarm profile for this DSL alarm profile templates.
Channel Alarm Profile Name	Select a channel alarm profile for this DSL alarm profile templates.
Apply	Click Apply to save your changes in this screen.
New	While you are modifying a profile, you can click New to start configuring a fresh profile without saving your changes.

Table 108 Profile > DSL Alarm Profile > Alarm Template Profile (continued)

LABEL	DESCRIPTION
Cancel	Click Cancel to start configuring this screen again.
Index	This is the number of a DSL template profile.
Name	This field displays the descriptive name of a profile.
Modify	Select a profile's Select radio button and click Modify to edit the profile.
Delete	Select a profile's Select radio button and click Delete to remove the profile.

13.6 QoS Screens

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control the use of bandwidth. Without QoS, all traffic data is equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for delay-sensitive applications such as VoIP or video-on-demand (VOD).

Configure QoS to group and prioritize downstream application traffic in queues and fine-tune network performance.

- QoS applies only to the downstream traffic (traffic going to the subscribers).
- QoS limits the data rate of traffic flowing through the Device's physical queues.

13.6.1 VC-Shaping Screen

Click **Profile > QoS > VC-Shaping** to open the following screen. Use this screen to view, add, edit, or delete a Virtual Circuit (VC) shaping profile.

Figure 160 Profile > QoS > VC-Shaping

VC-Shaping Profile

VC-Shaping Shaping WRR-WFQ

Name

Depth [30 ~ 255]

Rate [32 ~ 100000] kbps

Apply New Cancel

Index	Name	Select
1	DEFVAL	☒

Modify Delete

The following table describes the fields in this screen.

Table 109 Profile > QoS > VC-Shaping

LABEL	DESCRIPTION
Name	Type a name to identify the VC-Shaping profile (you cannot change the name of the DEFVAL profile). You can use up to 31 English keyboard characters; spaces are not allowed.
Depth	Specify the maximum number of packets allowed to be queued in Queue0 to Queue7.
Rate	Specify the maximum data transmission rate.
Apply	Click Apply to save the changes in this screen.
New	While you are modifying a profile, you can click New to start configuring a fresh profile without saving your changes.
Cancel	Click Cancel to start configuring the screen again.
Index	This is the index number of the VC-Shaping profile.
Name	This is the name of the VC-Shaping profile.
Modify	Select a profile's Select radio button and click Modify to edit the profile.
Delete	Select a profile's Select radio button and click Delete to remove the profile.

13.6.2 Shaping Screen

Click **Profile > QoS > Shaping** to open the following screen. Use this screen to view, add, edit, or delete a shaping profile.

Figure 161 Profile > QoS > Shaping

The following table describes the fields in this screen.

Table 110 Profile > QoS > Shaping

LABEL	DESCRIPTION
Name	Type a name to identify the profile (you cannot change the name of the DEFVAL profile). You can use up to 31 English keyboard characters; spaces are not allowed.
Depth	Specify the maximum number of packets allowed to be queued in Queue0 to Queue7.
Rate	Specify the maximum data transmission rate of Queue0 to Queue7.
Apply	Click Apply to save the changes in this screen.

Table 110 Profile > QoS > Shaping (continued)

LABEL	DESCRIPTION
New	While you are modifying a profile, you can click New to start configuring a fresh profile without saving your changes.
Cancel	Click Cancel to start configuring the screen again.
Index	This is the index number of the Shaping profile.
Name	This is the name of the Shaping profile.
Modify	Select a profile's Select radio button and click Modify to edit the profile.
Delete	Select a profile's Select radio button and click Delete to remove the profile.

13.6.3 WRR-WFQ Screen

Click **Profile > QoS > WRR-WFQ** to open the following screen. Use this screen to view, add, edit, or delete a Weighted Round Robin (WRR)/Weighted Fair Queuing (WFQ) profile.

Figure 162 Profile > QoS > WRR-WFQ

The following table describes the fields in this screen.

Table 111 Profile > QoS > WRR-WFQ

LABEL	DESCRIPTION
Name	Type a name to identify the profile (you cannot change the name of the DEFVAL profile). You can use up to 31 English keyboard characters; spaces are not allowed.
Weight	Specify the weight of a WRR or WFQ queue.
Depth	Specify the maximum number of packets allowed to be queued in Queue0 to Queue7.
Apply	Click Apply to save the changes in this screen.
New	While you are modifying a profile, you can click New to start configuring a fresh profile without saving your changes.
Cancel	Click Cancel to start configuring the screen again.
Index	This is the index number of the WRR-WFQ profile.
Name	This is the name of the WRR-WFQ profile.
Modify	Select a profile's Select radio button and click Modify to edit the profile.
Delete	Select a profile's Select radio button and click Delete to remove the profile.

13.7 VoIP Alarm Profile Screen

VoIP alarm profiles define VoIP port alarm thresholds. The system sends an alarm trap and generates a syslog entry when the thresholds of the alarm profile are exceeded. Click **Profile > VoIP Alarm Profile** to open the following screen.

Figure 163 Profile > VoIP Alarm Profile

VoIP Alarm Profile

Name

15min-rtpElapse-threshold [0 ~ 18446744073709551615]

15min-rtpRxBytes-threshold [0 ~ 18446744073709551615]

15min-rtpRxLostPkts-threshold [0 ~ 18446744073709551615]

15min-rtpRxPkts-threshold [0 ~ 18446744073709551615]

15min-rtpTxBytes-threshold [0 ~ 18446744073709551615]

15min-rtpTxLostPkts-threshold [0 ~ 18446744073709551615]

15min-rtpTxPkts-threshold [0 ~ 18446744073709551615]

Index	Name	Select
1	DEFVAL	☐

The following table describes the fields in this screen.

Table 112 Profile > VoIP Alarm Profile

LABEL	DESCRIPTION
Name	Enter a descriptive name for identification purposes.
15min-rtpElapse-threshold	Specify the accumulated time of RTP sessions allowed in any 15-minute period. In other words, this is the amount of audio transmission time allowed within 15 minutes.
15min-rtpRxBytes-threshold	Specify the accumulated number of bytes of RTP packets that can be received in any 15-minute period.
15min-rtpRxLostPkts-threshold	Specify the number of RTP packets that can be failed to be received by the IES in any 15-minute period.
15min-rtpRxPkts-threshold	Specify the number of RTP packets that can be received in any 15-minute period.
15min-rtpTxBytes-threshold	Specify the accumulated number of bytes of RTP packets that can be transmitted in any 15-minute period.
15min-rtpTxLostPkts-threshold	Specify the number of RTP packets that can be lost during transmission in any 15-minute period.
15min-rtpTxPkts-threshold	Specify the number of RTP packets that can be transmitted in any 15-minute period.
Apply	Click Apply to save your changes in this screen.

Table 112 Profile > VoIP Alarm Profile (continued)

LABEL	DESCRIPTION
New	While you are modifying a profile, you can click New to start configuring a fresh profile without saving your changes.
Cancel	Click Cancel to start configuring this screen again.
Index	This is the number of a VoIP alarm profile.
Name	This field displays the descriptive name of a profile.
Modify	Select a profile's Select radio button and click Modify to edit the profile.
Delete	Select a profile's Select radio button and click Delete to remove the profile.

13.8 VoIP DSP Profile Screen

Use this screen to configure the VoIP Digital Signal Processing (DSP) settings. Click **Profile > VoIP DSP**. The following screen displays.

Figure 164 Profile > VoIP DSP

DSP Profile

Name:

802.1p Priority:

DSCP: [0 ~ 63]

Codec:

Codec Allowed: g711a, g711mu

Codec not Allowed: g723, g726-16, g726-24, g726-32, g726-40, g729ab

Priority:

Min Play Buffer Delay: [10 ~ 500] ms

Max Play Buffer Delay: [10 ~ 500] ms

Echo Tail:

Echo Cancel:

VAD:

g711vpi:

g723vpi:

g726vpi:

g729vpi:

Index	Name	Select
1	DEFVAL	☒

The following table describes the labels in this screen.

Table 113 Profile > VoIP DSP

LABEL	DESCRIPTION
Name	Enter a name for this DSP profile (up to 31 ASCII characters; spaces are not allowed).
802.1p Priority	Set the IEEE 802.1p priority value (0~7) for traffic using this profile.
DSCP	Set the DiffServ Code Point (DSCP) value for traffic using this profile.
Codec Allowed	This is the list of codecs to use in negotiation for this DSP profile. The codecs are listed by priority: the system tries to use the codec at the top of the list first and, if that is not possible, tries the second, and so on.
Codec not Allowed	This is the list of codecs supported by the system but not used in this DSP profile.
<<	Use this to move the selected codec from the Not Allowed list to the Allowed list.
>>	Use this to move the selected codec from the Allowed list to the Not Allowed list.
Priority +	Use this to increase the priority of the selected codec by moving it up one place in the list.
Priority -	Use this to decrease the priority of the selected codec by moving it down one place in the list.
Min Play Buffer Delay (10~500)	This is the minimum time delay of the play buffer (10 ~ 500 milliseconds, must be less than or equal to the Max Play Buffer Delay).
Max Play Buffer Delay (10~500)	This is the maximum time delay of the play buffer (10 ~ 500 milliseconds, must be greater than or equal to the Min Play Buffer Delay).
Echo Tail	This is the echo-cancellation echo tail period (8/16/32/128 milliseconds).
Echo Cancel	Select this to enable echo cancellation.
VAD	Select this to enable Voice Activity Detection (VAD).
g711vpi	Set the Voice Packetization Interval (10ms, 20ms, 30ms or 40ms) for G.711.
g723vpi	Set the Voice Packetization Interval (30ms or 60ms) for G.723.
g726vpi	Set the Voice Packetization Interval (10ms, 20ms, 30ms or 40ms) for G.726.
g729vpi	Set the Voice Packetization Interval (10ms, 20ms, 30ms, 40ms, 50ms or 60ms) for G.729.
Apply	Click Apply to save the changes in this screen.
New	While you are modifying a profile, you can click New to start configuring a fresh profile without saving your changes.
Cancel	Click this to start configuring the screen again.
Index	This is an incremental number indicating the order in which the DSP profiles were created.
Name	This is the name of the DSP profile.
Select	Select the DSP profile you wish to load or delete.
Modify	Select a DSP profile and click this in order to edit its configuration.
Delete	Select a DSP profile and click this to delete the profile. Once deleted, information cannot be retrieved.

13.9 FE Alarm Profile Screens

Click **Profile > FE Alarm Profile** to configure alarm profiles for the FE ports. These define Fast Ethernet port alarm thresholds. The system sends an alarm trap and generates a syslog entry when the thresholds of the alarm profile are exceeded.

Figure 165 Profile > FE Alarm Profile

FE Alarm Profile

Name

15min-collision-threshold

	RX	TX
15min-Octets-threshold	0	0
15min-Pkts-threshold	0	0
15min-BcastPkts-threshold	0	0
15min-McastPkts-threshold	0	0
15min-Crc-threshold	0	
15min-Under-threshold	0	
15min-Over-threshold	0	
15min-Frag-threshold	0	
15min-64Octets-threshold	0	
15min-127Octets-threshold	0	
15min-255Octets-threshold	0	
15min-511Octets-threshold	0	
15min-1023Octets-threshold	0	
15min-1518Octets-threshold	0	

threshold range: [0 ~ 18446744073709551615]

Apply New Cancel

Index	Name	Select
1	DEFVAL	☐
2	test-FE	☐

Modify Delete

The following table describes the fields in this screen.

Table 114 Profile > FE Alarm Profile

LABEL	DESCRIPTION
Name	Enter a descriptive name for identification purposes.
15min-collision-threshold	Specify the number of frames for which transmission failed due to excessive collisions allowed to receive or transmit in any 15-minute period. Excessive collision is defined as the number of maximum collisions before the retransmission count is reset.
RX/TX	Received and transmitted thresholds.
15min-Octets-threshold	Specify the number of octets of Ethernet frames allowed to receive or transmit in any 15-minute period.
15min-Pkts-threshold	Specify the number of packets allowed to receive or transmit in any 15-minute period.
15min-BcastPkts-threshold	Specify the number of broadcast packets allowed to receive or transmit in any 15-minute period.
15min-McastPkts-threshold	Specify the number of multicast packets allowed to receive or transmit in any 15-minute period.

Table 114 Profile > FE Alarm Profile (continued)

LABEL	DESCRIPTION
15min-Crc-threshold	Specify the number of CRC (Cyclical Redundancy Check) alignment errors allowed to be received in any 15-minute period.
15min-Under-threshold	Specify the number of packets that were too small allowed to be received in any 15-minute period.
15min-Over-threshold	Specify the number of packets that were too big allowed to receive in any 15-minute period.
15min-Frag-threshold	Specify the number of fragmented frames allowed to receive in any 15-minute period.
15min-64Octets-threshold	Specify the number of frames 64 octets or less in length allowed to receive or transmit in any 15-minute period.
15min-127Octets-threshold	Specify the number of frames 65 to 127 octets in length allowed to receive or transmit in any 15-minute period.
15min-255Octets-threshold	Specify the number of frames 128 to 255 octets in length allowed to receive or transmit in any 15-minute period.
15min-511Octets-threshold	Specify the number of frames 256 to 511 octets in length allowed to receive or transmit in any 15-minute period.
15min-1023Octets-threshold	Specify the number of frames 512 to 1023 octets in length allowed to receive or transmit in any 15-minute period.
15min-1518Octets-threshold	Specify the number of frames 1024 to 1518 octets in length allowed to receive or transmit in any 15-minute period.
Apply	Click Apply to save your changes in this screen.
New	While you are modifying a profile, you can click New to start configuring a fresh profile without saving your changes.
Cancel	Click Cancel to start configuring this screen again.
Index	This is the number of an FE port alarm profile.
Name	This field displays the descriptive name of a profile.
Modify	Select a profile's Select radio button and click Modify to edit the profile.
Delete	Select a profile's Select radio button and click Delete to remove the profile.

13.10 Profile VoIP SIP Screen

This is available when using SIP firmware. Click **Profile > VoIP SIP** to configure basic SIP settings used by the VoIP line cards. See [Section 12.11 on page 159](#) to assign SIP profiles to SIP ports.

Figure 166 Profile > VoIP SIP

SIP Profile

Name

SIP Server IP/Domain Name Port [1025 ~ 65535]

Registration Server IP/Domain Name Port [1025 ~ 65535]

Proxy Server IP/Domain Name Port [1025 ~ 65535]

Dual-Server

2nd SIP Server IP/Domain Name Port [1025 ~ 65535]

2nd Registration Server IP/Domain Name Port [1025 ~ 65535]

2nd Proxy Server IP/Domain Name Port [1025 ~ 65535]

DSCP [0 ~ 63]

Switch Type

URI Type

PRACK

Keep Alive Session expiration time [90 ~ 65535] sec

RTP Port Start Port [4000 ~ 64000] End Port [5000 ~ 65000]

Registration Period Registration expiration time [120 ~ 65535] sec

Registration Retry Time [120 ~ 900] sec

Index	Name	Select
1	DEFVAL	☐
2	test	☐

The following table describes the labels in this screen.

Table 115 Profile > VoIP SIP

LABEL	DESCRIPTION
Name	Enter a descriptive name for this SIP profile. Use up to 31 ASCII characters. Spaces are not allowed.
SIP Server IP / Domain Name	Enter the IP address or domain name of the SIP server. Use up to 64 printable ASCII characters. It can be a proxy, redirect, or register SIP server.
Port	Enter the listening port number the SIP server uses.
Registration Server IP / Domain Name	If you have the IP address or domain name of the SIP registrar server, enter it here. Otherwise, enter the same address you entered in the SIP IP / Domain Name field. You can use up to 64 printable ASCII characters.
Port	If you have the IP address or domain name of the SIP registrar server, enter its listening port number. Otherwise, enter the same port number you entered in the SIP IP / Domain Name Port field.
Proxy Server IP / Domain Name	If you have the IP address or domain name of the SIP server or outbound proxy SIP server, enter it here.
Port	Enter the SIP outbound server's listening port number, if the service provider gave you one. Otherwise, enter the same port number you entered in the SIP IP / Domain Name Port field.

Table 115 Profile > VoIP SIP (continued)

LABEL	DESCRIPTION
Dual-Server	Select ON to turn on the dual server function that lets the IES use a secondary VoIP server whenever the first VoIP server goes down. Select OFF to have the IES use only one VoIP server.
2nd SIP Server IP / Domain Name	Enter the IP address or domain name of your VoIP provider's secondary SIP server. You can use up to 64 printable ASCII characters. It does not matter whether the SIP server is a proxy, redirect, or register server.
Port	Enter the secondary SIP server's listening port number, if the VoIP service provider gave you one. Otherwise, keep the default value.
2nd Registration Server IP / Domain Name	Enter the IP address or domain name of the secondary SIP registrar server, if the VoIP service provider gave you one. Otherwise, enter the same address you entered in the SIP IP / Domain Name field. You can use up to 64 printable ASCII characters.
Port	Enter the secondary SIP registrar server's listening port number, if the VoIP service provider gave you one. Otherwise, enter the same port number you entered in the SIP IP / Domain Name Port field.
2nd Proxy Server IP / Domain Name	Enter the IP address or domain name of the secondary SIP server or outbound proxy SIP server (if supplied by your VoIP service provider). The system uses this address to communicate with the SIP server.
Port	Enter the secondary SIP outbound server's listening port number, if the service provider gave you one. Otherwise, enter the same port number you entered in the SIP IP / Domain Name Port field.
DSCP	Set the DiffServ Code Point (DSCP) value for SIP and RTP traffic using this SIP profile.
Switch Type	Select the type of VoIP switch. ZTE : ZTE Soft Switch NSN : NSN Soft Switch ALU : Alcatel-Lucent-HPSS/3.0.3 Soft Switch HUA : HUAWEI Soft3000 SoftSwitch
URI Type	Use this to configure how Universal Resource Indicators (URIs) are sent. Select sip where SIP messages are sent to a domain name or IP address. Select tel where SIP messages are sent to addresses represented as telephone numbers.
PRACK	Sets whether the system sends provisional acknowledgment messages (on), or not (off).
Keep Alive	Turn SIP session keep alive on or off. When this is on, the SIP UA periodically sends SIP session refresh requests.
Session expiration time	Enter the minimum number of seconds after which the system tears down the session (if no successful session refresh has occurred).
RTP Port	SIP VoIP calls use RTP (Real time Transport Protocol) for the voice data transfer. Use these fields to specify a range of ports to use for the VoIP voice data transfer. See RFC 1889 for details on RTP.
Registration Period	Set the SIP registration period in seconds.
Registration expiration time	Enter the number of seconds the SIP account is registered with the SIP register server before the registration is downgraded to 'inactive' and all SIP functions for the account are blocked. The IES automatically tries to re-register the SIP account when one-half of this time has passed. (The SIP register server might have a different expiration, which takes priority over this setting.)
Registration Retry Time	Enter the number of seconds the IES waits before it tries again to register the SIP account, if the first try failed or if there is no response.

Table 115 Profile > VoIP SIP (continued)

LABEL	DESCRIPTION
Apply	Click Apply to save your changes in this screen.
New	While you are modifying a profile, you can click New to start configuring a fresh profile without saving your changes.
Cancel	Click Cancel to start configuring the screen again.
The bottom part of the screen lists the configured profiles.	
Index	This is the SIP profile index number.
Name	These are the names of individual profiles. The DEFVAL profile always exists, and is assigned to all ports by default.
Modify	Select a profile's Select radio button and click Modify to edit the profile.
Delete	Select a profile's Select radio button and click Delete to remove the profile.

13.11 Profile VoIP SIP Call Service Screen

This is available when using SIP firmware. Click **Profile > VoIP SIP Callservice** to configure the call service information used by the system. See [Section 12.11 on page 159](#) to assign call service profiles to SIP ports.

Figure 167 Profile > VoIP SIP Callservice

SVC Profile

Name:

First Digit Timeout: [1 ~ 255] sec

Inter Digit Timeout: [1 ~ 255] sec

Call Transfer: ▼

Call Wait: ▼

CLIP: ▼

clir: ▼

Conference: ▼

DND: ▼

Centrex: ▼

FAX: ▼

DTMF: ▼

RFC2833 Payload Type: [96 ~ 127]

Flash: ▼

sipinfo5 rc:

sipinfo6 info:

Dial Plan: ▼

Country Code:

NDC:

Dial Plan Name:

Key Pattern Name:

Index	Name	Select
1	DEFVAL	☐

The following table describes the labels in this screen.

Table 116 Profile > VoIP SIP Callservice

LABEL	DESCRIPTION
Name	Enter the name for this call service profile. Use up to 31 ASCII characters. Spaces are not allowed. This also serves as a user account if you do not configure port-specific SIP accounts.
First Digit Timeout	Set the length of time a person has to dial the first digit after taking the phone off-hook before hearing the howler tone.
Inter Digit Timeout	Set the length of time a person has between dialing digits before hearing the howler tone.
Call Transfer	Select on to turn on the call transfer service.
Call Wait	Select on to turn on the call waiting service.
CLIP	Select on to allow subscribers to present caller ID to the called party (Calling Line Identification Presentation).
clir	Select on to allow subscribers to not present caller ID to the called party (Calling Line Identification Restriction).
Conference	Select on to have the system process three-way conference calls.

Table 116 Profile > VoIP SIP Callservice (continued)

LABEL	DESCRIPTION
DND	Select on to allow subscribers to use the do not disturb service to forbid incoming calls.
Centrex	Select on to enable centrex operation.
FAX	Sets whether to send fax signals by ITU-T T38 using UDP format or through RTP packets according to ITU-T G.711. Select t38 to send fax signals according to ITU-T T-38. Select g711mu in North America and Japan. Select g711a in Europe.
DTMF	Select how to handle DTMF signals. bypass: Do not relay DTMF signals. rfc2833: Relay DTMF tones according to RFC2833. The IES transmits DTMF tones by RTP packet whose payload type is specific and adjusted by negotiated SDP. RFC2833 Payload Type: When you enable RFC 2833, set the RTP payload type (96-127) for identifying RFC 2833 packets. sipinfo: Relay DTMF signals via SIP INFO message. rfc2833like: Relay DTMF signals via SIP INFO but carrying RFC 2833 payload. plaintext: Relay DTMF signals as plain text.
Flash	Use this field to select the method the system uses to process the flash signal from a user. Invite: relays flash by SIP INVITE signal. The flash type cannot be Invite when you use the v5sip Op Mode. rfc2833: relays flash according to RFC 2833. rfc2833like: relays flash in SIP INFO packets, but carried as RFC 2833 payload sipinfo1: relays flash in SIP INFO packets (a <code>signal=16</code> message) sipinfo2: relays flash in SIP INFO packets (a <code>signal=hf</code> message) sipinfo3: relays flash in SIP INFO packets (a <code>signal=hook-flash</code> message) sipinfo4: relays flash in SIP INFO packets (a plain text "FLASH" message). sipinfo5: relays flash in SIP INFO packets (multiple SIP messages). The message content is determined by the characters you enter (up to 7) in the sipinfo5 rc field. A separate SIP INFO message is sent for each character you enter. sipinfo6: relays flash in SIP INFO packets where the content of the message is determined by the text (1-31 printable characters) you enter in the sipinfo6 info field.
Dial Plan	Select on to enable and be able to configure the dial plan feature for this profile. Country Code: Enter the E.164 Country Code, up to 7 characters. NDC: Enter the E.164 National Destination Code, up to 7 characters. Dial Plan Name: Enter the name of a dial plan table.
Key Pattern Name	Enter the name of a key pattern table for supplementary services.
Apply	Click Apply to save your changes in this screen.
New	While you are modifying a profile, you can click New to start configuring a fresh profile without saving your changes.
Cancel	Click Cancel to start configuring the screen again.
Index	This is an incremental number indicating the order in which the call service profiles were created.
Name	This is the name of the call service profile.
Select	Select the call service profile you wish to modify or delete.

Table 116 Profile > VoIP SIP Callservice (continued)

LABEL	DESCRIPTION
Modify	Select a call service profile and click this in order to edit its configuration.
Delete	Select a call service profile and click this to delete the profile. Once deleted, information cannot be retrieved.

13.12 Profile VoIP SIP Dial Plan Screen

This is available when using SIP firmware. The IES uses number plans to identify specific types of phone numbers dialed by a user, and to process the number before transmission by deleting, replacing, or adding digits according to the relevant rule. Click **Profile > VoIP SIP Dialplan** to display the following screen.

Figure 168 Profile > VoIP SIP Dialplan

Dial Plan Profile

Name

Index	Pattern	Rule
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		
21		
22		
23		
24		
25		
26		
27		
28		
29		
30		
31		
32		

Apply

New

Cancel

Index	Name	Select
1	DEFVAL	☒

Modify

Delete

The following table describes the labels in this screen.

Table 117 Profile > VoIP SIP Dialplan

LABEL	DESCRIPTION
Name	Enter the name of the number plan table. Use up to 31 ASCII characters. If you are configuring a new number plan table, you can enter the name of the new table here. If you are looking an existing number plan table, this field is not editable.
1~16	This is the pattern / rule number. When the system checks a dialed number against the table, it checks the patterns in numerical order from 1 ~ 16, so ordering is important.
Pattern	This is the dialed number for which this table entry applies, up to 47 characters. Allowed characters are: - Numerals "0" ~ "9" "x" representing a digit 0 ~ 9, a "*", or a "#". - Asterisk "*" (meaning just an "*") - Period "." (representing zero or more repetitions of the character or range preceding it). For example "5." means no fives (nothing) or any number of fives; but not any other character. "[1~3]." means no ones, twos, or threes (nothing) or any number of ones, twos, or threes; but not any other character. - Tilde "~" (representing a range of digits, for example "[3~9]"). The tilde must be used in brackets, and characters to either side of the tilde must both be digits. - Comma "," (representing a choice of digits. for example "[4,9]"). The comma must be used in brackets, and characters to either side of the comma must both be digits. - Pipe " ", separating number plan patterns. - Brackets "[" and "]" (representing an allowed range, for example "[1,3~5]"). - A maximum of one pair of parentheses "(" and ")" "T" if a user dials some numbers and then presses "#", the rule will be applied and the numbers will be dialed out at once. For example: take the pattern "002(1.)T" and rule "\1". The "002(1.)" pattern represents "002" followed by zero or more ones. The "\1" rule replaces the "002" with the zero or more ones. So, if a user presses 00211111#, the VOP will dial out 11111 immediately. Note: If only pattern is set, the indexed pattern and rule pair will be cleared.
Rule	This is the rule applied to the corresponding Pattern string. Up to 15 characters, allowed characters are 0~9, and: "\c" = the Pattern String is replaced by the countrycode (specified in the relevant call service profile). "\d" = the Pattern String is replaced by the national destination (region) code (specified in the relevant call service profile). "\1" = the Pattern String is replaced by the characters represented inside the parentheses "(" and ")" in the Pattern String. This means the characters represented inside the Pattern String's parentheses are used in dialing the call and the rest of the Pattern String's represented characters are discarded. "deny" = the Pattern String is not allowed. For example: - If the Pattern String is "00244(x.)", the Rule String is "\c\1" and the country code in the relevant call service profile is "28", the dialed number "00244123456" becomes "28123456". - If the Pattern String is "010(x.)", the Rule String is "\d\1" and the national destination code in the relevant call service profile is "01473", the dialed number "010456789" becomes "01473456789". - If the Pattern String is "0440(1x.)" and the Rule String is "\1", the dialed number "04401473987654" becomes "1473987654".
Apply	Click Apply to save your changes in this screen.
New	While you are modifying a number plan table, you can click New to start configuring a fresh table without saving your changes.
Cancel	Click Cancel to start configuring the screen again.
Index	This is an incremental number indicating the order in which the number plan tables were created.
Name	These are the names of individual tables. The DEFVAL table always exists, and is assigned to all ports by default.

Table 117 Profile > VoIP SIP Dialplan (continued)

LABEL	DESCRIPTION
Select	Select the number plan table you wish to modify or delete.
Modify	Select a number plan table and click this in order to edit its configuration.
Delete	Select a number plan table and click this to delete the profile. Once deleted, information cannot be retrieved.

13.13 Xdsl Bonding Profile Screens

Click **Profile > Xdsl Bonding Profile** to configure two-port DSL port bonding. Bonding allows a subscriber to connect to the IES using data streams spread over two DSL lines. The total available bandwidth for the subscriber then becomes the sum of the bandwidth available for the two lines. The additional DSL line also provides backup support.

The two ports in a bonding group must be sequential. Members of a bonding group must also be in the same DSL physical layer. This means that on the VLC ports 12 and 13 cannot be in a group together.

Figure 169 Profile > Xdsl Bonding

Name	Active	Port	Protocol	Line Template	Fallback Template	Group Rate	Port Rate	Select
test	No	3/1	ATM	DEFVAL	DEFVAL	128000/128000	100032/100032	☐
		3/2	ATM	DEFVAL	DEFVAL		100032/100032	☐
test2	No	3/12	ATM	DEFVAL	DEFVAL	128000/128000	100032/100032	☐
		3/13	ATM	DEFVAL	DEFVAL		100032/100032	☐
test3	No	5/1	Auto	DEFVAL	DEFVAL	128000/128000	100032/100032	☐
		5/2	Auto	DEFVAL	DEFVAL		100032/100032	☐

The following table describes the fields in this screen.

Table 118 Profile > Xdsl Bonding

LABEL	DESCRIPTION
Group Name	The group represents a bundle of DSL lines connecting the line card and CPE DSL device. Enter a descriptive name for identification purposes.
Active	Select this to turn on DSL port bonding for this group.
Port	Select a DSL port to add to this group. Selecting a port adds that port and the subsequent port. For example, select port 1 to bond ports 1 and 2.
Protocol	Select whether the group uses ATM , PTM , or Auto mode. ATM supports ADSL2 or ADSL2+. PTM supports VDSL2. Auto has the IES automatically determine which to use.
Line Template	Select the DSL line template the group uses.

Table 118 Profile > Xdsl Bonding (continued)

LABEL	DESCRIPTION
Fallback Template	Select a DSL line template for the group to use for fallback.
Apply	Click Apply to save your changes in this screen.
New	While you are modifying a profile, you can click New to start configuring a fresh profile without saving your changes.
Cancel	Click Cancel to start configuring this screen again.
Name	This field displays the descriptive name of a profile.
Active	This field displays whether or not the DSL port bonding is enabled for this group.
Port	This shows the ports in this DSL port bonding group.
Protocol	This shows the traffic type (PTM or ATM) of this bonding group.
Line Template	This shows the DSL line template the group uses.
Fallback Template	This shows the DSL line template the group uses for fallback.
Group Rate	This shows the bonding group's maximum downstream/upstream transmission rates in kbps. This is the sum of the rates of the 2 ports. The maximum value is 128000 (128000 displays if the sum exceeds 128000). These values are theoretical rates before real training of the DSL ports.
Port Rate	This shows the individual DSL ports' maximum downstream/upstream transmission rates in kbps. These are defined in the mapped DSL template. These values are theoretical rates before real training of the DSL ports.
Modify	Select a profile's Select radio button and click Modify to edit the profile.
Delete	Select a profile's Select radio button and click Delete to remove the profile.

CHAPTER 14

Statistics Screens

This chapter describes the run-time statistics.

14.1 ARP Table

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address, also known as a Media Access Control or MAC address, on the local area network.

An IP (version 4) address is 32 bits long. In an Ethernet LAN, MAC addresses are 48 bits long. The ARP table maintains an association between each MAC address and its corresponding IP address.

14.1.1 How ARP Works

When an incoming packet destined for a host device on a local area network arrives at the switch, the switch's ARP program looks in the ARP table and, if it finds the address, sends it to the device.

If no entry is found for the IP address, ARP broadcasts the request to all the devices on the LAN. The switch fills in its own MAC and IP address in the sender address fields, and puts the known IP address of the target in the target IP address field. In addition, the switch puts all ones in the target MAC field (FF.FF.FF.FF.FF.FF is the Ethernet broadcast address). The replying device (which is either the IP address of the device being sought or the router that knows the way) replaces the broadcast address with the target's MAC address, swaps the sender and target pairs, and unicasts the answer directly back to the requesting machine. ARP updates the ARP table for future reference and then sends the packet to the MAC address that replied.

14.1.2 ARP Table Screen

Click **Statistics > ARP Table** to open the following screen. This screen lists the IP addresses that the system has mapped to MAC addresses.

Figure 170 Statistics > ARP Table

ARP Table			
Total: 2			
Index	IP Address	MAC Address	Interface
1	172.23.31.21	c0:3f:d5:b3:36:ae	Ethernet
2	172.23.31.254	00:04:80:9b:78:00	Ethernet

Page 1 of 1

The following table describes the labels in this screen.

Table 119 Statistics > ARP Table

LABEL	DESCRIPTION
Refresh	Click Refresh to renew the number of entries in the ARP table.
Flush	Click Flush to remove all of the entries from the ARP table.
Total	This displays the number of entries in the ARP table.
Index	This is the ARP table entry number.
IP Address	This is the learned IP address of a device connected to one of the system's ports.
MAC Address	This is the MAC address of the device with the listed IP address.
Interface	This identifies to which interface (inband or outband) the device is connected.
Page X of X	This identifies which page of information is displayed and the total number of pages of information.
Previous/Next	Click one of these buttons to show the preceding/following screen if the information cannot be displayed in one screen.

14.2 DHCP Snoop

To view DHCP packet counters on a port, click **Statistics > DHCP Snoop**.

Figure 171 Statistics > DHCP Snoop

Figure 14-14 Statistics: DHCP Snoop

DHCP Snoop

Slot 2 Port 1

Load

Version	Discover	Offer	Request	Ack	Release
Dhcpv4	0	0	0	0	0

Version	Solicit	Advertise	Request	Reply	Renew	Rebind	Release	Relay-Relay-reply forward
Dhcpv6	0	0	0	0	0	0	0	0

Clear

Index

Mac

IPv4/IPv6

VID

Overflow: 0

The following table describes the labels in this screen.

Table 120 Statistics > DHCP Snoop

LABEL	DESCRIPTION
Slot	Select the number of a line card's slot.
Port	Select the number of a DSL port on the line card.
Load	Click Load to retrieve the port's IGMP filter profile setting and display it in the Profile drop-down list box.
Version	This field displays the DHCP version.
Discover	This field displays the number of DHCPv4 Discover packets on this port.
Offer	This field displays the number of DHCPv4 Offer packets on this port.
Request	This field displays the number of DHCPv4 Request packets on this port.
Ack	This field displays the number of DHCPv4 Acknowledge packets on this port.
Release	This field displays the number of DHCPv4 Release packets on this port.
Version	This field displays the DHCP version.
Solicit	This field displays the number of DHCPv6 Solicit packets on this port.
Advertise	This field displays the number of DHCPv6 Advertise packets on this port.
Request	This field displays the number of DHCPv6 Request packets on this port.
Reply	This field displays the number of DHCPv6 Reply packets on this port.
Renew	This field displays the number of DHCPv6 Renew packets on this port.
Rebind	This field displays the number of DHCPv6 Rebind packets on this port.
Release	This field displays the number of DHCPv6 Release packets on this port.
Relay-forward	This field displays the number of DHCPv6 Relay packets transmitted on this port.
Relay-reply	This field displays the number of DHCPv6 Relay packets replied on this port.
Clear	Click Clear to clear all of the statistics from the table above.
Overflow	This field displays the number of IP addressees not added to the DHCP snooping table when it is full.
Index	This field displays the index number.
MAC	This field displays the MAC address of the client computer.
IPv4/IPv6	This field displays the IPv4/IPv6 address assigned to a client on this port.
VID	This field displays the VLAN ID of the VLAN to which the client computer belongs.

14.3 DDMI

Click **Statistics > DDMI** to view your IES device's current status details you can use for troubleshooting. The SFP transceiver's support for the Digital Diagnostics Monitoring Interface (DDMI) function lets you monitor the transceiver's parameters to perform component monitoring, fault isolation, and failure prediction tasks.

Figure 172 Statistics > DDMI

DDMI	
Port	Enet 1
Refresh	
Vendor Name	N/A
Vendor Part Number	N/A
Vendor Revision Level	N/A
Vendor Serial Number	N/A
Date Code	N/A
Supply Voltage(vcc)	0.0000 (V)
TX Bias Current	0.0000 (mA)
TX output power	0.0000 (mW)
RX input power (OMA)	0.0000 (mW)
Module Temperature	0.0000 (C)

The following table describes the labels in this screen.

Table 121 Statistics > DDMI

LABEL	DESCRIPTION
Port	Select the number of an Ethernet port.
Refresh	Click Refresh to renew the status on this port.
Vendor Name	This is the name of the transceiver vendor.
Vendor Part Number	This is the part number defined by the transceiver vendor.
Vendor Revision Level	This is the revision level for the part number provided by the transceiver vendor.
Vendor Serial Number	This is the serial number provided by the transceiver vendor.
Date Code	This is the date code provided by the transceiver vendor.
Supply Voltage	This field displays the level of voltage currently being supplied to the SFP module.
TX Bias Current	This field displays the current milliamps (mA) being supplied to the SFP module's Laser Diode Transmitter. Track the Tx bias to know how the laser component is aging relative to your network's other SFP modules. This helps you know when to do preventative maintenance instead of having to deal with an unexpected SFP module failure.
TX output power	This field displays the number of micro Watts (mW) of light the SFP module is currently transmitting. This value does not reflect the condition of the cable. Refer to this number to monitor the laser's health. Compare the Tx power at one end of a fiber cable with the Rx power at the other end to measure the attenuation. This lets you check if the cable path's performance is as expected or if there may be some interference. Tracking the attenuation over time also helps you see if the cable is deteriorating.
RX input power (OMA)	This field displays the number of micro Watts (mW) of light currently being received from the fiber optic cable.
Module Temperature	This field displays the current temperature inside the SFP module.

14.4 Dot3ad Status

Click **Statistics > Dot3ad Status** to display the following screen. Use this screen to view IEEE 802.3ad link aggregation settings and statistics.

Figure 173 Statistics > Dot3ad Status

The screenshot shows the 'Dot3ad Status' screen. At the top, there is a blue header with the title 'Dot3ad Status' and a 'Refresh' button. Below this is a table with columns: Index, Agg, Enable, Type, and Port. The first row shows Index 1, Agg 1, Enable -, Type -, and Port enet1 enet2. Below the table is a section for Actor and Partner settings, including Actor Priority, Actor Key, Partner Priority, Partner Key, and Syncs. At the bottom, there is a section for Data rate and Utilization, followed by a list of statistics for enetTxBytes, enetTxPkts, enetTxBroadcastPkts, enetTxMulticastPkts, enetRxBytes, enetRxPkts, enetRxBroadcastPkts, enetRxMulticastPkts, enetRxCRCAlignErrors, enetRxUndersizePkts, enetRxOversizePkts, enetRxFragments, enetCollisions, enetPkts64Bytes, enetPkts65to127Bytes, enetPkts128to255Bytes, enetPkts256to511Bytes, enetPkts512to1023Bytes, enetPkts1024to1518Bytes, and enetPkts1519to1522Bytes, all showing 0.

Index	Agg	Enable	Type	Port
1	1	-	-	enet1 enet2

Actor	-	Partner	-
Actor Priority	-	Partner Priority	-
Actor Key	-	Partner Key	-
Links	-	Syncs	-

Data rate : 0/0 kbps Utilization : 0.00/ 0.00%

enetTxBytes	0
enetTxPkts	0
enetTxBroadcastPkts	0
enetTxMulticastPkts	0
enetRxBytes	0
enetRxPkts	0
enetRxBroadcastPkts	0
enetRxMulticastPkts	0
enetRxCRCAlignErrors	0
enetRxUndersizePkts	0
enetRxOversizePkts	0
enetRxFragments	0
enetCollisions	0
enetPkts64Bytes	0
enetPkts65to127Bytes	0
enetPkts128to255Bytes	0
enetPkts256to511Bytes	0
enetPkts512to1023Bytes	0
enetPkts1024to1518Bytes	0
enetPkts1519to1522Bytes	0

The following table describes the labels in this screen.

Table 122 Statistics > Dot3ad Status

LABEL	DESCRIPTION
Refresh	Click Refresh to renew the status on this port.
Index	This is the number of a link aggregation entry.
Agg	This field displays the aggregation group ID. The value is always 1 because the IES can only have 1 aggregation group.
Enable	This field displays whether link aggregation is activated on ports.
Type	This field displays the Gigabit Ethernet uplink ports' IEEE 802.3ad mode.
Port	This field displays the member ports of a link aggregation group.

Table 122 Statistics > Dot3ad Status (continued)

LABEL	DESCRIPTION
Actor	This field displays the MAC address of the Actor in a link aggregation group. The Actor is one end of two devices, which has higher system priority than the other end (called Partner).
Partner	This field displays the MAC address of the partner in a link aggregation group. The Partner is one end of two devices, which has lower system priority than the Actor.
Actor Priority	This field displays the Actor's priority level. The smaller the priority number, the higher the priority level.
Partner Priority	This field displays the partner's priority level.
Actor Key	This field displays the operational key of the Actor. The key is used to identify a link aggregation group on the Actor. That is, the ports which have the same actor key can be aggregated together.
Partner Key	This field displays the operational key of the Partner. The key is used to identify a link aggregation group on the Partner. That is, the ports which have the same partner key can be aggregated together.
Links	These are the ports you have configured to be in the trunk group.
Syncs	These are the ports that are currently transmitting data as one logical link in this trunk group.
Data rate	This field displays the real time transmission rates of the Gigabit Ethernet uplink ports.
Utilization	This field displays the utilization of the Gigabit Ethernet uplink ports.
enetTxBytes	This field displays the total number of bytes transmitted.
enetTxPkts	This field displays the total number of packets transmitted.
enetTxBroadcast Pkts	This field displays the total number of broadcast packets transmitted.
enetTxMulticast Pkts	This field displays the total number of multicast packets transmitted.
enetRxBytes	This field displays the total number of bytes received.
enetRxPkts	This field displays the total number of packets received.
enetRxBroadcast Pkts	This field displays the total number of broadcast packets received.
enetRxMulticast Pkts	This field displays the total number of multicast packets received.
enetRxCRCAlignment Errors	This field displays the total number of packets received that are between 64 bytes to 1518/1522 bytes in length for untagged/tagged frames and have an FCS error of Alignment Error.
enetRxUndersize Pkts	This field displays the total number of packets received that are less than 64 bytes long and well formed.
enetRxOversize Pkts	This field displays the total number of packets received that are longer than 1518/1522 bytes for untagged/tagged frames and well formed.
enetRxFragments	This field displays the total number of packets received that are less than 64 bytes and have an FCS error or Alignment Error.
enetCollisions	This field displays the total number of collision events.
enetPkts64Bytes	This field displays the total number of packets received and transmitted that are 64 bytes in length.
enetPkts65to127Bytes	This field displays the total number of packets received and transmitted that are 65 to 127 bytes in length.
enetPkts128to255Bytes	This field displays the total number of packets received and transmitted that are 128 to 255 bytes in length.
enetPkts256to511Bytes	This field displays the total number of packets received and transmitted that are 256 to 511 bytes in length.
enetPkts512to1023Bytes	This field displays the total number of packets received and transmitted that are 512 to 1023 bytes in length.

Table 122 Statistics > Dot3ad Status (continued)

LABEL	DESCRIPTION
enetPkts1024 to 518Bytes	This field displays the total number of packets received and transmitted that are 1024 to 1518 bytes in length.
enetPkts1519 to 1522Bytes	This field displays the total number of packets received and transmitted that are 1519 to 1522 bytes in length.

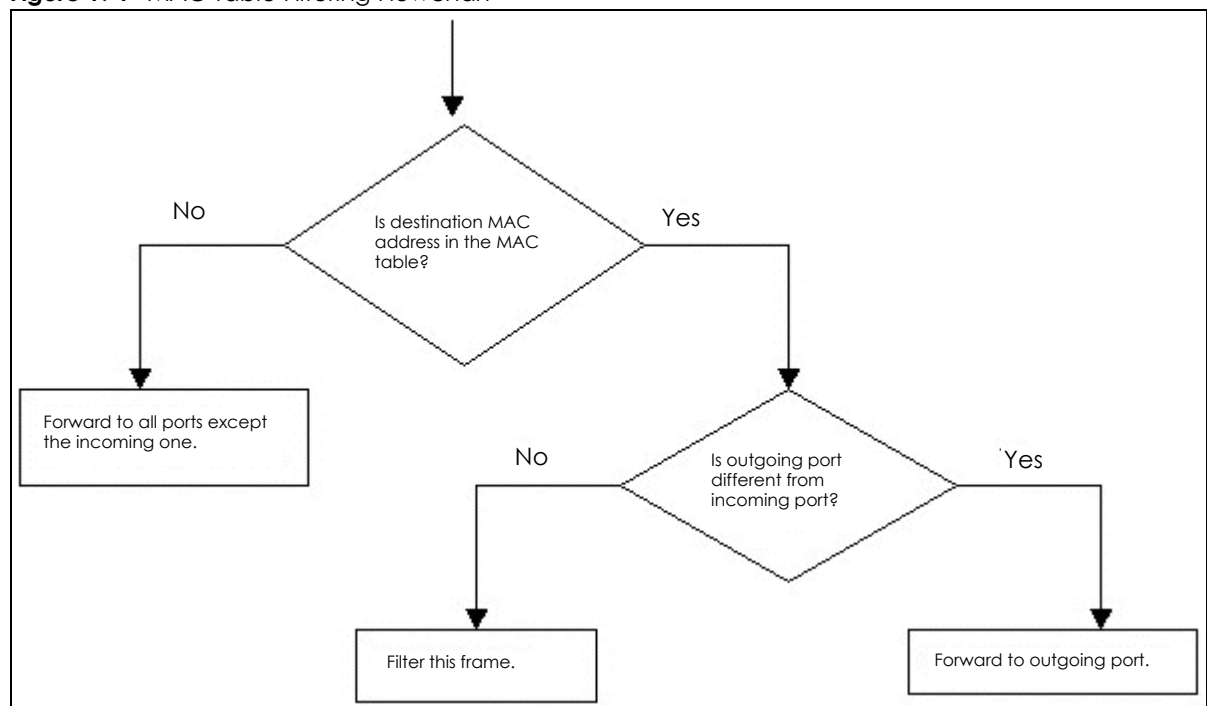
14.5 MAC Table Screen

The MAC table lists device MAC addresses that are dynamically learned by the system. The table shows the following for each MAC address: the port upon which Ethernet frames were received from the device, to which VLAN groups the device belongs (if any) and to which channel it is connected (for devices connected to DSL ports).

The switch uses the MAC table to determine how to forward frames. See the following figure.

- 1 The switch examines a received frame and learns the port on which this source MAC address came.
- 2 The switch checks to see if the frame's destination MAC address matches a source MAC address already learned in the MAC table.
 - If the switch has already learned the port for this MAC address, then it forwards the frame to that port.
 - If the switch has not already learned the port for this MAC address, then the frame is flooded to all ports. Too much port flooding leads to network congestion.
 - If the switch has already learned the port for this MAC address, but the destination port is the same as the port it came in on, then it filters the frame.

Figure 174 MAC Table Filtering Flowchart



Click **Statistics > MAC Table** to display the following screen. This screen lists device MAC addresses that the system dynamically learned.

Figure 175 Statistics > MAC Table

MAC Table					
VLAN ☒ all ☐ Vid ☐ Untag Port ☒ all ☐ enet 1 ☐ Slot 2 Port 1 Refresh Flush					
					Total: 24
Index	uni-vlan(inner/outer)	nni-vlan(inner/outer)	MAC Address	Port	Type
1	untag	1	00:13:49:6a:e0:33	Enet 1	dynamic
2	untag	1	00:0ffe:0d:78:8b	Enet 1	dynamic
3	untag	1	00:21:28:6b:44:be	Enet 1	dynamic
4	untag	1	00:e0:4c:36:03:af	Enet 1	dynamic
5	untag	1	c8:6c:87:22:33:80	Enet 1	dynamic
6	untag	1	e8:37:7a:da:db:c6	Enet 1	dynamic
7	untag	1	ce:5d:0e:a6:60:00	Enet 1	dynamic
8	untag	1	00:1a:80:3f:d3:20	Enet 1	dynamic
9	untag	1	00:26:18:6c:3f:8c	Enet 1	dynamic
10	untag	1	00:1f:29:38:11:44	Enet 1	dynamic
11	untag	1	00:18:fe:6e:51:6c	Enet 1	dynamic
12	untag	1	60:02:92:60:26:83	Enet 1	dynamic
13	untag	1	e8:e0:b7:d2:24:67	Enet 1	dynamic
14	untag	1	00:a0:0c:c9:89:56	Enet 1	dynamic
15	untag	1	00:1e:37:25:be:f6	Enet 1	dynamic
16	untag	1	00:0ffe:09:c9:97	Enet 1	dynamic
17	untag	1	e8:9a:8f:4e:ef:0d	Enet 1	dynamic
18	untag	1	00:16:17:58:ba:ce	Enet 1	dynamic
19	untag	1	00:16:17:58:94:f3	Enet 1	dynamic
20	untag	1	00:0ffe:ed:f4:13	Enet 1	dynamic
21	untag	1	00:1e:0b:24:dd:e7	Enet 1	dynamic
22	untag	1	c8:9c:dc:bd:b1:c5	Enet 1	dynamic
23	untag	1	00:13:49:24:ac:88	Enet 1	dynamic
24	untag	1	00:04:80:9b:78:00	Enet 1	dynamic
Page: 1 of 1					Previous Next

The following table describes the labels in this screen.

Table 123 Statistics > MAC Table

LABEL	DESCRIPTION
VLAN	Select all to display the MAC address table of the port/slot belonging to all VLANs. Select Vid to enter a VLAN ID to display the MAC address table of the port/slot belonging to this VLAN. Select Untag to display the MAC address table of the port/slot that does not belong to any VLAN group.
Port	Select all to display the MAC address table of all the ports. Otherwise select an individual management switch card port or line card for which to show information.
Refresh	Click Refresh to update the list of dynamically learned MAC addresses.
Flush	Click Flush to remove all of the dynamically learned MAC address entries from the MAC table.
Total	This is the total number of connected MAC addresses that the system has learned are connected.

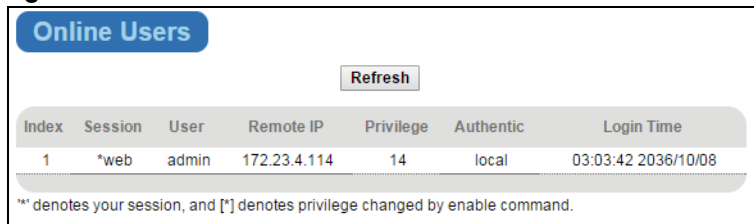
Table 123 Statistics > MAC Table (continued)

LABEL	DESCRIPTION
Index	This is the number of the MAC table entry.
uni-vlan	This displays the VLAN ID on the User Network Interface (UNI) port.
nni-vlan	This displays the VLAN ID on the Network Node Interface (NNI) port.
MAC Address	This is the MAC address of the device that the system has learned is connected to the port.
Port	This is the port to which the MAC address is associated.
Type	This displays whether the MAC address is static or dynamic.
Page X of X	This identifies which page of information is displayed and the total number of pages of information.
Previous/Next	Click one of these buttons to show the previous/next screen if all of the information cannot be seen in one screen.

14.6 Online Users Screen

Click **Statistics > Online Users** to display the following screen. Use this screen to view information about administrators that are logged into the system.

Figure 176 Statistics > Online Users



Online Users						
Refresh						
Index	Session	User	Remote IP	Privilege	Authentic	Login Time
1	*web	admin	172.23.4.114	14	local	03:03:42 2036/10/08
** denotes your session, and [*] denotes privilege changed by enable command.						

The following table describes the labels in this screen.

Table 124 Statistics > Online Users

LABEL	DESCRIPTION
Refresh	Click Refresh to update the list of online users.
Index	This is the number of the online user entry.
Session	This is the type of connection that the administrator is using (web, console, or telnet).
User	This is the user name that the administrator is using.
Remote IP	This is the IP address of the administrator's computer.
Login Time	This displays the time and date that the administrator logged into the system. The time is in (24-hour) hour, minute and second format. The date is in year, month and day format.

14.7 Port Statistics

Click **Statistics > Port** to display the following screen. Use this screen to view port information (such as packet counts, uptime etc.).

Note: You can only view port information on an active card.

Figure 177 Statistics > Port

Statistics			
Index	State	Card Type	Uptime
1	Active	MSC1002GA	165:08:20
2	Active	VOP1164A-61	165:07:07
3	Active	ALC1132A-51	165:07:32
4	Active	ELC1132A-45	165:06:50
5	Active	VLC1124A-51	165:06:32

The following table describes the labels in this screen.

Table 125 Statistics > Port

LABEL	DESCRIPTION
Index	This column lists the slot numbers of the cards. Click the ID number of an active card to go to a screen where you can view port status and statistics.
State	This field displays the line card's current operational status. Active means the line card is operating normally. init means the IES is initializing the line card. disable means a manager has disabled the line card. inactive means the line card is starting up or is not operating normally. This could be due to the card starting, a firmware upgrade in progress or a malfunction.
Card Type	This field displays the type of a card.
Uptime	This field displays how long the card has been running since the last time it was started.

14.7.1 Ethernet Port Statistics

Click the **Index** of the management card in the **Port Statistics** screen to view Ethernet port status and statistics.

Figure 178 Ethernet Port Statistics

Enet Port Status							
Port	Name	Status	Mode	Duplex	Uptime	TX	RX
enet1		link up	100copper	full duplex	25:17:43	0kbps (0.00%)	2kbps (0.00%)
enet2		link down	-	-	-		
Refresh							

The following table describes the labels in this screen.

Table 126 Ethernet Port Statistics

LABEL	DESCRIPTION
Port	This field displays the port name. Click one of these links to see detailed Ethernet port statistics.
Name	This is the descriptive name that identifies the port or the subscriber connected to the port.
Status	This field displays whether the port is connected (link up) or not (link down).
Mode	This field displays the link up speed and media type (copper or fiber).
Duplex	This field displays the duplex mode the port applies.

Table 126 Ethernet Port Statistics (continued)

LABEL	DESCRIPTION
Uptime	This field displays how long the port has been running (or connected) since the last time it was started.
TX / RX	These fields display the numbers of Kbps of Ethernet traffic transmitted and received per second.
Refresh	Click Refresh to update the Ethernet port status.

14.7.1.1 Detailed Ethernet Port Statistics

To view detailed port statistics on a selected Ethernet port, click the port index number in the **ENET Port Status** screen.

Figure 179 Ethernet Port Statistics: Details

Port Statistics: enet1	
Statistics	PM Current PM 15-min PM 1-day
Packet Counter	Counter
enetTxBytes	10752627
enetTxPkts	14508
enetTxBroadcastPkts	3
enetTxMulticastPkts	2277
enetRxBytes	537902247
enetRxPkts	1563961
enetRxBroadcastPkts	356860
enetRxMulticastPkts	1195600
enetRxCRCAlignErrors	0
enetRxUndersizePkts	0
enetRxOversizePkts	0
enetRxFragments	0
enetCollisions	0
enetPkts64Bytes	750918
enetPkts65to127Bytes	213418
enetPkts128to255Bytes	135344
enetPkts256to511Bytes	54821
enetPkts512to1023Bytes	64143
enetPkts1024to1518Bytes	359825
enetPkts1519to1522Bytes	0
Flush Refresh	

The following table describes labels in this example.

Table 127 Ethernet Port Statistics: Details

LABEL	DESCRIPTION
enetTxBytes	This field displays the total number of bytes transmitted.
enetTxPkts	This field displays the total number of packets transmitted.
enetTxBroadcast Pkts	This field displays the total number of broadcast packets transmitted.
enetTxMulticast Pkts	This field displays the total number of multicast packets transmitted.
enetRxBytes	This field displays the total number of bytes received.
enetRxPkts	This field displays the total number of packets received.
enetRxBroadcast Pkts	This field displays the total number of broadcast packets received.

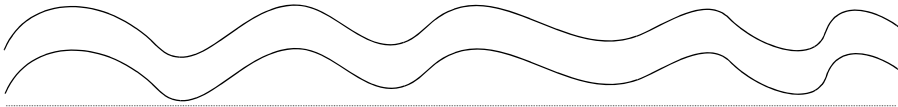
Table 127 Ethernet Port Statistics: Details (continued)

LABEL	DESCRIPTION
enetRxMulticast Pkts	This field displays the total number of multicast packets received.
enetRxCRCAlign Errors	This field displays the total number of packets received that are between 64 bytes to 1518/1522 bytes in length for untagged/tagged frames and have an FCS error of Alignment Error.
enetRxUndersize Pkts	This field displays the total number of packets received that are less than 64 bytes long and well formed.
enetRxOversizePkts	This field displays the total number of packets received that are longer than 1518/1522 bytes for untagged/tagged frames and well formed.
enetRxFragments	This field displays the total number of packets received that are less than 64 bytes and have an FCS error or Alignment Error.
enetCollisions	This field displays the total number of collision events.
enetPkts64Bytes	This field displays the total number of packets received and transmitted that are 64 bytes in length.
enetPkts65to127Bytes	This field displays the total number of packets received and transmitted that are between 65 to 127 bytes in length.
enetPkts128to255Bytes	This field displays the total number of packets received and transmitted that are between 128 to 255 bytes in length.
enetPkts256to511Bytes	This field displays the total number of packets received and transmitted that are between 256 to 511 bytes in length.
enetPkts512to1023Bytes	This field displays the total number of packets received and transmitted that are between 512 to 1023 bytes in length.
enetPkts1024to1518Bytes	This field displays the total number of packets received and transmitted that are between 1024 to 1518 bytes in length.
enetPkts1519to1522Bytes	This field displays the total number of packets received and transmitted that are between 1519 to 1522 bytes in length.
Flush	Click Flush to clear the counters.
Refresh	Click Refresh to update this screen.

14.7.2 VoIP Port Statistics

Click the slot ID for a VOP card in the **Port Statistics** screen to view port status and statistics.

Figure 180 VoIP Port Statistics

VOIP Port Status: Slot 2			
Port	Name	Status	Mode
1		disabled	disabled
2		disabled	disabled
3		disabled	disabled
4		disabled	disabled
5		disabled	disabled
6		disabled	disabled
7		disabled	disabled
8		disabled	disabled
9		disabled	disabled
10		disabled	disabled
11		disabled	disabled
12		disabled	disabled
13		disabled	disabled
14		disabled	disabled
15		disabled	disabled
16		disabled	disabled
17		disabled	disabled
18		disabled	disabled
19		disabled	disabled
20		disabled	disabled
21		disabled	disabled
22		disabled	disabled
23		disabled	disabled
24		disabled	disabled
25		disabled	disabled
26		disabled	disabled
			
58		disabled	disabled
59		disabled	disabled
60		disabled	disabled
61		disabled	disabled
62		disabled	disabled
63		disabled	disabled
64		disabled	disabled
Refresh			

The following table describes labels in this example.

Table 128 VoIP Port Statistics

LABEL	DESCRIPTION
Index	This field displays the port number. Click one of these links to see detailed VoIP port statistics.
Name	This is the descriptive name that identifies the port or the subscriber connected to the port.
Status	This field displays the current status of the analog phone port.
Mode	This field displays the protocol/service status of the VoIP port.
Refresh	Click Refresh to update this screen.

14.7.2.1 Detailed VoIP Port Statistics: Statistics

Click the slot ID for a VOP card in the **Port Statistics** screen and click the **Statistics** tab to view port status and statistics.

Figure 181 Detailed VoIP Port Statistics: Statistics

Packet Counter	TX	RX
rate (bps)	0	0
packet count	0	0
frac lost (%)	0.000000	0.000000
jitter (ms)	0	0
average delay (ms)	0	0

Flush Refresh

The following table describes labels in this example.

Table 129 Detailed VoIP Port Statistics: Statistics

LABEL	DESCRIPTION
Packet Counter	This displays the numbers of transmitted (TX) and received (RX) packets on this port.
rate	This displays the data transmission/receiving rate in bits per second.
packet count	This displays the numbers of packets transmitted and received on this port.
frac lost	This field displays the percentage of packets lost.
jitter	This displays the average delay interval between two packets transmitted/received.
average delay	This displays the average latency delay for transmitted/received traffic.
Flush	Click Flush to clear the counters.
Refresh	Click Refresh to update this screen.

14.7.2.2 Detailed VoIP Port Statistics: PM Current / PM 15-min / PM 1-day

To display the packet counters since the system was started up or for the last 15 minutes/the past one day, click the port number in the VoIP port statistics screen and click the **PM Current/PM 15-min/PM 1-day** tab.

Figure 182 Detailed VoIP Port Statistics: PM Current

Packet Counter	TX	RX
ElapsedTime	0	
Bytes	0	0
Packets	0	0
LostPackets	0	0

Flush Refresh

The following table describes labels in this example.

Table 130 Detailed VoIP Port Statistics: PM Current

LABEL	DESCRIPTION
Packet Counter	This displays the numbers of transmitted (TX) and received (RX) packets on this port.
ElapsedTime	This field displays the effective elapsed time (the time VoIP call has established).
Bytes	This field displays the number of bytes transmitted/received on this port.
Packets	This field displays the number of packets transmitted/received on this port.

Table 130 Detailed VoIP Port Statistics: PM Current (continued)

LABEL	DESCRIPTION
LostPackets	This field displays the number of TX/RX packets lost on this port.
Flush	Click Flush to clear the counters.
Refresh	Click Refresh to update this screen.

14.7.3 DSL Line Card Statistics

Click the ID for a DSL line card in the **Port Statistics** screen to view port status and statistics on the line card. Statistics screens for the line cards are similar. Example screens for the VLC are shown.

Figure 183 DSL Line Card Statistics

DSL Port Status: Slot 3						
Port	Name	Status	Mode	Up/Downstream	Uptime	Error Second(15M/24H)
1		inactive	-	-/-	-	-
2		inactive	-	-/-	-	-
3		inactive	-	-/-	-	-
4		inactive	-	-/-	-	-
5		inactive	-	-/-	-	-
6		inactive	-	-/-	-	-
7		inactive	-	-/-	-	-
8		inactive	-	-/-	-	-
9		inactive	-	-/-	-	-
10		inactive	-	-/-	-	-
11		inactive	-	-/-	-	-
12		inactive	-	-/-	-	-
13		inactive	-	-/-	-	-
14		inactive	-	-/-	-	-
15		inactive	-	-/-	-	-
16		inactive	-	-/-	-	-
17		inactive	-	-/-	-	-
18		inactive	-	-/-	-	-
19		inactive	-	-/-	-	-
20		inactive	-	-/-	-	-
21		inactive	-	-/-	-	-
22		inactive	-	-/-	-	-
23		inactive	-	-/-	-	-
24		inactive	-	-/-	-	-
25		inactive	-	-/-	-	-
26		inactive	-	-/-	-	-
27		inactive	-	-/-	-	-
28		inactive	-	-/-	-	-
29		inactive	-	-/-	-	-
30		inactive	-	-/-	-	-
31		inactive	-	-/-	-	-
32		inactive	-	-/-	-	-

The following table describes the labels in this screen.

Table 131 DSL Line Card Statistics

LABEL	DESCRIPTION
Port	This field displays the port number.
Name	This is the descriptive name that identifies the port or the subscriber connected to the port.
Status	This field displays the current status of the analog phone port.
Mode	This field displays the DSL link up mode.

Table 131 DSL Line Card Statistics (continued)

LABEL	DESCRIPTION
Up/ Downstream	This field displays the upstream and downstream link up rate.
Uptime	This field displays how long the connection is up.
Error Second	This field displays the error seconds within the current 15 minutes/the last 24 hours.
Refresh	Click Refresh to update this screen.

14.7.3.1 DSL Line Card Statistics: Statistics/Status Current/Status 15-min/Status 1-day

Click the slot ID for a DSL line card in the **Port Statistics** screen and click the **Statistics/Status Current/Status 15-min/Status 1-day** tab to view port status and statistics.

Figure 184 DSL Line Card Statistics: Statistics/Status Current/Status 15-min/Status 1-day

Port Statistics: DSL 3/2		
Statistics	Stats Current	Stats 15-min
Stats 1-day	PM Current	PM 15-min
PM 1-day		
Packet Counter	TX	RX
Bytes	0	0
Pkts	0	0
UnicastPkts	0	0
BroadcastPkts	0	0
MulticastPkts	0	0
DiscardPkts	0	0
Flush Refresh		

The following table describes the labels in this screen.

Table 132 DSL Line Card Statistics: Statistics/Status Current/Status 15-min/Status 1-day

LABEL	DESCRIPTION
Packet Counter	This displays the numbers of transmitted (TX) and received (RX) packets on this port.
Bytes	This field displays the number of bytes transmitted/received on this port.
Pkts	This field displays the number of packets transmitted/received on this port.
UnicastPkts	This field displays the number of unicast packets transmitted/received on this port.
BroadcastPkts	This field displays the number of broadcast packets transmitted/received on this port.
MulticastPkts	This field displays the number of multicast packets transmitted/received on this port.
DiscardPkts	This field displays the number of received/transmitted packets there were discarded on this port.
Flush	Click Flush to clear the counters.
Refresh	Click Refresh to update this screen.

14.7.3.2 DSL Line Card Statistics: PM Current/PM 15-min/PM 1-day

To display the packet counters since the system was started up or for the last 15 minutes/the past one day, click the port number in the DSL line card statistics screen and click the **PM Current/PM 15-min/PM 1-day** tab.

Figure 185 DSL Line Card Statistics: PM Current/PM 15-min/PM 1-day

Port Statistics: DSL 3/2		
Statistics	Stats Current	Stats 15-min
Stats 1-day	PM Current	PM 15-min
PM 1-day		
	Current	
line/channel performance	XTUC	XTUR
TimeElapsed (seconds)	456	456
MonitoredTime (seconds)	457	457
Fecs (seconds)	0	0
Lofs (seconds)	0	0
Loss (seconds)	0	0
Lols (seconds)	0	-
Lol	0	-
Lprs (seconds)	-	0
Lpr	-	0
Es	0	0
Ses	0	0
Uas	0	0
FullInit	0	-
FailFullInit	0	-
TimeElapsed (seconds)	456	456
CorrectedBlks	0	0
UncorrectBlks	0	0
CodeViolations	0	0
Flush Refresh		

The following table describes the labels in this screen.

Table 133 DSL Line Card Statistics: PM Current/PM 15-min/PM 1-day

LABEL	DESCRIPTION
Current	Select the time period for which to display packet counters.
line/channel performance	This displays the downstream (XTUC) and upstream (XTUR) performance counters on this port.
TimeElapsed	This field displays the time since the last 15-minute/the last 1-day data collection for the downstream (XTUC) and upstream (XTUR) directions. Note: This label only displays in PM 15-min and PM 1-day screens.
MonitoredTime	These are the DSL line's downstream and upstream lengths of time the system has collected the line performance data in this current 15-minute/1-day time period. Note: This label only displays in PM 15-min and PM 1-day screens.
Fecs (seconds)	These are the DSL line's downstream and upstream numbers of Forward Error Correction Seconds (FECS) that have occurred since the system last started up or for the past 15-minute/1-day period.
Lofs (seconds)	These are the DSL line's downstream and upstream numbers of Loss of Frame Seconds (LOFS) that have occurred since the system last started up or for the past 15-minute/1-day period.
Loss (seconds)	These are the DSL line's downstream and upstream numbers of Loss of Signal Seconds (LOSS) that have occurred since the system last started up or for the past 15-minute/1-day period.
Lols (seconds)	This is the DSL line's downstream numbers of Loss of Link Seconds (LOLS) that have occurred since the system last started up or for the past 15-minute/1-day period.
Lol	This is the number of times the DSL line's downstream connection has experienced a Loss of Link (LOL) during the past 15-minute/1-day period. Note: This label only displays in PM 15-min and PM 1-day screens.

Table 133 DSL Line Card Statistics: PM Current/PM 15-min/PM 1-day (continued)

LABEL	DESCRIPTION
Lprs (seconds)	This is the DSL line's upstream number of Loss of Power Seconds (LPRS) that have occurred since the system last started up or for the past 15-minute/1-day period.
Lpr	This is the number of times the DSL line's upstream connection has experienced a Loss of Power (LPR) since the system last started up or during the past 15-minute/1-day period. Note: This label only displays in PM 15-min and PM 1-day screens.
Es	These are the DSL line's downstream and upstream numbers of Errored Seconds that have occurred since the system last started up or for the past 15-minute/1-day period.
Ses	These are the DSL line's downstream and upstream numbers of Severely Errored Seconds that have occurred since the system last started up or for the past 15-minute/1-day period. This is how many seconds contained 30% or more errored blocks or at least one defect. This is a subset of ES.
Uas	These are the DSL line's downstream and upstream numbers of UnAvailable Seconds that have occurred since the system last started up or for the past 15-minute/1-day period.
FullInit	These are the DSL line's downstream and upstream numbers of successful initialization traps that have occurred since the system last started up or for the past 15-minute/1-day period.
FailFullInit	These are the DSL line's downstream and upstream numbers of initialization failure traps that have occurred since the system last started up or within the current 15-minute/1-day period.
TimeElapsed	This field displays the time since the last 15-minute/the last 1-day data collection for the downstream (XTUC) and upstream (XTUR) directions. Note: This label only displays in PM 15-min and PM 1-day screens.
CorrectedBlks	These are the numbers of corrected blocks for downstream and upstream transmission.
UncorrectedBlks	These are the numbers of uncorrected blocks for downstream and upstream transmission.
CodeViolations	These are the numbers of incorrect cyclic redundancy checks that have occurred since the system last started up or within the current 15-minute/1-day period.
Flush	Click Flush to clear the counters.
Refresh	Click Refresh to update this screen.

14.7.4 FE Port Statistics

Click the ID for a FE line card in the **Port Statistics** screen to view Fast Ethernet port status and statistics.

Figure 186 FE Port Statistics

FE Port Status: Slot 4					
Port	Name	Status	Mode	Duplex	Uptime
1		inactive	-	-	-
2		inactive	-	-	-
3		inactive	-	-	-
4		inactive	-	-	-
5		inactive	-	-	-
6		inactive	-	-	-
7		inactive	-	-	-
8		inactive	-	-	-
9		inactive	-	-	-
10		inactive	-	-	-
11		inactive	-	-	-
12		inactive	-	-	-
13		inactive	-	-	-
14		inactive	-	-	-
15		inactive	-	-	-
16		inactive	-	-	-
17		inactive	-	-	-
18		inactive	-	-	-
19		inactive	-	-	-
20		inactive	-	-	-
21		inactive	-	-	-
22		inactive	-	-	-
23		inactive	-	-	-
24		inactive	-	-	-
25		inactive	-	-	-
26		inactive	-	-	-
27		inactive	-	-	-
28		inactive	-	-	-
29		inactive	-	-	-
30		inactive	-	-	-
31		inactive	-	-	-
32		inactive	-	-	-
Refresh					

The following table describes the labels in this screen.

Table 134 FE Port Statistics

LABEL	DESCRIPTION
Port	This field displays the port name. Click these links to see detailed Ethernet port statistics.
Name	This is the descriptive name that identifies the port or the subscriber connected to the port.
Status	This field displays whether the port is connected (link up) or not (link down).
Mode	This field displays the link up speed and media type (copper or fiber).
Duplex	This field displays the duplex mode the port applies.
Uptime	This field displays how long the port has been running (or connected) since the last time it was started.
Refresh	Click Refresh to update the Ethernet port status.

14.7.4.1 Detailed FE Port Statistics

Click an FE port's index number in the **FE Port Status** screen to view detailed port statistics.

Figure 187 FE Port Statistics: Details

Port Statistics: 4/1	
Statistics	PM Current PM 15-min PM 1-day
Packet Counter	Counter
enetTxBytes	0
enetTxPkts	0
enetTxBroadcastPkts	0
enetTxMulticastPkts	0
enetRxBytes	0
enetRxPkts	0
enetRxBroadcastPkts	0
enetRxMulticastPkts	0
enetRxCRCAlignErrors	0
enetRxUndersizePkts	0
enetRxOversizePkts	0
enetRxFragments	0
enetCollisions	0
enetRxPkts64Bytes	0
enetRxPkts65to127Bytes	0
enetRxPkts128to255Bytes	0
enetRxPkts256to511Bytes	0
enetRxPkts512to1023Bytes	0
enetRxPkts1024to1518Bytes	0
Flush Refresh	

The following table describes labels in this example.

Table 135 FE Port Statistics: Details

LABEL	DESCRIPTION
enetTxBytes	This field displays the total number of bytes transmitted.
enetTxPkts	This field displays the total number of packets transmitted.
enetTxBroadcast Pkts	This field displays the total number of broadcast packets transmitted.
enetTxMulticastPkts	This field displays the total number of multicast packets transmitted.
enetRxBytes	This field displays the total number of bytes received.
enetRxPkts	This field displays the total number of packets received.
enetRxBroadcast Pkts	This field displays the total number of broadcast packets received.
enetRxMulticast Pkts	This field displays the total number of multicast packets received.
enetRxCRCAlign Errors	This field displays the total number of packets received that are between 64 bytes to 1518/1522 bytes in length for untagged/tagged frames and have an FCS error of Alignment Error.
enetRxUndersize Pkts	This field displays the total number of packets received that are less than 64 bytes long and well formed.
enetRxOversizePkts	This field displays the total number of packets received that are longer than 1518/1522 bytes for untagged/tagged frames and well formed.
enetRxFragments	This field displays the total number of packets received that are less than 64 bytes and have an FCS error or Alignment Error.
enetCollisions	This field displays the total number of collision events.
enetRxPkts64Bytes	This field displays the total number of packets received that are 64 bytes in length.

Table 135 FE Port Statistics: Details (continued)

LABEL	DESCRIPTION
enetRxPkts65to127Bytes	This field displays the total number of packets received that are 65 to 127 bytes in length.
enetRxPkts128to255Bytes	This field displays the total number of packets received that are 128 to 255 bytes in length.
enetRxPkts256to511Bytes	This field displays the total number of packets received that are 256 to 511 bytes in length.
enetRxPkts512to1023Bytes	This field displays the total number of packets received that are 512 to 1023 bytes in length.
enetRxPkts1024to1518Bytes	This field displays the total number of packets received that are 1024 to 1518 bytes in length.
Flush	Click Flush to clear the counters.
Refresh	Click Refresh to update this screen.

14.8 RSTP Statistics

Use the Rapid Spanning Tree Protocol (RSTP) statistics screen to display the status and statistics for the device's RSTP settings. Click **Statistics > RSTP** to display the following screen.

Figure 188 Statistics > RSTP

RSTP Statistics									
Bridge ID	0x8000001349000001								
Designated Root ID	0x8000001349000001								
Time Since Change	865970								
Topology Change Times	0								
Root Port ID	0x00								
Root Cost	0								
Root Hello Time	2 second(s)								
Root Max Age	20 second(s)								
Root Forward Delay	15 second(s)								
Priority	32768								
Hello Time	2 second(s)								
Max Age	20 second(s)								
Forward Delay	15 second(s)								
Port	Port ID	Priority	Path Cost	State	Designated Cost	Designated Root ID	Designated Bridge ID	Designated Port ID	
enet1	-	-	-	-	-	-	-	-	
enet2	-	-	-	-	-	-	-	-	

The following table describes the labels in this screen.

Table 136 Statistics > RSTP

LABEL	DESCRIPTION
Bridge ID	This is the unique identifier for this bridge, consisting of bridge priority plus MAC address.
Designated Root ID	This is the unique identifier for the root bridge, consisting of bridge priority plus MAC address.
Time Since Change	This is the time since the spanning tree has been reconfigured.
Topology Change Times	This is the number of times the spanning tree has been reconfigured.
Root Port ID	This is the unique identifier for the port that connects to the external root bridge.
Root Cost	This is the path cost of the link to the root bridge.
Root Hello Time	This is the time interval (in seconds) at which the root transmits a configuration message through the root port. The root bridge determines the Hello Time, Max Age and Forward Delay.
Root Max Age	This is the maximum time (in seconds) the spanning tree can wait without receiving a configuration message before attempting to reconfigure on the root port.
Root Forward Delay	This is the time (in seconds) the root bridge will wait before changing states (that is, listening to learning or learning to forwarding) on the root port. Each change in states requires the forward delay time before the change.
Priority	This field displays the RSTP bridge priority of the IES.
Hello Time	This is the time interval (in seconds) at which the root switch transmits a configuration message. The root bridge determines the Hello Time, Max Age and Forward Delay.
Max Age	This is the maximum time (in seconds) the root bridge can wait without receiving a configuration message before attempting to reconfigure.
Forward Delay	This is the time (in seconds) the root switch will wait before changing states (that is, listening to learning to forwarding).
Port	These are the IES's uplink Ethernet ports.
Port ID	This field displays the port ID.
Priority	This field displays the configured port priority.
Path Cost	This field displays the path cost of this port to an external bridge.
State	This field displays the STP status on this port.
Designated Cost	This field displays the path cost to the designated root bridge.
Designated Root ID	This is the unique identifier for the designated root bridge.
Designated Bridge ID	This is the unique identifier for the bridge in the LAN segment to which this bridge belongs that has the lowest path cost to reach the root bridge, consisting of bridge priority plus MAC address.
Designated Port ID	This is the port on the designated bridge that has the lowest path cost to reach the root bridge, consisting of bridge priority.

14.9 Bonding Status

Click **Statistics > Bonding Status** to display the status and counters for the DSL bonding groups.

Figure 189 Statistics > Bonding Status: ATM

Bonding Group Status

Group Name : test5 ▼ Load

Group Status

Active	Yes
Member Port	5/15,5/16
Active Port	
Main Port	5/15
Transfer Mode	ATM
Group Rate DS	0
Group Rate US	0

Time : 15-mins ▼ History-1 ▼

2037/02/05 10:30:00 ~ 2037/02/05 10:45:00

Group Counters

gbondTxCells	0
gbondRxCells	0
gbondNumFlushRequests	0
gbondNumTimeouts	0
gbondNumDirectSidResets	0
gbondNumDiscards	0

Flush

Figure 190 Statistics > Bonding Status: PTM

Bonding Group Status

Group Name : test5 ▼ Load

Group Status

Active	Yes
Member Port	5/15,5/16
Active Port	5/15,5/16
Main Port	5/15
Transfer Mode	PTM
Group Rate DS	100028
Group Rate US	40030

Time : 15-mins ▼ History-4 ▼

2037/02/06 01:45:00 ~ 2037/02/06 02:00:00

Group Counters

gbondRxPackets	46
gbondNumFlushRequests	0
gbondNumTimeouts	0
gbondNumDirectSidResets	0
gbondRxSmallFragments	0
gbondRxLargeFragments	0
gbondRxBadFragments	0
gbondRxLostFragments	0
gbondRxLostStarts	0
gbondRxLostEnds	0
gbondTxPackets	0

Flush

The following table describes the labels in this screen.

Table 137 Statistics > Bonding Status

LABEL	DESCRIPTION
Group Name	Select a bonding group and click Load to display its status.
Active	This field displays whether or not DSL port bonding is enabled for this group.
Member Port	This shows the ports in this DSL port bonding group.
Active Port	This field displays which DSL ports are active in this group.
Main Port	The lower-numbered port in the port bonding group is automatically selected as the main port. All data plane features such as VLAN setting, QoS, and ACL apply to the main port.
Transfer Mode	This shows the traffic type (PTM or ATM) of this bonding group.
Group Rate DS	This shows the bonding group's downstream traffic rate in kbps.
Group Rate US	This shows the bonding group's upstream traffic rate in kbps.
Time	Display the accumulated counters (Current) or by 15-minute periods, or by day. For 15-minute periods or by day, use the field to the right to select the time period to display.
Group Counters (ATM)	
gbondTxCells	This field displays the number of correctly transmitted ATM user data cells.
gbondRxCells	This field displays the number of correctly received ATM user data cells.
gbondNumFlushRequests	This field displays a bonding error counter indicating the number of flush requests due to buffer overflow.
gbondNumTimeouts	This field displays a bonding error counter indicating the number of cell timeouts.
gbondNumDirectSidResets	This field displays a bonding error counter indicating the number of Sequence Identifier (SID) resyncs.
gbondNumDiscards	This field displays a bonding error counter indicating the number of cells discarded due to unexpected SID.
Group Counters (PTM)	
gbondRxPackets	This field displays the number of correctly reassembled packets transmitted upstream.
gbondNumFlushRequests	This field displays the bonding error counter.
gbondNumTimeouts	This field displays the number of reassembly queue flushes caused by a fragment spending too much time in the queue.
gbondNumDirectSidResets	This field displays the number of times to give up waiting for the next expected SID.
gbondRxSmallFragments	This field displays the number of fragments discarded because they are too small.
gbondRxLargeFragments	This field displays the number of fragments discarded because they are too long. This parameter can be used to detect whether the remote end complies with the bonding standard.
gbondRxBadFragments	This field displays the number of fragments that do not fit into the sequence expected by the frame assembly function.
gbondRxLostFragments	This field displays the number of gaps in the sequence of fragments. The frame is flushed until the start of the next packet is received.
gbondRxLostStarts	This field displays the number of missing Start of Packets (SOPs).
gbondRxLostEnds	This field displays the number of missing End of Packets (EOPs).
gbondTxPackets	This field displays the number of correctly transmitted PTM user data packets.
Flush	Click Flush to clear the counters.

CHAPTER 15

Switch Screens

This chapter describes the screens you use to configure Ethernet ports, multicast VLAN, and global switch parameters such as link aggregation, priority queues, and queuing method.

15.1 Mirror Screen

Port mirroring allows you to copy an uplink port's traffic flow to a monitor port so you can examine the traffic without interfering with the original port's traffic flow.

Click **Switch > Mirror** to display the **Mirror** screen. Use this screen to select a monitor port and specify the traffic flow to be copied to the monitor port.

Figure 191 Switch > Mirror

The following table describes the labels in this screen.

Table 138 Switch > Mirror

LABEL	DESCRIPTION
Source	Select the source interface (Enet , DSL , or FE), and then choose the number of slot and port from which traffic flow is copied. Then specify the Virtual Path Indicator (VPI) and Virtual Channel Indicator (VCI) of an individual Permanent Virtual Circuit (PVC). The VPI setting can be 0 to 255. The VCI setting can be 255 to 65535.
Destination	The destination is the port you copy the traffic to in order to examine it in more detail without interfering with the traffic flow on the original ports. Select an uplink Gigabit Ethernet port.
Mirror Mode	Specify the direction of the traffic to mirror by selecting from the drop-down list box. Choices are Egress (outgoing), Ingress (incoming), or both incoming and outgoing (Both) traffic.
Apply	Click Apply to save the changes in this section.
Index	This is the number of a port mirroring entry.

Table 138 Switch > Mirror (continued)

LABEL	DESCRIPTION
Source Interface	This field displays the type of the source interface.
Slot	This field displays the number of the slot of the source interface.
Port	This field displays the number of the port of the source interface.
VPI/VCI	This field displays the VPI/VCI settings.
Enet Port	This field displays the destination Ethernet port.
Mode	This field displays the mirror mode.
Select	Click Select of an entry and then click Delete to remove the specified entry.
Delete	

15.2 RSTP

The IES supports Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP) as defined in the following standards.

- IEEE 802.1d Spanning Tree Protocol
- IEEE 802.1w Rapid Spanning Tree Protocol

RSTP adds rapid reconfiguration capability to STP. The IES supports RSTP and earlier STP. RSTP and STP detect and break network loops and provide backup links between switches, bridges or routers. They allow a device to interact with other RSTP or STP-aware devices in your network to ensure that only one path exists between any two stations on the network. The switch uses RSTP by default but can still inter-operate with STP switches (although without RSTP's benefits).

The root bridge is the base of the spanning tree; it is the bridge with the lowest identifier value (MAC address). Path cost is the cost of transmitting a frame onto a LAN through that port. It is assigned according to the speed of the link to which a port is attached. The slower the media, the higher the cost - see the following table.

Table 139 STP/RSTP Path Costs

LINK SPEED	RECOMMENDED VALUE	RECOMMENDED RANGE	ALLOWED RANGE
4Mbps	250	100 to 1000	1 to 65535
10Mbps	100	50 to 600	1 to 65535
16Mbps	62	40 to 400	1 to 65535
100Mbps	19	10 to 60	1 to 65535
1Gbps	4	3 to 10	1 to 65535
10Gbps	2	1 to 5	1 to 65535

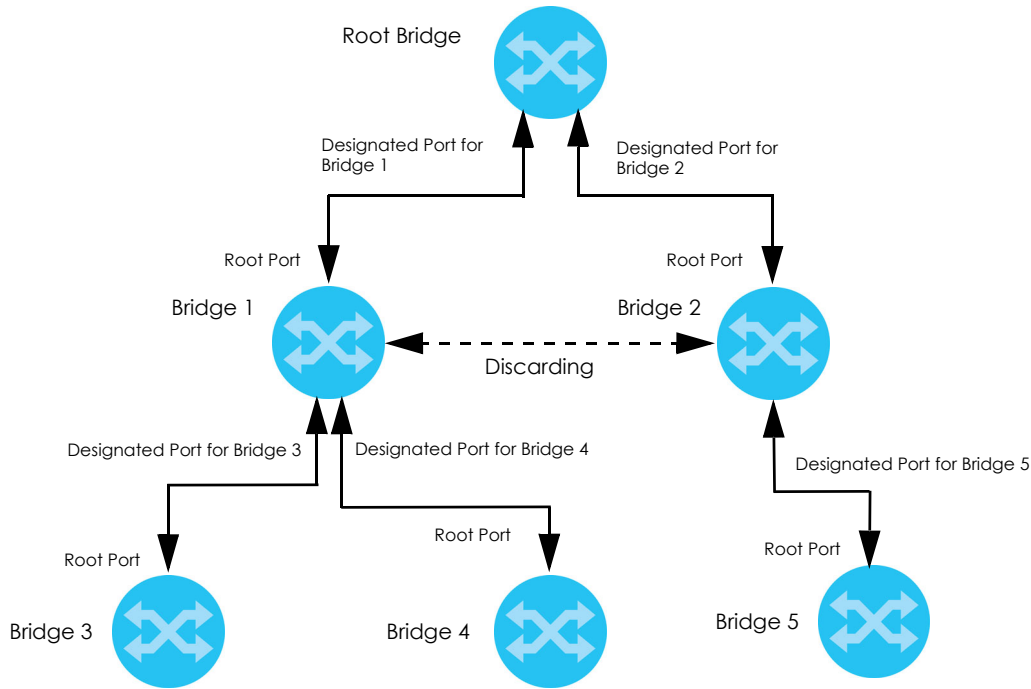
On each bridge, the root port is the port through which this bridge communicates with the root. It is the port on this switch with the lowest path cost to the root (the root path cost). If there is no root port, then this switch has been accepted as the root bridge of the spanning tree network.

For each LAN segment, a designated bridge is selected. This bridge has the lowest cost to the root among the bridges connected to the LAN.

After a bridge determines the lowest cost-spanning tree with RSTP, it enables the root port and the ports that are the designated ports for the connected LANs, and disables all other ports that participate in

RSTP. Network packets are therefore only forwarded between enabled ports, eliminating any possible network loops.

Figure 192 STP Root Ports and Designated Ports



RSTP-aware devices exchange Bridge Protocol Data Units (BPDUs) periodically. When the bridge LAN topology changes, a new spanning tree is constructed.

In RSTP, the devices send BPDUs every Hello Time. If an RSTP-aware device does not get a Hello BPDU after three Hello Times pass (or the Max Age), the device assumes that the link to the neighboring bridge is down. This device then initiates negotiations with other devices to reconfigure the network to re-establish a valid network topology.

In STP, once a stable network topology has been established, all devices listen for Hello BPDUs transmitted from the root bridge. If an STP-aware device does not get a Hello BPDU after a predefined interval (Max Age), the device assumes that the link to the root bridge is down. This device then initiates negotiations with other devices to reconfigure the network to re-establish a valid network topology.

RSTP assigns three port states to eliminate packet looping while STP assigns five (see the following table). A device port is not allowed to go directly from blocking state to forwarding state so as to eliminate transient loops.

Table 140 RSTP and STP Port States

RSTP PORT STATE	STP PORT STATE	DESCRIPTION
Discarding	Disabled	STP is disabled (default).
Discarding	Blocking	Only configuration and management BPDUs are received and processed.
Discarding	Listening	All BPDUs are received and processed.

Table 140 RSTP and STP Port States

RSTP PORT STATE	STP PORT STATE	DESCRIPTION
Learning	Learning	All BPDUs are received and processed. Information frames are submitted to the learning process but not forwarded.
Forwarding	Forwarding	All BPDUs are received and processed. All information frames are received and forwarded.

15.2.1 RSTP Setup

Use the MSTP screens to enable RSTP on the switch and configure RSTP bridge and port settings.

15.2.1.1 RSTP Bridge Settings

Click **Switch > RSTP > RSTP Bridge** to display the screen shown next. Use this screen to configure RSTP settings.

Figure 193 Switch > RSTP > RSTP Bridge

The following table describes the labels in this screen.

Table 141 Switch > RSTP > RSTP Bridge

LABEL	DESCRIPTION
Priority	Priority is used in determining the root switch. The switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch. Enter a number between 0 and 61140. The system will automatically round the number to the nearest multiple of 4096. The lower the numeric value you assign, the higher the priority for this switch. Bridge Priority determines the root bridge, which in turn determines Hello Time, Max Age and Forwarding Delay.
Hello Time	This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 to 10 seconds.
Maximum Age	This is the maximum time (in seconds) a switch can wait without receiving a BPDU before attempting to reconfigure. All switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that ages out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the switch ports attached to the network. The allowed range is 6 to 40 seconds.
Forwarding delay	This is the maximum time (in seconds) a switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds. As a general rule: $2 * (\text{Forward Delay} - 1) \geq \text{Max Age} \geq 2 * (\text{Hello Time} + 1)$

Table 141 Switch > RSTP > RSTP Bridge (continued)

LABEL	DESCRIPTION
Apply	Click Apply to save the changes in this screen.
Cancel	Click Cancel to start configuring this screen again.

15.2.1.2 RSTP Port Settings

Click **Switch > RSTP > RSTP Port** to display the configuration screen as shown. Use this screen to set the path cost and priority settings on the switch ports.

Figure 194 Switch > RSTP > RSTP Port

Port	Active	Path Cost[1 ~ 65535]	Priority[0 ~ 240] in step of 16
enet1	☒	4	128
enet2	☒	4	128

The following table describes the labels in this screen.

Table 142 Switch > RSTP > RSTP Port

LABEL	DESCRIPTION
Port	This column lists the IES's Gigabit Ethernet interfaces.
Active	Select this option to enable RSTP on the specified port.
Path Cost	When a loop occurs, RSTP selects the port with the lowest path cost to the root bridge. Specify the path cost (between 1 and 65535) for the port. Enter a smaller number to have the switch select this port first. Enter 0 to have the system automatically determines the path cost based on the link speed. If two ports have the same path cost, the switch will select the one with the highest priority.
Priority	When a loop occurs and two ports have the same path cost, the port with a higher priority (lower numerical value) becomes the root port and the other port becomes an alternate port. Specify the port priority in the spanning tree. Enter a number (between 0 and 240). Enter a smaller number to have the switch select this port first. If two ports have the same priority, the switch will select the one with the smallest port ID (which consists of the port priority and port number).
Apply	Click Apply to save the changes in this screen.
Cancel	Click Cancel to start configuring this screen again.

15.3 Switch Port Setup Screen

Click **Switch > Switch Port Setup** to display the screen shown next. Use this screen to configure basic settings for the Gigabit Ethernet interfaces.

Figure 195 Switch > Switch Port Setup

Port	Active	Name	Speed-duplex
enet1	☒		auto
enet2	☒		auto

Apply Cancel

The following table describes the labels in this screen.

Table 143 Switch > Switch Port Setup

LABEL	DESCRIPTION
Port	This is the label of a Gigabit Ethernet interface.
Active	Select this check box to turn on an interface. The factory default for all ports is enabled. A port must be enabled for data transmission to occur.
Name	Enter a descriptive name that identifies this port. You can use up to 31 English keyboard characters; spaces are not allowed.
Speed/Duplex	Select the type of Ethernet connection for this port. When you don't use auto-negotiation, you must make sure that the settings of the peer Ethernet port are the same in order to connect. Select auto (auto-negotiation) to have the system automatically determine the type of connection that the Ethernet port has. When the peer Ethernet device has auto-negotiation turned on, the system negotiates with the peer to determine the connection speed. If the peer Ethernet port does not have auto-negotiation turned on, the system determines the connection speed by detecting the signal on the cable and using full duplex. Select 1000-full if the Ethernet port has a 1000 MB full-duplex electrical connection. Select 100-full if the Ethernet port has a 100 MB full-duplex electrical connection. Select 10-full if the Ethernet port has a 10 MB full-duplex electrical connection. Select 1000-fiber if the Ethernet port has a 1000 MB full-duplex fiber cable connection. Select 100-half if the Ethernet port has a 100 MB half-duplex electrical connection. Select 10-half if the Ethernet port has a 10 MB half-duplex electrical connection.
Apply	Click Apply to save the changes in this screen.
Cancel	Click Cancel to begin configuring this screen afresh.

15.4 Switch Setup

Click **Switch > Switch Setup** to configure switching functions.

15.4.1 General Screen

Click **Switch > Switch Setup > General** to display the screen as shown.

Figure 196 Switch > Switch Setup > General

The screenshot shows the 'General' configuration page for a switch. At the top, there's a 'General' tab highlighted, followed by 'Dot3ad', 'Isolation', 'DSCP', 'Storm Control', and 'VC-Shaping'. Below the tabs, there's a section for 'Priority Queue Assignment' with a table of priority levels (0-7) and their corresponding queue numbers (0-7). Each priority level has a drop-down menu showing the assigned queue number. Below this table are 'Apply' and 'Cancel' buttons. Further down, there's an 'Aging Time' section with a text input field containing '300' and a label '[10 ~ 3600]seconds'. It also has 'Apply' and 'Cancel' buttons.

The following table describes the labels in this screen.

Table 144 Switch > Switch Setup > General

LABEL	DESCRIPTION
Priority Queue Assignment	
IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Frames without an explicit priority tag are given the default priority of the ingress port. Use the drop-down list boxes to configure the priority level-to-physical queue mapping.	
The system has 8 physical queues that you can map to the 8 priority levels. On the switch, traffic assigned to higher index queues gets through faster while traffic in lower index queues is dropped if the network is congested.	
Priority Levels (The following descriptions are based on the traffic types defined in the IEEE 802.1d standard (which incorporates IEEE 802.1p).	
priority 0	Typically used for best-effort traffic.
priority 1	This is typically used for non-critical "background" traffic such as bulk transfers that are allowed but that should not affect other applications and users.
priority 2	This is for "spare bandwidth".
priority 3	Typically used for "excellent effort" or better than best effort and would include important business traffic that can tolerate some delay.
priority 4	Typically used for controlled load, latency-sensitive traffic such as SNA (Systems Network Architecture) transactions.
priority 5	Typically used for video that consumes high bandwidth and is sensitive to jitter.
priority 6	Typically used for voice traffic that is especially sensitive to jitter (jitter is the variations in delay).
priority 7	Typically used for network control traffic such as router configuration messages.
Apply	Click Apply to save the changes in this screen.
Cancel	Click Cancel to begin configuring this screen afresh.
Aging Time	Enter a time from 10 to 3600 seconds. This is how long all dynamically learned MAC addresses remain in the MAC address table before they age out (and must be relearned).
Apply	Click Apply to save the changes in this screen.
Cancel	Click Cancel to begin configuring this screen afresh.

15.4.2 Dot3ad Screen

Click **Switch > Switch Setup > Dot3ad** to configure IEEE 802.3ad Link Aggregate Control Protocol (LACP) settings.

Figure 197 Switch > Switch Setup > Dot3ad

The following table describes the labels in this screen.

Table 145 Switch > Switch Setup > Dot3ad

LABEL	DESCRIPTION
Mode	Select the Gigabit Ethernet uplink ports' IEEE 802.3ad mode. disable: turn off or disable LACP. static: statically aggregate the Gigabit Ethernet ports. lacp: have LACP aggregate and control the Gigabit Ethernet ports.
Lacp Priority	Type a number between 0 and 65,535 for the LACP system priority. The switch with the lowest system priority (and lowest port number if system priority is the same) becomes the LACP "server". The LACP "server" controls the operation of LACP setup. Enter a number to set the priority of an active port using LACP. The smaller the number, the higher the priority level.
Lacp Timeout	LACP timeout is the time interval between the individual port exchanges of LACP packets in order to check that the peer port in the trunk group is still up. If a port does not respond after three tries, then it is deemed to be "down" and is removed from the trunk. Set a short timeout (one second) for busy trunked links to ensure that disabled ports are removed from the trunk group as soon as possible. Select either short (1 second) or long (30 seconds).
Load Distribution	Specify the fields in packets that the load sharing mechanism uses. src-mac: Load distribution based on source MAC address of the incoming packets. dst-mac: Load distribution based on destination MAC address of the incoming packets. src-dst-mac: Load distribution based on both source and destination MAC address of the incoming packets. src-ip: Load distribution based on source IP address of the incoming packets. dst-ip: Load distribution based on destination IP address of the incoming packets. src-dst-ip: Load distribution based on both source and destination IP address of the incoming packets. src-dst-ipmac: Load distribution based on both source and destination IP and MAC address of the incoming packets.
Apply	Click Apply to save the changes in this screen.
Cancel	Click Cancel to begin configuring this screen afresh.

15.4.3 Isolation Screen

Click **Switch > Switch Setup > Isolation** to display the screen as shown.

Figure 198 Switch > Switch Setup > Isolation

The following table describes the labels in this screen.

Table 146 Switch > Switch Setup > Isolation

LABEL	DESCRIPTION
Enable	Turn on port isolation to block communications between subscriber ports. When you enable port isolation you do not need to configure the VLAN to isolate subscribers.
Apply	Click Apply to save the changes in this screen.
Cancel	Click Cancel to begin configuring this screen afresh.
Index	This field displays the index number of the isolated VLAN.
Isolated VLAN	This field displays the number of a VLAN for which communications with other VLAN are blocked.
Select	Select an entry's Select check box and click Delete to remove the entry.
Delete	
Isolated VLAN	Specify the number of a VLAN for which you want to block communications with other VLANs.
Apply	Click Apply to save the changes in this screen.
Cancel	Click Cancel to begin configuring this screen afresh.

15.4.4 DSCP Screen

DSCP (Differentiated Services Code Point) is a field in the header of IP packets for packet classification purposes. The QoS (Quality-of-Service) in the IES uses DSCP to provide different level of services and priorities for downstream data transmission.

IEEE 802.1p enables the IES transmit frames according to their 3-bit priority (0~7) in an 802.1q header. Frames with higher priority are served first.

Click **Switch > Switch Setup > DSCP** to display the screen as shown. Use this screen to overwrite the IEEE 802.1p priority value of traffic received through the Gigabit Ethernet interfaces based on its DSCP value.

Figure 199 Switch > Switch Setup > DSCP

DSCP

General Dot3ad Isolation **DSCP** Storm Control VC-Shaping

DSCP mapping (codepoint/priority)

	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0	0
30	0	0	0	0	0	0	0	0	0	0
40	0	0	0	0	0	0	0	0	0	0
50	0	0	0	0	0	0	0	0	0	0
60	0	0	0	0						

Apply Cancel

Slot 3

Enable/Disable DSCP to p-bit mapping function

All	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	

Apply Cancel

The following table describes the labels in this screen.

Table 147 Switch > Switch Setup > DSCP

LABEL	DESCRIPTION
DSCP mapping (codepoint/priority)	Set the IEEE 802.1p priority (0~7) to use for downstream traffic with each DSCP code point service level (0~63).
Apply	Click Apply to save the changes in this section of the screen.
Cancel	Click Cancel to begin configuring this screen afresh.
Slot	Select a slot to configure the priority bit mapping.
Enable/Disable DSCP to p-bit mapping function	Select All or the number of ports to activate or deactivate DSCP to IEEE 802.1p priority mapping.
Apply	Click Apply to save the changes in this section of the screen.
Cancel	Click Cancel to begin configuring this screen afresh.

15.4.5 Storm Control Screen

Click **Switch > Switch Setup > Storm Control** to display the screen as shown. Use this screen to configure broadcast storm control settings for the Gigabit Ethernet interfaces.

Figure 200 Switch > Switch Setup > Storm Control

The following table describes the labels in this screen.

Table 148 Switch > Switch Setup > Storm Control

LABEL	DESCRIPTION
Broadcast	Specify the rate limit for broadcast packets on the IES.
DLF	Specify the rate limit for Destination Lookup Failure (DLF) packets on the IES.
Apply	Click Apply to save the changes in this section of the screen.
Cancel	Click Cancel to begin configuring this screen afresh.

15.4.6 VC-Shaping Screen

Click **Switch > Switch Setup > VC-Shaping** to display the screen as shown.

Figure 201 Switch > Switch Setup > VC-Shaping

The following table describes the labels in this screen.

Table 149 Switch > Switch Setup > VC-Shaping

LABEL	DESCRIPTION
Enable	Click the check box to enable VC-shaping.
Apply	Click Apply to save the changes in this section of the screen.
Cancel	Click Cancel to begin configuring this screen afresh.

CHAPTER 16

Sys Screens

This chapter describes the Sys screens you use to configure general system, access control, syslog, administrator login accounts and management IP settings.

16.1 Authentication, Authorization and Accounting

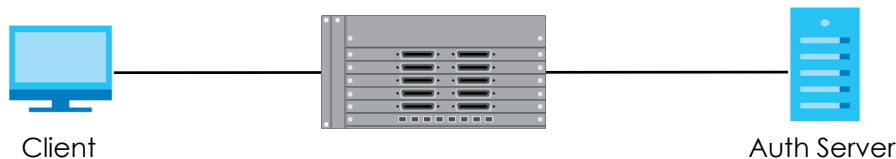
Authentication is the process of determining who a user is and validating access to the system. The system can authenticate users who try to log in based on user accounts configured on the system itself. The system can also use an external authentication server to authenticate a large number of users

Authorization is the process of determining what a user is allowed to do. Different user accounts may have higher or lower privilege levels associated with them. For example, user A may have the right to create new login accounts on the system but user B cannot. The system can authorize users based on user accounts configured on the system itself or it can use an external server to authorize a large number of users.

Accounting is the process of recording what a user is doing. The system can use an external server to track when users log in, log out, execute commands and so on. Accounting can also record system related actions such as boot up and shut down times of the system.

The external servers that perform authentication, authorization and accounting functions are known as AAA servers. The system supports RADIUS (Remote Authentication Dial-In User Service) and TACACS+ (Terminal Access Controller Access-Control System Plus) as external authentication, authorization and accounting servers.

Figure 202 AAA Server



16.1.1 Local User Accounts

By storing user profiles locally on the system, your system is able to authenticate and authorize users without interacting with a network authentication server. However, there is a limit on the number of users you may authenticate in this way.

16.1.2 RADIUS and TACACS+

RADIUS and TACACS+ are security protocols used to authenticate users by means of an external server instead of (or in addition to) an internal device user database that is limited to the memory capacity of the device. In essence, RADIUS and TACACS+ authentication both allow you to validate an unlimited number of users from a central location.

The following table describes some key differences between RADIUS and TACACS+.

Table 150 RADIUS vs. TACACS+

	RADIUS	TACACS+
Transport Protocol	UDP (User Datagram Protocol)	TCP (Transmission Control Protocol)
Encryption	Encrypts the password sent for authentication.	All communication between the client (the IES) and the TACACS server is encrypted.

16.1.3 Accounting Setup

Click **Sys > AAA > Accounting** to display the following screen. Use this screen to configure accounting settings.

Figure 203 Sys > AAA > Accounting

Accounting

Accounting Authentication Authorization Radius Server Tacacs Server

Update Period: 1 1 ~ 2147483647 minute

Apply Cancel

Type	Action	Mode	Method	Privilege
System	☒	-	none	-
Exec	☒	start-stop	none	-
Commands	☒	-	-	0

Apply Cancel

The following table describes the labels in this screen.

Table 151 Sys > AAA > Accounting

LABEL	DESCRIPTION
Update Period	This is the amount of time in minutes before the system sends an update to the accounting server. This is only valid if you select the start-stop option for the Exec entries.
Type	The system supports the following types of events to be sent to the accounting servers: System: Configure the system to send information when the following system events occur: system boots up, system shuts down, system accounting is enabled, system accounting is disabled Exec: Configure the system to send information when an administrator logs in and logs out via the console port, Telnet or SSH. Commands: Configure the system to send information when commands of specified privilege level and higher are executed on the system.
Action	Select this to activate accounting for a specified event types.

Table 151 Sys > AAA > Accounting (continued)

LABEL	DESCRIPTION
Mode	The IES supports two modes of recording login events. Select: start-stop : to have the system send information to the accounting server when a user begins a session, during a user's session (if it lasts past the Update Period), and when a user ends a session. stop-only : to have the system send information to the accounting server only when a user ends a session.
Method	Select whether you want to use RADIUS or TACACS+ for accounting of specific types of events.
Privilege	This field is only configurable for the Commands type of event. Select the threshold command privilege level for which the system should send accounting information. The system will send accounting information when commands at the level you specify and higher are executed on the system.
Apply	Click Apply to save the changes in this screen.
Cancel	Click Cancel to begin configuring this screen afresh.

16.1.4 Authentication Setup

Click **Sys > AAA > Authentication** to display the following screen. Use this screen to specify the methods used to authenticate users accessing the system or changing access privilege levels while logged in.

Figure 204 Sys > AAA > Authentication

Type	Method1	Method2	Method3
Enable	local	none	
Login	local	none	none

Apply Cancel

The following table describes the labels in this screen.

Table 152 Sys > AAA > Authentication

LABEL	DESCRIPTION
Type	This identifies to which kind of access the authentication settings apply. Enable is for using the Enable Privilege screen or <code>enable</code> command to change the privilege level during a configuration session. Login is for logging into a Web Configurator or command configuration session.
Method1 ~ Method3	Specify the databases the system uses to authenticate privilege level changes and logins. Set up the corresponding database properly before you select a method. Configure the local passwords for changing the privilege level in the Enable > Password screen. Configure the local login user accounts in the Sys > User Account screen. The TACACS+ and RADIUS are external servers. You can specify up to two methods for authenticating privilege level changes and up to three methods for authenticating administrator logins. You must configure the Method1 field. If you want the system to check other sources for authentication, specify them in the Method2 and (if applicable) Method3 fields. The system uses Method1 first, then Method2 and finally, (if applicable) Method3. For the Enable type, select local to have the system use its local database to authenticate privilege level change attempts or select tacacs+ to have the system check them against your TACACS+ server. Select local to have the system check the administrator logins against the accounts configured in the Sys > User Account screen. Select radius to have the system check the administrator logins against the accounts configured in your RADIUS server. Select tacacs+ to have the system check the administrator logins against the accounts configured in your TACACS+ server.
Apply	Click Apply to save the changes in this screen.
Cancel	Click Cancel to begin configuring this screen afresh.

16.1.5 Authorization Screen

Click **Sys > AAA > Authorization** to open this screen where you can configure how the system checks whether a user is authorized to execute commands of specific privilege levels.

Which commands a user can access can be controlled by command shell sets configured in the TACACS+ server. This allows you to set certain commands to only be authorized for a specific user. For example, to allow only one user "A" to use the multicast commands, you can configure this system so all the `igmp-mld` commands require a specific privilege level and set the authorization method for this privilege level to **tacacs+**. Then you set the command shell set configured in the TACACS+ server to only give user "A" access to multicast commands.

Figure 205 Sys > AAA > Authorization

Privilege	Method
1	local
2	local
3	local
4	local
5	local
6	local
7	local
8	local
9	local
10	local
11	local
12	local
13	local
14	local

The following table describes the labels in this screen.

Table 153 Sys > AAA > Authorization

LABEL	DESCRIPTION
Privilege	These are the command access levels.
Method	Specify the database the system uses to check whether a user is authorized to execute commands of the specific privilege level. Make sure you set up the corresponding database properly before you select a method. Select local to have the system use its local database. Select tacacs+ to have the system use your TACACS+ server. Select tacacs+ then local to have the system use your TACACS+ server and if the TACACS+ server does not respond, use its local database.
Apply	Click Apply to save the changes in this screen.
Cancel	Click Cancel to begin configuring this screen afresh.

16.1.6 RADIUS Server Setup

Use this screen to configure your RADIUS server settings. Click **Sys > AAA > RADIUS Server** to view the screen as shown.

Figure 206 Sys > AAA > RADIUS Server

RADIUS Server

Accounting Authentication Authorization **RADIUS Server** Tacacs Server

Accounting Server

Mode:

Timeout: [1 ~ 60] sec

Index	IP Address	Port [1 ~ 65535]	Shared Secret
1	0.0.0.0	1813	
2	0.0.0.0	1813	

Authentication Server

Mode:

Timeout: [1 ~ 300] sec

Index	IP Address	Port [1 ~ 65535]	Shared Secret
1	0.0.0.0	1812	
2	0.0.0.0	1812	

The following table describes the labels in this screen.

Table 154 Sys > AAA > RADIUS Server

LABEL	DESCRIPTION
Accounting Server	
Use this section to configure your RADIUS accounting server settings.	
Mode	This field is only valid if you configure multiple RADIUS servers. Select index-priority and the system tries to use the first configured RADIUS server for accounting, if the RADIUS server does not respond then the system tries to use the second RADIUS server. Select round-robin to alternate between the RADIUS servers to which it sends accounting requests.
Timeout	Specify the amount of time in seconds that the system waits for an accounting request response from the RADIUS accounting server.
Apply	Click Apply to save the changes in this screen.
Cancel	Click Cancel to begin configuring this screen afresh.
Index	This is a read-only number representing a RADIUS accounting server entry.
IP Address	Enter the IP address of an external RADIUS accounting server in dotted decimal notation.
Port	The default port of a RADIUS server for accounting is 1813 . You need not change this value unless your network administrator instructs you to do so.

Table 154 Sys > AAA > RADIUS Server (continued)

LABEL	DESCRIPTION
Shared Secret	Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external RADIUS accounting server and the system. This key is not sent over the network. This key must be the same on the external RADIUS accounting server and the system.
Apply	Click Apply to save the changes in this screen.
Cancel	Click Cancel to begin configuring this screen afresh.
Authentication Server	
Use this section to configure your RADIUS authentication settings.	
Mode	This field is only valid if you configure multiple RADIUS servers. Select index-priority and the system tries to authenticate with the first configured RADIUS server, if the RADIUS server does not respond then the system tries to authenticate with the second RADIUS server. Select round-robin to alternate between the RADIUS servers that it sends authentication requests to.
Timeout	Specify the amount of time in seconds that the system waits for an authentication request response from the RADIUS server. If you are using index-priority for your authentication and you are using two RADIUS servers then the timeout value is divided between the two RADIUS servers. For example, if you set the timeout value to 30 seconds, then the system waits for a response from the first RADIUS server for 15 seconds and then tries the second RADIUS server.
Apply	Click Apply to save the changes in this screen.
Cancel	Click Cancel to begin configuring this screen afresh.
Index	This is a read-only number representing a RADIUS server entry.
IP Address	Enter the IP address of an external RADIUS server in dotted decimal notation.
Port	The default port of a RADIUS server for authentication is 1812 . You need not change this value unless your network administrator instructs you to do so.
Shared Secret	Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external RADIUS server and the IES. This key is not sent over the network. This key must be the same on the external RADIUS server and the IES.
Apply	Click Apply to save the changes in this screen.
Cancel	Click Cancel to begin configuring this screen afresh.

16.1.7 TACACS+ Server Setup

Use this screen to configure your TACACS+ server settings. Click **Sys > AAA > Tacacs Server** to view the screen as shown.

Figure 207 Sys > AAA > Tacacs Server

Tacacs Server

Accounting | Authentication | Authorization | Radius Server | **Tacacs Server**

Accounting Server

Mode: index-priority ▼
 Timeout: 30 [1 ~ 60] sec

Apply Cancel

Index	IP Address	Port[1 ~ 65535]	Shared Secret
1	0.0.0.0	49	
2	0.0.0.0	49	

Apply Cancel

Authentication Server

Mode: index-priority ▼
 Timeout: 30 [1 ~ 300] sec

Apply Cancel

Index	IP Address	Port[1 ~ 65535]	Shared Secret
1	0.0.0.0	49	
2	0.0.0.0	49	

Apply Cancel

Authorization Server

Mode: index-priority ▼
 Timeout: 30 [1 ~ 300] sec

Apply Cancel

Index	IP Address	Port[1 ~ 65535]	Shared Secret
1	0.0.0.0	49	
2	0.0.0.0	49	

Apply Cancel

The following table describes the labels in this screen.

Table 155 Sys > AAA > Tacacs Server

LABEL	DESCRIPTION
Accounting Server	
Use this section to configure your TACACS+ accounting server settings.	
Mode	This field is only valid if you configure multiple TACACS+ servers. Select index-priority and the system tries to use the first configured TACACS+ server for accounting, if the TACACS+ server does not respond then the system tries to use the second TACACS+ server. Select round-robin to alternate between the TACACS+ servers.
Timeout	Specify the amount of time in seconds that the system waits for an accounting request response from the TACACS+ accounting server.
Apply	Click Apply to save the changes in this screen.

Table 155 Sys > AAA > Tacacs Server (continued)

LABEL	DESCRIPTION
Cancel	Click Cancel to begin configuring this screen afresh.
Index	This is a read-only number representing a TACACS+ accounting server entry.
IP Address	Enter the IP address of an external TACACS+ accounting server in dotted decimal notation.
Port	The default port of a TACACS+ server for accounting is 49 . You need not change this value unless your network administrator instructs you to do so.
Shared Secret	Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external TACACS+ accounting server and the system. This key is not sent over the network. This key must be the same on the external TACACS+ accounting server and the system.
Apply	Click Apply to save the changes in this screen.
Cancel	Click Cancel to begin configuring this screen afresh.
Authentication Server	
Use this section to configure your TACACS+ authentication settings.	
Mode	This field is only valid if you configure multiple TACACS+ servers. Select index-priority and the system tries to authenticate with the first configured TACACS+ server, if the TACACS+ server does not respond then the system tries to authenticate with the second TACACS+ server. Select round-robin to alternate between the TACACS+ servers that it sends authentication requests to.
Timeout	Specify the amount of time in seconds that the system waits for an authentication request response from the TACACS+ server. If you are using index-priority for your authentication and you are using two TACACS+ servers then the timeout value is divided between the two TACACS+ servers. For example, if you set the timeout value to 30 seconds, then the system waits for a response from the first TACACS+ server for 15 seconds and then tries the second TACACS+ server.
Apply	Click Apply to save the changes in this screen.
Cancel	Click Cancel to begin configuring this screen afresh.
Index	This is a read-only number representing a TACACS+ server entry.
IP Address	Enter the IP address of an external TACACS+ server in dotted decimal notation.
Port	The default port of a TACACS+ server for authentication is 49 . You need not change this value unless your network administrator instructs you to do so.
Shared Secret	Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external TACACS+ server and the IES. This key is not sent over the network. This key must be the same on the external TACACS+ server and the IES.
Apply	Click Apply to save the changes in this screen.
Cancel	Click Cancel to begin configuring this screen afresh.
Authorization Server	
Use this section to configure your TACACS+ authorization settings.	
Mode	This field is only valid if you configure multiple TACACS+ servers. Select index-priority and the system tries to authorize with the first configured TACACS+ server, if the TACACS+ server does not respond then the system tries to authorize using the second TACACS+ server. Select round-robin to alternate between the TACACS+ servers.

Table 155 Sys > AAA > Tacacs Server (continued)

LABEL	DESCRIPTION
Timeout	Specify the amount of time in seconds that the system waits for an authorization request response from the TACACS+ server. If you are using index-priority for your authorization and you are using two TACACS+ servers then the timeout value is divided between the two TACACS+ servers. For example, if you set the timeout value to 30 seconds, then the system waits for a response from the first TACACS+ server for 15 seconds and then tries the second TACACS+ server.
Apply	Click Apply to save the changes in this screen.
Cancel	Click Cancel to begin configuring this screen afresh.
Index	This is a read-only number representing a TACACS+ server entry.
IP Address	Enter the IP address of an external TACACS+ server in dotted decimal notation.
Port	The default port of a TACACS+ server for authorization is 49 . You need not change this value unless your network administrator instructs you to do so.
Shared Secret	Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external TACACS+ server and the IES. This key is not sent over the network. This key must be the same on the external TACACS+ server and the IES.
Apply	Click Apply to save the changes in this screen.
Cancel	Click Cancel to begin configuring this screen afresh.

16.2 Service Access Control

Click **Sys > Access Control** to open the following screens. Use these screens to set management IP settings and to configure which services may be used to access the system.

16.2.1 SNMP

Click **Sys > Access Control > SNMP** to open the following screen.

Figure 208 Sys > Access Control > SNMP

SNMP | Secured Client | Secured Client6

General Settings

Get Community: public
Set Community: public
Trap Community: public
Version: v2c

Apply Cancel

Trap Destination

Index	Version	IP	Port[1 ~ 65535]	User Name
1	v2c	0.0.0.0	162	-
2	v2c	0.0.0.0	162	-
3	v2c	0.0.0.0	162	-
4	v2c	0.0.0.0	162	-

Apply Cancel

User

Index	Enable	Name	Level	Hash	Encrypt
1	V	admin	auth	md5	des

Apply Cancel

The following table describes the labels in this screen.

Table 156 Sys > Access Control > SNMP

LABEL	DESCRIPTION
General Settings	
Get Community	Enter the get community, which is the password for the incoming Get- and GetNext- requests from the management station. You can use up to 31 English keyboard characters; spaces are not allowed.
Set Community	Enter the set community, which is the password for incoming Set-requests from the management station. You can use up to 31 English keyboard characters; spaces are not allowed.
Trap Community	Enter the trap community, which is the password sent with each trap to the SNMP manager. You can use up to 31 English keyboard characters; spaces are not allowed.
Version	Specify the SNMP version and access mode. Select v2c to allow SNMPv2 read/write access. Select v3 to allow SNMPv3 read/write access with additional user authentication and data encryption options. Select v3v2c to allow SNMPv3 read/write and SNMPv2 read-only access.
Apply	Click Apply to save the changes in this screen.
Cancel	Click Cancel to begin configuring this screen afresh.
Trap Destination	
Enter the IP address of a station to send your SNMP trap to.	

Table 156 Sys > Access Control > SNMP (continued)

LABEL	DESCRIPTION
Index	This field displays the number of a station entry.
Version	Specify the format of the SNMP trap Protocol Data Unit (PDU) to be sent. The default is v2c .
IP	Enter the IP address of the trap server. Use an IPv4 address in dotted decimal notation or an IPv6 address and prefix in colon hexadecimal notation.
Port	Enter the port number upon which the station listens for SNMP traps.
User Name	This field is applicable when you select v3 in the Version field. Enter the username to be included in the trap PDUs.
Apply	Click Apply to save the changes in this screen.
Cancel	Click Cancel to begin configuring this screen afresh.
User Configure the administrative login accounts for SNMP management. Use the User Account screen to create administrative login accounts.	
Index	This field displays the index number.
Enable	This field displays whether the administrative login account is activated or not.
Name	This field displays the administrative login account user name.
Level	Select noauth to disable SNMPv3 user authentication and encryption for SNMP communication. Select auth to enable SNMPv3 user authentication. Select priv to enable SNMPv3 user authentication and encryption for SNMP communication using a private key generated from the password.
Hash	Specify an authentication method. Select md5 (Message Digest 5) to produce a 128-bit digest for minimal authentication security. Select sha (Secure Hash Algorithm) to produce a 160-bit digest for maximum authentication security.
Encrypt	Specify an encryption method. Select des or aes . Data Encryption Standard (DES) is a widely used method of data encryption using a secret key. DES applies a 56-bit key to each 64-bit block of data. Advanced Encryption Standard (AES) is a newer method of data encryption that also uses a secret key. AES is more secure than DES.
Apply	Click Apply to save the changes in this screen.
Cancel	Click Cancel to begin configuring this screen afresh.

16.2.2 Secured Client Screen

Click **Sys > Access Control > Secured Client** to open the following screen. Use this screen to configure IPv4 address ranges of trusted computers that may manage the system.

Figure 209 Sys > Access Control > Secured Client

Index	Enable	Start Address	End Address	Telnet	SSH	SNMP	FTP	Web	ICMP	HTTPS	VoIP
1	☒	0.0.0.0	0.0.0.0	☒	☒	☒	☒	☒	☒	☒	☒
2	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐	☐
3	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐	☐
4	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐	☐
5	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐	☐
6	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐	☐
7	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐	☐
8	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐	☐
9	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐	☐
10	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐	☐
11	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐	☐
12	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐	☐
13	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐	☐
14	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐	☐
15	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐	☐
16	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐	☐

Apply Cancel

The following table describes the labels in this screen.

Table 157 Sys > Access Control > Secured Client

LABEL	DESCRIPTION
Index	This is the client set index number. A "client set" is a group of one or more "trusted computers" from which an administrator may use a service to manage the system.
Enable	Select this check box to activate this secured client set. Clear the check box if you wish to temporarily disable the set without deleting it.
Start Address End Address	Configure the IP address range of trusted computers from which you can manage the system. The system checks if the client IP address of a computer requesting a service or protocol matches the range set here. The system immediately disconnects the session if it does not match.
Telnet/SSH/SNMP/ FTP/Web/ICMP/ HTTPS/VoIP	Select services that may be used for managing the system from the specified trusted computers.
Apply	Click Apply to save the changes in this screen.
Cancel	Click Cancel to begin configuring this screen afresh.

16.2.3 Secured Client6 Screen

Click **Sys > Access Control > Secured Client6** to open the following screen. Use this screen to configure IPv6 address ranges of trusted computers that may manage the system.

Figure 210 Sys > Access Control > Secured Client6

Index	Enable	IP6 Address	Mask	Telnet	SNMP	FTP	Web	ICMP	HTTPS
1	☒	::	0	☒	☒	☒	☒	☒	☒
2	☐	::	0	☐	☐	☐	☐	☐	☐
3	☐	::	0	☐	☐	☐	☐	☐	☐
4	☐	::	0	☐	☐	☐	☐	☐	☐
5	☐	::	0	☐	☐	☐	☐	☐	☐
6	☐	::	0	☐	☐	☐	☐	☐	☐
7	☐	::	0	☐	☐	☐	☐	☐	☐
8	☐	::	0	☐	☐	☐	☐	☐	☐
9	☐	::	0	☐	☐	☐	☐	☐	☐
10	☐	::	0	☐	☐	☐	☐	☐	☐
11	☐	::	0	☐	☐	☐	☐	☐	☐
12	☐	::	0	☐	☐	☐	☐	☐	☐
13	☐	::	0	☐	☐	☐	☐	☐	☐
14	☐	::	0	☐	☐	☐	☐	☐	☐
15	☐	::	0	☐	☐	☐	☐	☐	☐
16	☐	::	0	☐	☐	☐	☐	☐	☐

Apply Cancel

The following table describes the labels in this screen.

Table 158 Sys > Access Control > Secured Client6

LABEL	DESCRIPTION
Index	This is the client set index number. A "client set" is a group of one or more "trusted computers" from which an administrator may use a service to manage the system.
Enable	Select this check box to activate this secured client set. Clear the check box if you wish to temporarily disable the set without deleting it.
IP6 Address	Configure the IPv6 address range of trusted computers from which you can manage the system. The system checks if the client IP address of a computer requesting a service or protocol matches the range set here and immediately disconnects the session if it does not match.
Mask	Specify the bit number of the subnet mask of an IP address. The range is 0 to 128 for IPv6.

Table 158 Sys > Access Control > Secured Client6 (continued)

LABEL	DESCRIPTION
Telnet/SNMP/FTP/ Web/ICMP/HTTPS	Select services that may be used for managing the system from the specified trusted computers.
Apply	Click Apply to save the changes in this screen.
Cancel	Click Cancel to begin configuring this screen afresh.

16.3 Syslog

Click **Sys > SYSLOG** to configure settings for sending logs to external syslog servers.

Figure 211 Sys > SYSLOG

The following table describes the labels in this screen.

Table 159 Sys > SYSLOG

LABEL	DESCRIPTION
SYSLOG Enable	Select this check box to activate syslog (system logging) and then configure the syslog parameters described in the following fields.
IP	Enter the IP address of the syslog server for the corresponding log facility. Use an IPv4 address in dotted decimal notation or an IPv6 address and prefix in colon hexadecimal notation.
Apply	Click Apply to save the changes in this screen.
Cancel	Click Cancel to begin configuring this screen afresh.

16.4 General Setup

Click **Sys > General Setup** to open the following screen.

Figure 212 Sys > General Setup

General Setup

Host Name: aln

Location:

Contact Person's Name:

Product Model: IES4105

System Up Time: 0(days) : 3:07:01

Bootbase Version: V1.01 | 02/23/2017

Session Login Message:

Apply Cancel

Time Server Type: None

Time Server IP Address: Sync

Current Time: 11 : 37 : 38

New Time (hh:mm:ss): 11 : 37 : 38

Current Date: 2037 - 2 - 5

New Date (yyyy-mm-dd): 2037 - 2 - 5

Time Zone: UTC

Daylight Saving Time: ☐

Start Time: First Sunday of January at 0:00

End Time: First Sunday of January at 0:00

Apply Cancel

The following table describes the labels in this screen.

Table 160 Sys > General Setup

LABEL	DESCRIPTION
Host Name	Choose a descriptive name for identification purposes. This name consists of up to 63 English keyboard characters; spaces are not allowed.
Location	Enter the geographic location of your system. You can use up to 31 English keyboard characters; spaces are not allowed.
Contact Person's Name	Enter the name of the person in charge of this system. You can use up to 31 English keyboard characters; spaces are not allowed.
Product Model	This field displays your device type.
System Up Time	This field shows how long the system has been running since the last time it was started.
Bootbase Version	This field displays the bootbase version that the IES is using and its build date.
Session Login Message	Specify a note to display when users attempt to log into the system's management interfaces.
Apply	Click Apply to save the changes in this screen.
Cancel	Click Cancel to begin configuring this screen afresh.

Table 160 Sys > General Setup (continued)

LABEL	DESCRIPTION
Time Server Type	Enter the time service protocol that a timeserver uses. Not all timeservers support all protocols, so you may have to use trial and error to find a protocol that works. The main differences between them are the time format. When you select the Daytime (RFC 867) format, the system displays the day, month, year and time with no time zone adjustment. When you use this format it is recommended that you use a Daytime timeserver within your geographical time zone. Time (RFC-868) format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. NTP (RFC-1305) is similar to Time (RFC 868). None is the default value. Enter the time manually. Each time you turn on the system, the time and date will be reset to 2000-1-1 0:0.
Time Server IP Address	Enter the IP address (or URL if you configure a domain name server in the IP Setup screen) of your timeserver. The system searches for the timeserver for up to 60 seconds. If you select a timeserver that is unreachable, then this screen will appear locked for 60 seconds. Please wait.
Current Time	This field displays the time you open this menu (or refresh the menu).
New Time (hh:min:ss)	Enter the new time in hour, minute and second format. The new time then appears in the Current Time field after you click Apply .
Current Date	This field displays the date you open this menu.
New Date (yyyy-mm-dd)	Enter the new date in year, month and day format. The new date then appears in the Current Date field after you click Apply .
Time Zone	Select the time difference between UTC (Universal Time Coordinated, formerly known as GMT, Greenwich Mean Time) and your time zone from the drop-down list box.
Daylight Saving Time	Daylight saving is a period from late spring to fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Click the check box to enable the daylight saving time.
Start Time	Configure the date when Daylight Saving Time starts.
End Time	Configure the date when Daylight Saving Time ends.
Apply	Click Apply to save the changes in this screen.
Cancel	Click Cancel to begin configuring this screen afresh.

16.5 IP Setup

Click **Sys > IP Setup** to configure the management IPv4 and IPv6 addresses.

16.5.1 IPv4 Setup

Click **Sys > IP Setup > IPv4 Setup** to open the following screen. Use this screen to configure the system and management IPv4 settings.

Figure 213 Sys > IP Setup > IPv4 Setup

IPv4 Setup

IPv4 Setup **IPv6 Setup**

Inband

DHCP Operation: **Release** **Renew** Note, after pressing button "Release", you can't access device through management network.

DHCP mode: disable ▾

VID: 1

Pbit: 7

IP Address: 172.23.44.201

Subnet Mask: 255.255.255.0

Default Gateway: 172.23.44.254

Outband

IP Address: 192.168.0.1

Subnet Mask: 255.255.255.0

Apply **Cancel** **Refresh**

The following table describes the labels in this screen.

Table 161 Sys > IP Setup > IPv4 Setup

LABEL	DESCRIPTION
Inband	These fields configure in-band management settings. In-band management refers to accessing the management interface through a network port (not the management port).
DHCP Operation	Click Release to release the IES's dynamic IPv4 inband management IP address. You will no longer be able to access the IES through the inband management IP address. Click Renew to renew the IES's dynamic IPv4 inband management IP address.
DHCP Mode	Select enable to have the IES use a dynamic IPv4 inband management IP address. Select disable to have the IES use a static IPv4 inband management IP address.
VID	Enter the VLAN ID (Identifier) of the management (CPU) VLAN. You must connect to the system through a port that is a member of the management (CPU) VLAN in order to perform in-band management.
Pbit	Enter the priority bit of the management VLAN.
IP Address	Enter the in-band management IPv4 address for the system.
Subnet Mask	Enter the in-band management IPv4 subnet mask for the system in dotted decimal notation for example 255.255.255.0.
Default Gateway	Enter the IP address of the default outgoing gateway in dotted decimal notation.
Outband	These fields configure out-of-band management settings. Out-of-band management refers to accessing the management interface through a management port.
IP Address	Enter the out-of-band management IPv4 address for the management port.
Subnet Mask	Enter the out-of-band management IP subnet mask for the management port in dotted decimal notation for example 255.255.255.0.
Apply	Click Apply to save the changes in this screen.
Cancel	Click Cancel to begin configuring this screen afresh.

16.5.2 IPv6 Setup

Click **Sys > IP Setup > IPv6 Setup** to open the following screen. Use this screen to configure the system and management IPv6 settings.

Figure 214 Sys > IP Setup > IPv6 Setup

The following table describes the labels in this screen.

Table 162 Sys > IP Setup > IPv6 Setup

LABEL	DESCRIPTION
Default Management	Select Inband to connect to the network port's IPv6 address to access the management interface. Select Outband to connect to the management port's IPv6 address to access the management interface.
Inband	These fields configure in-band management settings. In-band management refers to accessing the management interface through a network port (not the management port).
IP Address	Enter the in-band management IPv6 address for the system.
Default Netmask	Enter the default subnet mask for this IPv6 address.
Outband	These fields configure out-of-band management settings. Out-of-band management refers to accessing the management interface through a management port.
IP Address	Enter the out-of-band management IPv6 address for the management port.
Default Netmask	Enter the default subnet mask for this IPv6 address.
Default Gateway	Enter the IPv6 address of the default outgoing gateway.
Apply	Click Apply to save the changes in this screen.
Cancel	Click Cancel to begin configuring this screen afresh.

16.6 Monitor Screens

Click **Sys > Monitor** to configure and view hardware monitor thresholds.

16.6.1 Monitor

Click **Sys > Monitor > Monitor** to open the following screen. Use this screen to view hardware status information and set the hardware monitor high and low thresholds for generating alarms.

Figure 215 Sys > Monitor > Monitor

The screenshot shows the 'Monitor' screen with three tabs: 'Monitor' (selected), 'Statistics', and 'CPU Utilization'. A 'Slot' dropdown is set to '1'. The screen is divided into three main sections: Voltage, Temperature, and Fan Speed. Each section has a table of hardware metrics and adjustable high/low limits. At the bottom, there is a 'Battery Saving' section with checkboxes for input1, input2, input3, and input4, and 'Apply' and 'Cancel' buttons.

Voltage					
Index	Volt	Current	Nominal	High_lmt[0 ~ 25000]mV	Low_lmt[0 ~ 25000]mV
1	+1.8V	1790 (mV)	1800 (mV)	1926 (mV)	1674 (mV)
2	+1.0V	1037 (mV)	1050 (mV)	1124 (mV)	977 (mV)
3	+3.3V	3360 (mV)	3300 (mV)	3531 (mV)	3069 (mV)
4	+2.5V	2486 (mV)	2500 (mV)	2675 (mV)	2325 (mV)
5	+14.0V	14484 (mV)	14000 (mV)	15120 (mV)	12880 (mV)

Temperature				
Index	Temperature	Current	High_lmt[-50~ 120]	Low_lmt[-50~ 120]
1	NP	36	71	-50
2	FPGA	32	69	-50
3	DDR	31	69	-50

Fan Speed				
Index	Fan Speed	Current	High_lmt[0~ 15000] RPM	Low_lmt[0~ 15000] RPM
1	Fan 1	2119	8800	1000
2	Fan 2	3011	7000	1000
3	Fan 3	2119	8800	1000

Battery Saving ☐ input1 ☐ input2 ☐ input3 ☐ input4

Apply Cancel

The following table describes the labels in this screen.

Table 163 Sys > Monitor > Monitor

LABEL	DESCRIPTION
Slot	Select the number of a card's slot.
Voltage	The power supply for each voltage has a sensor that can detect and report the voltage.
Index	This field displays the number of the power supply in the list.
Volt	This field displays the voltage that the power supply provides. Measured in volts (V).
Current	This field displays the current voltage reading. Measured in millivolts (mV).

Table 163 Sys > Monitor > Monitor (continued)

LABEL	DESCRIPTION
Nominal	This field displays the normal (expected) voltage in millivolts (mV).
High_Lmt	Use these fields to set the maximum voltage threshold for each sensor.
Low_Lmt	Use these fields to set the minimum voltage threshold for each sensor.
Temperature	Each temperature sensor can detect and report the temperature.
Index	This field displays the number of the temperature sensor in the list.
Temperature	This field displays the name of the temperature sensor.
Current	This field displays the current temperature at this sensor (in degrees Celsius).
High_Lmt	Use these fields to set the maximum temperature threshold for each sensor.
Low_Lmt	Use these fields to set the minimum temperature threshold for each sensor.
Fan Speed	A properly functioning fan is an essential component (along with a sufficiently ventilated, cool operating environment) in order for the device to stay within the temperature threshold. Each fan has a sensor that can detect and report the fan's RPM (Rotations Per Minute).
Index	This field displays the number of the fan in the list.
Fan Speed	This field displays the name of the fan.
Current	This is the fan's current RPM reading.
High_Lmt	Use these fields to set the maximum RPM threshold for each sensor.
Low_Lmt	Use these fields to set the minimum RPM threshold for each sensor.
Battery Saving	Configures battery saving mode on the specified alarm input. When you deploy the IES with a UPS and the specified alarm input is triggered, the IES turns off subscriber data traffic in order to support PSTN calls for as long as possible. See Section 3.6.1 on page 45 for details on the alarm inputs.
Apply	Click Apply to save the changes in this screen.
Cancel	Click Cancel to begin configuring this screen afresh.

16.6.2 Statistics

Click **Sys > Monitor > Statistics** to open the following screen. Use this screen to view hardware status information.

Figure 216 Sys > Monitor > Statistics

Statistics

MonitorStatisticsCPU Utilization

Slot1

Voltage					
Name	Nominal	Max	Min	Avg	Current
+1.8V	1800(mV)	1790(mV)	1790(mV)	1790(mV)	1790(mV)
+1.0V	1050(mV)	1048(mV)	1037(mV)	1037(mV)	1037(mV)
+3.3V	3300(mV)	3360(mV)	3360(mV)	3360(mV)	3360(mV)
+2.5V	2500(mV)	2513(mV)	2486(mV)	2486(mV)	2486(mV)
+14.0V	14000(mV)	14484(mV)	14389(mV)	14417(mV)	14389(mV)

Temperature					
Name	Nominal	Max	Min	Avg	Current
NP	-	38	31	34	36
FPGA	-	34	30	31	32
DDR	-	33	30	30	31

Fan Speed					
Name	Nominal	Max	Min	Avg	Current
Fan 1	-	2136	2071	2123	2119
Fan 2	-	3032	2980	3010	3013
Fan 3	-	2137	2070	2122	2118

The following table describes the labels in this screen.

Table 164 Sys > Monitor > Statistics

LABEL	DESCRIPTION
Slot	Select the number of a card's slot.
Voltage	The power supply for each voltage has a sensor that can detect and report the voltage.
Name	This field displays the voltage that the power supply provides. Measured in volts (V).
Nominal	This field displays the normal (expected) voltage in millivolts (mV).
Max	This field displays the maximum voltage in millivolts (mV).
Min	This field displays the minimum voltage in millivolts (mV).
Avg	This field displays the average voltage in millivolts (mV).
Current	This field displays the current voltage reading. Measured in millivolts (mV).
Temperature	Each temperature sensor can detect and report the temperature.
Name	This field displays the name of the temperature sensor.
Nominal	This field displays the normal temperature for each sensor.
Max	This field displays the maximum temperature detected at each sensor.
Min	This field displays the minimum temperature detected at each sensor.
Avg	This field displays the average temperature detected at each sensor.
Current	This field displays the current temperature for each sensor (in degrees Celsius).

Table 164 Sys > Monitor > Statistics (continued)

LABEL	DESCRIPTION
Fan Speed	A properly functioning fan is an essential component (along with a sufficiently ventilated, cool operating environment) in order for the device to stay within the temperature threshold. Each fan has a sensor that can detect and report the fan's RPM (Rotations Per Minute).
Name	This field displays the name of the fan.
Nominal	This field displays the normal RPM for each sensor.
Max	This field displays the maximum RPM detected at each sensor.
Min	This field displays the minimum RPM detected at each sensor.
Avg	This field displays the average RPM detected at each sensor.
Current	This is the fan's current RPM reading.

16.6.3 CPU Utilization

Click **Sys > Monitor > CPU Utilization** to display recent CPU utilization.

Figure 217 Sys > Monitor > CPU Utilization

The screenshot shows the 'CPU Utilization' screen with a 'Refresh' button and a table of CPU usage data. The table has 8 columns: 'sec' and 'util' repeated four times. The data shows a fluctuating but generally stable CPU utilization between 24% and 34% over the 60-second period.

CPU Utilization							
Monitor Statistics CPU Utilization							
Refresh							
sec	util	sec	util	sec	util	sec	util
0	38.19	1	30.75	2	32.09	3	25.98
4	28.55	5	28.32	6	27.63	7	28.51
8	29.34	9	26.76	10	28.36	11	29.61
12	29.94	13	26.80	14	27.07	15	29.77
16	25.90	17	31.19	18	26.32	19	29.56
20	32.41	21	31.54	22	27.12	23	26.87
24	30.26	25	31.89	26	28.73	27	29.82
28	27.84	29	28.22	30	29.62	31	29.05
32	24.33	33	29.04	34	27.96	35	30.38
36	29.54	37	28.27	38	28.23	39	32.47
40	29.19	41	24.71	42	32.32	43	28.05
44	24.06	45	29.14	46	29.26	47	30.19
48	28.94	49	29.92	50	30.96	51	24.92
52	32.24	53	27.17	54	24.42	55	31.14
56	30.65	57	25.17	58	27.68	59	34.70
60	29.19	61	30.02	62	29.01		

The following table describes the labels in this screen.

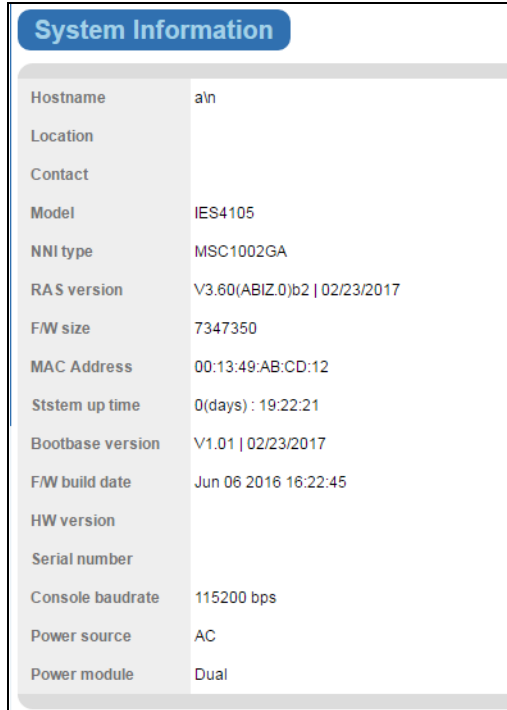
Table 165 Sys > Monitor > CPU Utilization

LABEL	DESCRIPTION
Refresh	Click this to update the screen's information.
sec	This field displays the individual second.
util	This field displays the percentage of CPU utilization.

16.7 System Information

Click **Sys > System Information** to display the general system information about the IES.

Figure 218 Sys > System Information



System Information	
Hostname	a/n
Location	
Contact	
Model	IES4105
NNI type	MSC1002GA
RAS version	V3.60(ABIZ.0)b2 02/23/2017
F/W size	7347350
MAC Address	00:13:49:AB:CD:12
System up time	0(days) : 19:22:21
Bootbase version	V1.01 02/23/2017
F/W build date	Jun 06 2016 16:22:45
HW version	
Serial number	
Console baudrate	115200 bps
Power source	AC
Power module	Dual

The following table describes the labels in this screen.

Table 166 Sys > System Information

LABEL	DESCRIPTION
Hostname	This field displays the system name.
Location	This field displays the geographic location of the system.
Contact	This field displays the system contact person information.
Model	This field displays the system's model name.
NNI type	This field displays the Network Node Interface (NNI) type. This is the management card.
RAS version	This field displays the firmware version.
F/W size	This field displays the firmware size.
MAC Address	This field displays the IES Media Access Control (MAC) address.
System up time	This field displays how long the system has been running since the last time it was started.
Bootbase version	This field displays the bootbase version that the IES is using and its build date.
F/W build date	This field displays when the firmware was built.
HW version	This field displays the hardware version.
Serial number	This field displays the hardware serial number.
Console baudrate	This field displays the console port baud rate.

Table 166 Sys > System Information (continued)

LABEL	DESCRIPTION
Power source	This field displays the type of power (AC or DC) the IES is currently using.
Power module	This field displays the type of power module (AC, DC, or Dual).

16.8 User Account Screen

Click **Sys > User Account** to open the following screen. Use this screen to manage administrator accounts.

Figure 219 Sys > User Account

Index	Enable	Name	Privilege	Select
1	V	admin	14	☒

The following table describes the labels in this screen.

Table 167 Sys > User Account

LABEL	DESCRIPTION
Name	Type a user name for the account
Password	Type a password for the account.
Retype Password to confirm	Type the password again to make sure you have entered it properly.
Privilege	Select the administrator account's level of access privileges.
Apply	Click Apply to save the changes in this screen.
Cancel	Click Cancel to begin configuring this screen afresh.
Index	This column numbers the administrator account entries.
Enable	This column displays a "V" if the administrator account is turned on or a "-" if the account is turned off.
Name	This column displays the user names of the accounts.
Privilege	This column displays the level of access privileges of the accounts.
Select	Select an entry's Select check box and click Delete to remove the entry or click Modify to edit the entry.
Modify	Click Modify to change the settings of the selected entry.
Delete	Click Delete to remove the selected entry.

CHAPTER 17

VLAN Screens

17.1 VLAN Introduction

A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same group or groups; the traffic must first go through a router.

In MTU (Multi-Tenant Unit) applications, VLAN is vital in providing isolation and security among the subscribers. When properly configured, VLAN prevents one subscriber from accessing the network resources of another on the same LAN, thus a user will not see the printers and hard disks of another user in the same building. If you have enabled port isolation in the **Switch Setup** screen, you do not need to configure the VLAN to isolate subscribers.

VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. In traditional switched environments, all broadcast packets go to each and every individual port. With VLAN, all broadcasts are confined to a specific broadcast domain.

17.2 IEEE 802.1Q Tagged VLAN

The IEEE 802.1Q Tagged VLAN uses both explicit and implicit tagging.

1 Explicit Tagging

A VLAN identifier is added to the frame header that identifies the source VLAN.

2 Implicit Tagging

The MAC (Media Access Control) number, the port or other information is used to identify the source of a VLAN frame.

Tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges - they are not confined to the switch on which they were created. The VLANs can be created statically by hand or dynamically through GVRP. The VLAN ID associates a frame with a specific VLAN and provides the information that switches need to process the frame across the network. A tagged frame is four bytes longer than an untagged frame and contains two bytes of TPID (Tag Protocol Identifier, residing within the type/length field of the Ethernet frame) and two bytes of TCI (Tag Control Information, starts after the source address field of the Ethernet frame).

The CFI (Canonical Format Indicator) is a single-bit flag, always set to zero for Ethernet switches. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port. The remaining twelve bits define the VLAN ID, giving a possible maximum number of

4,096 VLANs. Note that user priority and VLAN ID are independent of each other. A frame with VID (VLAN Identifier) of null (0) is called a priority frame, meaning that only the priority level is significant and the default VID of the ingress port is given as the VID of the frame. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

TPID	User Priority	CFI	VLAN ID
2 Bytes	3 Bits	1 Bit	12 bits

The system handles up to 4093 VLANs (VIDs 1-4093). The switch accepts incoming frames with VIDs 1-4093.

17.2.1 Forwarding Tagged and Untagged Frames

Each port on the switch is capable of passing tagged or untagged frames. To forward a frame from an 802.1Q VLAN-aware switch to an 802.1Q VLAN-unaware switch, the switch first decides where to forward the frame and then strips off the VLAN tag. To forward a frame from an 802.1Q VLAN-unaware switch to an 802.1Q VLAN-aware switch, the switch first decides where to forward the frame, and then inserts a VLAN tag reflecting the ingress port's default VID. The default PVID is VLAN 1 for all ports, but this can be changed.

The egress (outgoing) port of a frame is determined on the combination of the destination MAC address and the VID of the frame. For a unicast frame, the egress port based by the destination address must be a member of the VID, also; otherwise, the frame is blocked. A broadcast frame (or a multicast frame for a multicast group that is known by the system) is duplicated only on ports that are members of the VID (except the ingress port itself), thus confining the broadcast to a specific domain.

Whether to tag an outgoing frame depends on the setting of the egress port on an individual VLAN and port basis (remember that a port can belong to multiple VLANs). If the tagging on the egress port is enabled for the VID of a frame, then the frame is transmitted as a tagged frame; otherwise, it is transmitted as an untagged frame.

17.3 Enet VLAN Screen

Click **VLAN > Enet VLAN** to display the screen shown next. You can assign the IES's Gigabit Ethernet interfaces to be members of a VLAN group in this screen. This is an IEEE 802.1Q VLAN.

Figure 220 VLAN > Enet VLAN

Enet VLAN Setup

Enet Port [1 ~ 2]

VID all or [1 ~ 4093]

Apply **Cancel**

Show vlan from enet port 1 to 2 **Apply**

Index	VID	Enet Port	Select
1	1	1	☒
2	1	2	☐

Page 1 of 1 **Previous** **Next**

Delete

The following table describes the labels in this screen.

Table 168 VLAN > Enet VLAN

LABEL	DESCRIPTION
Enet Port	Enter a Gigabit Ethernet interface number.
VID	Enter the VLAN ID (VLAN Identifier) for this static VLAN entry; the valid range is between 1 and 4093.
Apply	Click Apply to save the changes in this screen.
New	Click New to start configuring the screen again.
Cancel	Click Cancel to start configuring the screen again.
Show vlan from enet port	Type a range of Gigabit Ethernet Ports that you want to view and click Apply to display them in the table below.
Index	This field displays the number of the VLAN entry in this list.
VID	This field displays the ID number of the VLAN group. Click the number to edit the VLAN settings.
Enet Port	This column displays the VLAN tagging settings of the Gigabit Ethernet interfaces.
Page X of X	This identifies which page of information is displayed and the total number of pages of information.
Previous/Next	Click one of these buttons to show the preceding/following screen if the information cannot be displayed in one screen.
Select	Select a VLAN's Select radio button and click Delete to remove the VLAN. You cannot delete the CPU (management) VLAN.
Delete	

17.4 Enet VLAN Untag Screen

Click **VLAN > Enet VLAN Untag** to display the screen shown next. You can assign the IES's Gigabit Ethernet interfaces to be members of an untagged VLAN group in this screen.

Figure 221 VLAN > Enet VLAN Untag

Enet Untag VLAN Setup

Enet Port [1 ~ 2]

Untag VID [1 ~ 4093]

Pbit [0 ~ 7]

Apply **Cancel**

Show vlan untag from enet port 1 to 2 **Apply**

Index	Untag VID	Pbit	Enet Port	Select
1	1	0	1	☐
2	1	0	2	☐

Delete

The following table describes the labels in this screen.

Table 169 VLAN > Enet VLAN Untag

LABEL	DESCRIPTION
Enet Port	Enter a Gigabit Ethernet interface number.
Untag VID	Enter the untagged VLAN ID (VLAN Identifier) for this static VLAN entry; the valid range is between 1 and 4093.
Pbit	Specify the priority bit of the specified untagged VLAN ID.
Apply	Click Apply to save the changes in this screen.
New	Click New to start configuring the screen again.
Cancel	Click Cancel to start configuring the screen again.
Show vlan untag from enet port	Type a range of Gigabit Ethernet ports that you want to view and click Apply to display them in the table below.
Index	This field displays the number of the VLAN entry in this list.
Untag VID	This field displays the ID number of the untagged VLAN group.
Pbit	This field displays the priority bit of the specified untagged VLAN ID.
Enet Port	This column displays the VLAN tagging settings of the Gigabit Ethernet interfaces.
Select	Select a VLAN's Select radio button and click Delete to remove the VLAN. You cannot delete the CPU (management) VLAN.
Delete	

17.5 Port VLAN TLS Screen

Click **VLAN > Port VLAN TLS** to display the screen shown next. You can configure Transparent LAN Service (TLS) of a port on a line card in this screen.

Figure 222 VLAN > Port VLAN TLS

ID	State	Card Type	Uptime
1	Active	MSC1002GA	19:28:30
2	Active	VOP1164A-61	19:27:15
3	-	ALC1132A-51	-
4	Active	ELC1132A-45	19:27:35
5	Active	VLC1124A-51	19:26:53

The following table describes the labels in this screen.

Table 170 VLAN > Port VLAN TLS

LABEL	DESCRIPTION
Slot	Use the drop down list boxes to select a DSL or FE port on a line card for which you want to configure VLAN TLS.
Port	
Load	Click Load to display the port's current settings.
Index	This field displays the number of a VLAN TLS entry.
VPI/VCI	This field displays the VPI and VCI values on the specified port.
svid	This field displays the Subscriber VLAN ID (SVID) on the specified port.
spbit (force)	This field displays the Subscriber priority bit on the specified port.
Select	Select a VLAN TLS' Select radio button and click Delete to remove the VLAN TLS on the specified port.
Delete	
PVC	Click the check box to enable PVC on the specified port.
VPI/VCI	Specify the Virtual Path Identifier and Virtual Circuit Identifier on the specified port.
svid	Specify the Subscriber VLAN ID on the specified port.
spbit	Specify the Subscriber priority bit on the specified.
Force spbit	Click the check box to have untagged, priority tagged, and customer tagged frames adopt the Subscriber priority bit in upstream traffic.
Apply	Click Apply to save the changes in this screen.
Cancel	Click Cancel to start configuring the screen again.
ID	This is the slot number of a line card. Click the index number of an active line card to display the VLAN TLS Setup screen where you can view and delete settings on the selected line card.

Table 170 VLAN > Port VLAN TLS (continued)

LABEL	DESCRIPTION
State	This field displays the line card's current operational status. Active means the line card is operating normally. init means the IES is initializing the line card. disable means a manager has disabled the line card. inactive means the line card is starting up or is not operating normally. This could be due to the card starting, a firmware upgrade in progress or malfunction.
Card Type	This field displays the type of a line card.
Uptime	This field displays how long the line card has been running since the last time it was started.

17.5.1 VLAN TLS Setup Screen

Click **VLAN > Port VLAN TLS** and then click the ID of an active line card. Use this screen to view the VLAN TLS settings on the line card's ports.

Figure 223 Port VLAN TLS: VLAN TLS Setup

The following table describes the labels in this screen.

Table 171 Port VLAN TLS: VLAN TLS Setup

LABEL	DESCRIPTION
Index	This field displays the number of a VLAN TLS entry.
Port	This field displays the port number of the specified line card.
PVC	This field displays the VPI and VCI values on the specified port.
svid	This field displays the Subscriber VLAN ID (SVID) on the specified port.
spbit (force)	This field displays the Subscriber priority bit on the specified port.
Select	Select a VLAN TLS' Select radio button and click Delete to remove the VLAN TLS on the specified port.
select All	Or, you can click the select All check box and then click Delete to remove all the VLAN TLS settings.
Delete	

17.6 Port VLAN Trunk Screens

Click **VLAN > Port VLAN Trunk** to configure VLAN tagging and trunk mode on a line card's ports.

17.6.1 Uni-Tag Setup

Click **VLAN > Port VLAN Trunk > uni-Tag** to display the screen shown below. You can select a port of a line card to configure its VLAN tagging settings.

Figure 224 VLAN > Port VLAN Trunk > uni-Tag

ID	State	Card Type	Uptime
1	Active	MSC1002GA	19:30:09
2	Active	VOP1164A-61	19:28:54
3	-	ALC1132A-51	-
4	Active	ELC1132A-45	19:29:14
5	Active	VLC1124A-51	19:28:32

The following table describes the labels in this screen.

Table 172 VLAN > Port VLAN Trunk > uni-Tag

LABEL	DESCRIPTION
Slot	Use the drop down list boxes to select a DSL or FE port on a line card for which you want to configure VLAN trunk.
Port	
Load	Click Load to display the port's current settings.
Index	This field displays the number of a VLAN trunk entry.
VPI/VCI	This field displays the VPI and VCI values on the specified port.
svid	This field displays the Service provider VLAN ID (SVID) on the specified port.
uni-vid	This field displays the UNI VLAN ID on the specified port.
Select	Select a VLAN trunk' Select radio button and click Delete to remove the VLAN trunk on the specified port.
Delete	
PVC	Click the check box to enable PVC on the specified port.
VPI/VCI	Specify the Virtual Path Identifier and Virtual Circuit Identifier on the specified port.
uni-vid	Specify a UNI VLAN ID on the specified port.
s-tag add	Click the check to add a Service provider VLAN tag.
svid	Specify the Service provider VLAN ID on the specified port.

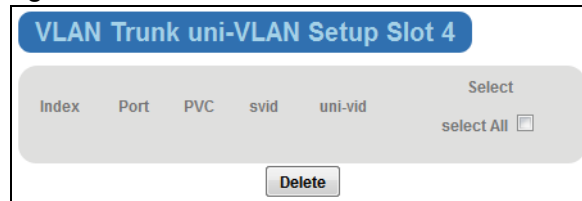
Table 172 VLAN > Port VLAN Trunk > uni-Tag (continued)

LABEL	DESCRIPTION
Apply	Click Apply to save the changes in this screen.
Cancel	Click Cancel to start configuring the screen again.
ID	This is the slot number of a line card. Click the index number of an active line card to display the VLAN Trunk uni-VLAN Setup screen where you can view and delete settings on the selected line card.
State	This field displays the line card's current operational status. Active means the line card is operating normally. init means the IES is initializing the line card. disable means a manager has disabled the line card. inactive means the line card is starting up or is not operating normally. This could be due to the card starting, a firmware upgrade in progress or malfunction.
Card Type	This field displays the type of a line card.
Uptime	This field displays how long the line card has been running since the last time it was started.

17.6.1.1 VLAN Trunk uni-VLAN Setup

Click **VLAN > Port VLAN Trunk** and then click the ID of an active line card. Use this screen to view the VLAN trunk settings on the line card's ports.

Figure 225 Port VLAN Trunk: VLAN Trunk uni-VLAN Setup



The following table describes the labels in this screen.

Table 173 Port VLAN Trunk: VLAN Trunk uni-VLAN Setup

LABEL	DESCRIPTION
Index	This field displays the number of a VLAN trunk entry.
Port	This field displays the port number of the specified line card.
PVC	This field displays the VPI and VCI values on the specified port.
svid	This field displays the Service provider VLAN ID (SVID) on the specified port.
uni-vid	This field displays the UNI VLAN ID on the specified port.
Select	Select a VLAN trunk's Select radio button and click Delete to remove the VLAN trunk on the specified port.
select All	Or, you can click the select All check box and then click Delete to remove all the VLAN trunk settings.
Delete	

17.6.2 Uni-Untag Setup

Click **VLAN > Port VLAN Trunk > uni-Untag** to display the screen shown below. You can select a port of a line card to configure its untagged packets' settings.

Figure 226 VLAN > Port VLAN Trunk > uni-Untag

The screenshot shows the 'VLAN Trunk Setup' window with the 'uni-Untag' tab selected. At the top, there are dropdown menus for 'Slot' (set to 3) and 'Port' (set to 1), followed by a 'Load' button. Below this is a table with columns: Index, VPI/VCI, Type, svid, spbit, cvid, cpbit, Ether type, and Select. A 'Delete' button is positioned below the table. The main configuration area contains several fields: 'PVC' with a checkbox, 'VPI/VCI' with two input boxes separated by a slash, 'Ether type set' with a checkbox, 'Ether type' with an input box, 'svid' with an input box and range '[1 ~ 4093]', 'spbit' with an input box and range '[0 ~ 7]', 'c-tag add' with a checkbox, 'cvid' with an input box and range '[1 ~ 4093]', and 'cpbit' with an input box and range '[0 ~ 7]'. 'Apply' and 'Cancel' buttons are at the bottom of the configuration area. At the very bottom is a table showing the status of various cards.

ID	State	Card Type	Uptime
1	Active	MSC1002GA	19:31:12
2	Active	VOP1164A-61	19:29:57
3	-	ALC1132A-51	-
4	Active	ELC1132A-45	19:30:17
5	Active	VLC1124A-51	19:29:35

The following table describes the labels in this screen.

Table 174 VLAN > Port VLAN Trunk > uni-Untag

LABEL	DESCRIPTION
Slot	Use the drop down list boxes to select a DSL or FE port on a line card for which you want to configure VLAN trunk.
Port	
Load	Click Load to display the port's current settings.
Index	This field displays the number of a VLAN trunk entry.
VPI/VCI	This field displays the VPI and VCI values on the specified port.
Type	This field displays whether the Ethernet Type is enabled or not.
svid	This field displays the Service provider VLAN ID (SVID) on the specified port.
spbit	This field displays the service provider priority bit on the specified port.
cvid	This field displays the Customer VLAN ID (CVID) on the specified port.
cpbit	This field displays the customer priority bit on the specified port.
Ether Type	This field displays the Ethernet type on the specified port.
Select	Select an entry's Select radio button and click Delete to remove the specified entry on the specified port.
Delete	
PVC	Click the check box to enable PVC on the specified port.
VPI/VCI	Specify the Virtual Path Identifier and Virtual Circuit Identifier on the specified port.

Table 174 VLAN > Port VLAN Trunk > uni-Untag (continued)

LABEL	DESCRIPTION
Ether type set	Click the check box to enable the Ethernet type setting.
Ether type	Specify the Ethernet type on the specified port, 0000-ffff in hexadecimal.
svid	Specify the Service provider VLAN ID on the specified port.
spbit	Specify the service provider priority bit on the specified port.
c-tag add	Click the check box to add a Customer tag.
cvid	Specify the customer VLAN ID on the specified port.
cpbit	Specify the customer priority bit on the specified port.
Apply	Click Apply to save the changes in this screen.
Cancel	Click Cancel to start configuring the screen again.
ID	This is the slot number of a line card. Click the index number of an active line card to display the VLAN Trunk Uni-untag Setup screen where you can view and delete settings on the selected line card.
State	This field displays the line card's current operational status. Active means the line card is operating normally. init means the IES is initializing the line card. disable means a manager has disabled the line card. inactive means the line card is starting up or is not operating normally. This could be due to the card starting, a firmware upgrade in progress or malfunction.
Card Type	This field displays the type of a line card.
Uptime	This field displays how long the line card has been running since the last time it was started.

17.6.2.1 VLAN Trunk Uni-untag Setup

Click **VLAN > Port VLAN Trunk** and then click the ID of an active line card. Use this screen to view the untagged packets' settings on the line card's ports.

Figure 227 Port VLAN Trunk: VLAN Trunk Uni-Untag Setup

The screenshot shows a web interface for configuring VLAN Trunk Uni-Untag settings for Slot 3. It features a table with columns for Index, Port, PVC, Type, svid, spbit, cvid, cpbit, and Ether type. There are 'Select' and 'select All' buttons to the right of the table, and a 'Delete' button at the bottom.

The following table describes the labels in this screen.

Table 175 Port VLAN Trunk: VLAN Trunk Uni-Untag Setup

LABEL	DESCRIPTION
Index	This field displays the number of a uni-untag entry.
Port	This field displays the port number of the specified line card.
PVC	This field displays the VPI and VCI values on the specified port.
Type	This field displays whether the Ethernet Type is enabled or not.
svid	This field displays the Service provider VLAN ID (SVID) on the specified port.
spbit	This field displays the service provider priority bit on the specified port.
cvid	This field displays the Customer VLAN ID (CVID) on the specified port.

Table 175 Port VLAN Trunk: VLAN Trunk Uni-Untag Setup (continued)

LABEL	DESCRIPTION
cpbit	This field displays the customer priority bit on the specified port.
Ether type	This field displays the Ethernet type on the specified port.
Select	Select a VLAN trunk's Select radio button and click Delete to remove the VLAN trunk on the specified port.
select All	Or, you can click the select All check box and then click Delete to remove all the VLAN trunk settings.
Delete	

17.7 Port VLAN Translation Screen

Click **VLAN > Port VLAN Translation** to display the screen shown below. Use this screen to change a VLAN tag to another VLAN ID.

Figure 228 VLAN > Port VLAN Translation

ID	State	Card Type	Uptime
1	Active	MSC1002GA	19:36:21
2	Active	VOP1164A-61	19:35:06
3	-	ALC1132A-51	-
4	Active	ELC1132A-45	19:35:26
5	Active	VLC1124A-51	19:34:44

The following table describes the labels in this screen.

Table 176 VLAN > Port VLAN Translation

LABEL	DESCRIPTION
Slot	Use the drop down list boxes to select a DSL or FE port on a line card for which you want to configure VLAN translation.
Port	
Load	Click Load to display the port's current settings.
Index	This field displays the number of a VLAN translation entry.
VPI/VCI	This field displays the VPI and VCI values on the specified port.

Table 176 VLAN > Port VLAN Translation (continued)

LABEL	DESCRIPTION
svid	This field displays the Service provider VLAN ID (SVID) on the specified port.
cvid	This field displays the Customer VLAN ID (CVID) on the specified port.
uni-vid	This field displays the UNI VLAN ID on the specified port.
tag	This field displays "V" to indicate the VLAN translation on this port is for tagged packets.
Select Delete	Select an entry's Select radio button and click Delete to remove the specified entry on the specified port.
PVC	Select the check box to enable PVC on the specified port.
VPI/VCI	Specify the Virtual Path Identifier and Virtual Circuit Identifier on the specified port.
uni-vid	Specify the UNI VLAN ID on the specified port.
svid	Specify the Service provider VLAN ID on the specified port.
c-tag add	Click the check box to add a Customer tag.
cvid	Specify the customer VLAN ID on the specified port.
Apply	Click Apply to save the changes in this screen.
Cancel	Click Cancel to start configuring the screen again.
ID	This is the slot number of a line card. Click the index number of an active line card to display the VLAN Translation Setup screen where you can view and delete settings on the selected line card.
State	This field displays the line card's current operational status. Active means the line card is operating normally. init means the IES is initializing the line card. disable means a manager has disabled the line card. inactive means the line card is starting up or is not operating normally. This could be due to the card starting, a firmware upgrade in progress or malfunction.
Card Type	This field displays the type of a line card.
Uptime	This field displays how long the line card has been running since the last time it was started.

17.7.1 VLAN Translation Setup

Click **VLAN > Port VLAN Translation** and then click the ID of an active line card. Use this screen to view the VLAN translation settings on the line card's ports.

Figure 229 Port VLAN Translation: VLAN Translation Setup

The screenshot shows a web interface for configuring VLAN translation on a specific line card (Slot 3). It features a table with columns for 'Index', 'Port', 'PVC', 'svid', 'cvid', and 'uni-vid'. A 'Select' column with radio buttons is on the right. Below the table is a 'Delete' button. A 'select All' checkbox is also present.

The following table describes the labels in this screen.

Table 177 Port VLAN Translation: VLAN Translation Setup

LABEL	DESCRIPTION
Index	This field displays the number of a VLAN translation entry.
Port	This field displays the port number of the specified line card.
PVC	This field displays the VPI and VCI values on the specified port.
svid	This field displays the Service provider VLAN ID (SVID) on the specified port.
cvid	This field displays the Customer VLAN ID (CVID) on the specified port.
uni-vid	This field displays the UNI VLAN ID on the specified port.
Select	Select a VLAN translation's Select radio button and click Delete to remove the VLAN translation on the specified port.
select All	Or, you can click the select All check box and then click Delete to remove all the VLAN translation settings.
Delete	

17.8 Port VLAN Transparent Screen

Click **VLAN > Port VLAN Transparent** to display the screen shown below. Use this screen to configure the transparent VLAN on a line card's ports.

Figure 230 VLAN > Port VLAN Transparent

ID	State	Card Type	Uptime
1	Active	MSC1002GA	19:37:19
2	Active	VOP1164A-61	19:36:04
3	-	ALC1132A-51	-
4	Active	ELC1132A-45	19:36:24
5	Active	VLC1124A-51	19:35:42

The following table describes the labels in this screen.

Table 178 VLAN > Port VLAN Transparent

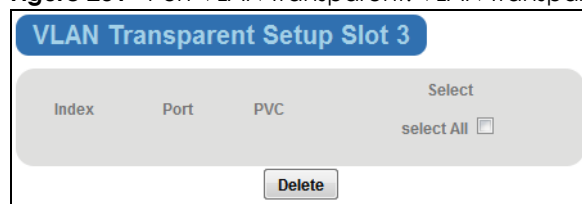
LABEL	DESCRIPTION
Slot	Use the drop down list boxes to select a DSL or FE port on a line card for which you want to configure VLAN transparent.
Port	
Load	Click Load to display the port's current settings.
Index	This field displays the number of a VLAN transparent entry.

Table 178 VLAN > Port VLAN Transparent (continued)

LABEL	DESCRIPTION
VPI/VCI	This field displays the VPI and VCI values on the specified port.
Select Delete	Select an entry's Select radio button and click Delete to remove the specified entry on the specified port.
PVC	Select the check box to enable PVC on the specified port.
VPI/VCI	Specify the Virtual Path Identifier and Virtual Circuit Identifier on the specified port.
Apply	Click Apply to save the changes in this screen.
Cancel	Click Cancel to start configuring the screen again.
ID	This is the slot number of a line card. Click the index number of an active line card to display the VLAN Transparent Setup screen where you can view and delete settings on the selected line card.
State	This field displays the line card's current operational status. Active means the line card is operating normally. init means the IES is initializing the line card. disable means a manager has disabled the line card. inactive means the line card is starting up or is not operating normally. This could be due to the card starting, a firmware upgrade in progress or malfunction.
Card Type	This field displays the type of a line card.
Uptime	This field displays how long the line card has been running since the last time it was started.

17.8.1 VLAN Transparent Setup

Click **VLAN > Port VLAN Transparent** and then click the ID of an active line card. Use this screen to view the transparent VLAN settings on the line card's ports.

Figure 231 Port VLAN Transparent: VLAN Transparent Setup

The following table describes the labels in this screen.

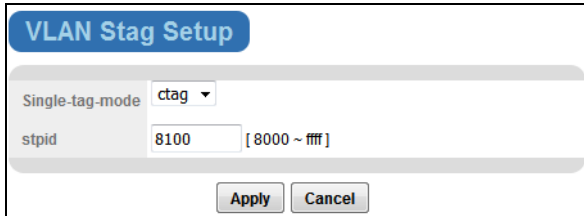
Table 179 Port VLAN Translation: VLAN Transparent Setup

LABEL	DESCRIPTION
Index	This field displays the number of a VLAN transparent entry.
Port	This field displays the port number of the specified line card.
PVC	This field displays the VPI and VCI values on the specified port.
Select select All Delete	Select a VLAN transparent's Select radio button and click Delete to remove the VLAN transparent on the specified port. Or, you can click the select All check box and then click Delete to remove all the VLAN transparent settings.

17.9 VLAN S-tag Setup

Click **VLAN > VLAN S-tag Setup** to configure the single tag mode and the Service provider Tag Protocol Identifier (S TPID).

Figure 232 VLAN > VLAN S-tag Setup



The following table describes the labels in this screen.

Table 180 VLAN > VLAN S-tag Setup

LABEL	DESCRIPTION
Single-tag-mode	Specify the single tag mode. stag : single-tag packets sent from NNI tagged with S tag ctag : single-tag packets sent from NNI tagged with C tag
stpid	Specify the S-tag TPID in hexadecimal format.
Apply	Click Apply to save the changes in this screen.
Cancel	Click Cancel to start configuring the screen again.

CHAPTER 18

VoIP

This chapter shows how to configure the Voice over IP (VoIP) features on your system.

18.1 Country Code Screen

Use this screen to configure the regional VoIP settings of the IES, and to see details of the VoIP settings affected by the country of operation you select. Click **VoIP** > **Country Code**. The following screen displays.

Figure 233 VoIP > Country Code

Country Code

Country

42,Turkey

Modify

Cancel

Country	42,Turkey
Impedance	270ohm_750ohm_150nf
Coding Type	ulaw
Loop Current	25 mA
Tax Type	metering

Ring Parameters

Frequency (Hz)	25.0
Amplitude (Vrms)	75.0
On time 1 (s)	2.00
Off time 1 (s)	4.00
On time 2 (s)	2.00
Off time 2 (s)	4.00

Caller ID Parameters

CID Type	during ring
Payload Type	ETSI-SDMF
First TAS Type	NULL
Second TAS Type	NULL
First TAS Interval (ms)	0
Second TAS Interval (ms)	0
Start To Ring (ms)	500

Tons Parameter

Dial Tone	450Hz -9.5dB continuous
Ring Back Tone	450Hz -9.5dB on 2.000s off 4.000s
Busy Tone	450Hz -9.5dB on 0.500s off 0.500s
Congestion Tone	3x(450Hz -9.5dB on 0.200s off 0.200s) 450Hz -9.5dB on 0.600s off 0.200s
Special Information Tone	950Hz -9.5dB on 0.300s 1400Hz -9.5dB on 0.300s 1800Hz -9.5dB on 0.300s off 1.000s
Call Wait Tone #1	450Hz -11.5dB on 0.200s off 0.600s 450Hz -11.5dB on 0.200s off 8.000s
Call Wait Tone #2	450Hz -11.5dB on 0.200s off 0.600s 450Hz -11.5dB on 0.200s off 8.000s
Special Dial Tone	450Hz -9.5dB on 1.000s off 0.250s
Howler Tone	1400+2060+2460+2600Hz -6.0dB on 0.100s off 0.100s
Warning Tone	450Hz -9.5dB on 0.200s off 0.200s 450Hz -9.5dB on 0.600s off 0.200s

ConformationTone	450Hz -9.5dB on 0.400s off 0.400s
Recall Dial Tone	3x(350+440Hz -12.5dB on 0.100s off 0.100s) 350+440Hz -12.5dB continuous
Holding Tone	350+450Hz -14.5dB on 0.500s off 0.500s 450Hz -11.5dB on 0.500s off 2.500s
Number Unobtainable Tone	450Hz -9.5dB on 0.200s off 0.200s

Pulse Parameter

Flash Min (ms)	90
Flash Max (ms)	500
Break Min (ms)	47
Break Max (ms)	80
Make Min (ms)	30
Make Max (ms)	55
Inter Digit Min (ms)	250
Off Hook Min (ms)	30
Pulse Digit	enabled

MeterParameters

Frequency (kHz)	12
Pulse On Time (ms)	200
Pulse Off Time (ms)	200
Reverse On Time (ms)	400
Reverse Off Time (ms)	600

The following table describes the labels in this screen.

Table 181 VoIP > Country Code

LABEL	DESCRIPTION
Country	Select the country in which the system will be used.
Modify	Click this to save your changes and display the region-specific VoIP settings below.
Cancel	Click this to return this screen to its last-saved values.
Country	This field displays the country you select from the Country drop-down list box.
Impedance	Displays the line impedance or impedance range in ohms.
Coding Type	This displays either alaw or ulaw . The a-law companding algorithm is commonly used in Europe, while the u-law (mu-law or μ -law) algorithm is commonly used in the USA and Japan.
Loop Current	Displays the supplied line current in milliamps.
Tax Type	Displays the payphone charging signal type; metering (12/16 Hz signal) or reversebattery (polarity reversal signal).
Ring Parameters	This section displays region-specific information about the phone's ring.
Frequency (Hz)	This displays the frequency of the phone ring in Hertz.
Amplitude (Vrms)	This displays the amplitude of the phone ring in Volts root-mean-squared.
On Time 1 (s)	This displays the duration of the first ring (in seconds).
Off Time 1 (s)	This displays the length of time between the first and second ring (in seconds).
On Time 2 (s)	This displays the duration of the second ring (in seconds).
Off Time 2 (s)	This displays the wait time after the second ring before the first ring is sent again (in seconds).
Caller ID Parameters	This section displays region-specific information about caller ID
CID Type	This displays whether the caller ID information is sent before the ring (prior ring displays) or at the same time as the ring (during ring displays).
Payload Type	This displays the caller ID payload type. SDMF displays if caller ID uses the Single Data Message Format (which transmits caller number, date and time). MDMF displays if caller ID uses the Multiple Data Message Format (which transmits caller name, number, date and time).
First TAS Type	TAS (Terminal equipment Alerting Signal) is a tone sent prior to the transmission of caller ID information. This is the primary TAS signal type, which is used in a line reversal scenario. The possible values are: NULL : No TAS signal is sent. DT_AS : Dual Tone Alerting Signal. RP_AS : Ringing Pulse Alerting Signal. Line_Reversal : Simple line polarity inversion.
Second TAS Type	This is the secondary TAS signal type, which is used in a line reversal followed by DT-AS/RP-AS scenario. NULL : No TAS signal is sent. DT_AS : Dual Tone Alerting Signal. RP_AS : Ringing Pulse Alerting Signal.
First TAS Interval (ms)	This is the first TAS timeout period in milliseconds.

Table 181 VoIP > Country Code (continued)

LABEL	DESCRIPTION
Second TAS Interval (ms)	This is the second TAS timeout period in milliseconds.
Start To Ring (ms)	This is the wait time between the caller ID information being sent and the ring signal being sent (available for the prior ring type only).
Tones Parameters	This section displays region-specific information about call progress tones.
Dial Tone	This is the tone sent to indicate that a call can be dialed.
Ring Back Tone	This is the tone sent to indicate that the callee's phone is ringing.
Busy Tone	This is the tone sent to indicate that the callee's line is busy.
Congestion Tone	This is the tone sent to indicate that the network is busy.
Special Information Tone	This field displays the tone sent only in H.248 when the softswitch asks for it.
Call Wait Tone #1	This is the tone sent to indicate that a second call is incoming while the first is still in progress.
Call Wait Tone #2	This is reserved for future use.
Special Dial Tone	This is the tone sent to indicate that certain three-way calling, conference and call transfer services are available.
Howler Tone	This is the tone sent to indicate that the handset has been left off-hook too long.
Warning Tone	This is the tone sent to indicate that the telephone circuit is operating abnormally.
Confirmation Tone	This is the tone sent to indicate that user-entered information has been successfully received.
Recall Dial Tone	This is the tone sent when some special digit pattern is pressed. The digit pattern is specified in the dial plan.
Holding Tone	This is the tone sent to indicate that the call has been put on hold.
Number Unobtainable Tone	This tone indicates that the system cannot reach the number the user dialed.
Pulse Parameters	This section displays region-specific information about pulse dialling.
Flash Min/Max (ms)	These display the minimum and maximum hook flash times.
Break Min/Max (ms)	These display the minimum and maximum times for ending a pulse.
Make Min/Max (ms)	These display the minimum and maximum times for beginning a pulse.
Inter Digit Min (ms)	This displays the minimum waiting time between pulsed digits.
Off Hook Min (ms)	This displays the minimum waiting time before entering off hook state.
Pulse Digit	This displays whether pulse digit detection is enabled.
Meter Parameters	This section displays region-specific information about call metering.
Frequency (kHz)	This displays the frequency of the call-metering tone (in kilohertz).
Pulse On Time (ms)	This displays the duration of the call-metering tone (in milliseconds).
Pulse Off Time (ms)	This displays the minimum time between call-metering tones (in milliseconds).
Reverse On Time (ms)	This displays the duration of the battery reversal.
Reverse Off Time (ms)	This displays the minimum interval between two battery reversal.

18.2 H.248 Screens

These screens are available when using H.248 firmware. Click **VoIP > H.248** to configure the H.248 settings and view H.248 packet statistics.

18.2.1 H.248 Setup

Click **VoIP > H.248 > H.248** to open the screen below. Use this screen to configure settings specific to the system's H.248 VoIP card.

Figure 234 VoIP > H.248 > H.248

The screenshot displays the H.248 configuration page. At the top, there are tabs for 'H.248' (selected) and 'Statistics'. Below the tabs, the configuration is organized into a list of settings on the left and their corresponding input fields on the right. The settings include MG Name, Enable, MG Port, MGC IP, MGC Port, Softswitch Type, MGC2, MGC2 IP, MGC2 Port, T.38, VBD, Force Version 1, RFC2833, RFC2833 Payload Type, DSCP, Encoding, Transport, Init Retransmission Time, Min Retransmission Time, Max Retransmission Time, Retransmission Window, Inactivity Timer, RTP Start Port, RTP End Port, RTP TID Prefix, RTP TID Suffix Start Number, RTP TID Suffix Length, Start Digit Map Timeout, Short Digit Map Timeout, Long Digit Map Timeout, and Registration Retry Timer. At the bottom, there are 'Apply' and 'Cancel' buttons.

Setting	Value
MG Name	DEFVAL
Enable	☐
MG Port [1025 ~ 65535]	2944
MGC IP	0.0.0.0
MGC Port [1025 ~ 65535]	2944
Softswitch Type	DEFVAL
MGC2	☐
MGC2 IP	
MGC2 Port [1025 ~ 65535]	0
T.38	☐
VBD	☐
Force Version 1	☐
RFC2833	☐
RFC2833 Payload Type [96 ~ 127]	101
DSCP [0 ~ 63]	48
Encoding	long
Transport	udp
Init Retransmission Time [1 ~ 200] * 100ms	20
Min Retransmission Time [1 ~ 10] * 100ms	1
Max Retransmission Time [10 ~ 200] * 100ms	40
Retransmission Window [10 ~ 600] * 100ms	250
Inactivity Timer [0 ~ 65535] * 10ms	0
RTP Start Port [4000 ~ 64000]	60000
RTP End Port [5000 ~ 65000]	65000
RTP TID Prefix	RTP/
RTP TID Suffix Start Number	1
RTP TID Suffix Length [0 ~ 15]	0
Start Digit Map Timeout [0 ~ 99] sec	16
Short Digit Map Timeout [1 ~ 99] sec	4
Long Digit Map Timeout [1 ~ 99] sec	4
Registration Retry Timer [0 ~ 1440] sec	60

Apply Cancel

The following table describes the labels in this screen.

Table 182 VoIP > H.248 > H.248

LABEL	DESCRIPTION
MG Name	Specify the H.248 Media Gateway's (MG) name.
Enable	Click the check to have the IES start the MG operation.
MG Port	Specify the TCP/UDP port number the H.248 MG uses.
MGC IP	Specify the H.248 primary Media Gateway Controller's (MGC) IP address.
MGC Port	Specify the TCP/UDP port number the H.248 primary MGC uses.
Softswitch Type	Select special call flows for interoperability with special MGCs. DEFVAL: The default call flow. zxss10-ss: Special call flow for interoperability with the ZTE zxss10 soft switch. huawei-soft3000: Special call flow for interoperability with the HUAWEI-soft3000 soft switch. alu-5020: Special call flow for interoperability with the ALU-5020 soft switch. nsn: Special call flow for interoperability with the NSN soft switch. iskratel: Special call flow for interoperability with the ISKRATEL soft switch.
MGC2	Click the check box to enable a secondary MGC.
MGC2 IP	Specify the H.248 secondary MGC's IP address.
MGC2 Port	Specify the TCP/UDP port number the H.248 secondary MGC uses.
T.38	Click the check box to enable support for the T.38 fax relay standard.
VBD	Click the check box to enable the Voice Band Data (VBD) service.
Force Version 1	Click the check box to force the IES to use only H.248 version 1 for VoIP.
RFC2833	Click the check box to enable RFC 2833 Dual Tone Multi Frequency (DTMF) relay.
RFC2833 Payload Type	Specify the RFC 2833 RTP payload type used for DTMF relay.
DSCP	Specify the DSCP value carried on the H.248 packets.
Encoding	Select the text encoding type of the H.248 messages the IES sends out. long: long text encoding short: short text encoding
Transport	Specify whether to use UDP or TCP as the H.248 transport protocol.
Init Retransmission Time	Specify the initial retransmit timer, which is used when the MG didn't establish a control link between the MG and MGC during this enable time.
Min Retransmission Time	Specify the minimum duration between any two packets after registration.
Max Retransmission Time	Specify the maximum duration between any two packets after registration.
Retransmission Window	Specify the total retransmit timer.
Inactivity Timer	Specify the inactivity timeout.
RTP Start Port	Specify the UDP port range used by RTP packets.
RTP End Port	start port: an even number from 4000-64000 end port: an even number from 5000-65000, at least 1000 larger than start port
RTP TID Prefix	Specify the RTP ephemeral termination ID's prefix. It can be up to 31 characters.

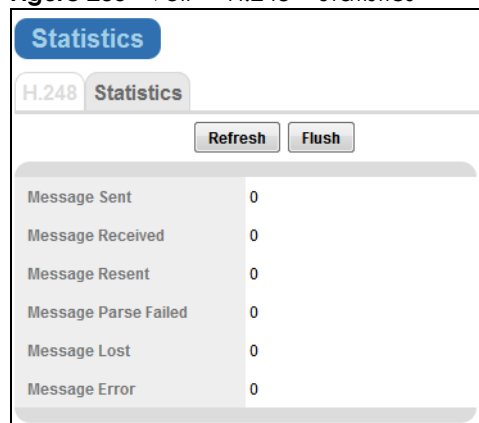
Table 182 VoIP > H.248 > H.248 (continued)

LABEL	DESCRIPTION
RTP TID Suffix Start Number	Specify the RTP ephemeral termination ID's suffix start number. It can be up to 15 digits.
RTP TID Suffix Length	Specify how many digits to use for the RTP ephemeral termination ID.
Start Digit Map Timeout	Specify the timeout period if the user doesn't send any DTMF signal after off-hook, in seconds (0-99). 0 disables the timeout.
Short Digit Map Timeout	Specify the H.248 short timeout, in seconds (1-99). You define the short and long timeout values and the IES selects which to use.
Long Digit Map Timeout	Specify the H.248 long timeout, in seconds (1-99). You define the short and long timeout values and the IES selects which to use.
Registration Retry Timer	Specify the registration retry time for the un-registered state.
Apply	Click Apply to save the changes in this screen.
Cancel	Click Cancel to start configuring the screen again.

18.2.2 H.248 Statistics

Click **VoIP > H.248 > Statistics** to view the H.248 message statistics.

Figure 235 VoIP > H.248 > Statistics



The following table describes the labels in this screen.

Table 183 VoIP > H.248 > Statistics

LABEL	DESCRIPTION
Refresh	Click Refresh to update all the statistics.
Flush	Click Flush to clear all the statistics.
Message Sent	This field displays the number of H.248 messages the system sent out.
Message Received	This field displays the number of H.248 messages the system received.
Message Resent	This field displays the number of H.248 messages the system resent.
Message Parse Failed	This field displays the number of H.248 RX messages that don't follow the H.248 syntax.

Table 183 VoIP > H.248 > Statistics (continued)

LABEL	DESCRIPTION
Message Lost	This field displays the number of H.248 messages the system lost.
Message Error	This field displays the number of error H.248 messages.

18.3 IP Setup Screens

Click **VoIP > IP Setup** to configure VoIP and RTP interfaces' settings.

18.3.1 VoIP Interface Screen

Use this screen to specify the DHCP, IP address, subnet mask, VLAN ID and DNS information for the VoIP interface managed by the IES. Click **VoIP > IP Setup > VoIP interface** to display the following screen.

Figure 236 VoIP > IP Setup > VoIP interface

The screenshot shows the 'VoIP IP Setup' screen with two tabs: 'VoIP interface' (active) and 'RTP interface'. The 'VoIP interface' tab contains two sections. The first section, 'DHCP Operation', includes 'Release' and 'Renew' buttons, a 'DHCP mode' dropdown set to 'disable', and input fields for 'Interface VLAN' (2), 'VoIP pbit' (7), 'VoIP IP address' (192.168.2.1), 'VoIP IP mask' (24), and 'Default gateway' (192.168.2.254). Below these fields are 'Apply', 'Cancel', and 'Refresh' buttons. The second section contains three input fields for 'First DNS server', 'Second DNS server', and 'Third DNS server', all set to '0.0.0.0', with 'Apply' and 'Cancel' buttons at the bottom.

The following table describes the labels in this screen.

Table 184 VoIP > IP Setup > VoIP interface

LABEL	DESCRIPTION
DHCP Operation	Specify the DHCP operations on the VoIP interface. release : release the dynamic IP address renew : renew the dynamic IP address
DHCP mode	Select the DHCP status (enable or disable) on the VoIP interface.

Table 184 VoIP > IP Setup > VoIP interface (continued)

LABEL	DESCRIPTION
Interface VLAN	Specify the VLAN ID of the VoIP interface.
VoIP pbit	Specify the priority bit of the VoIP interface.
VoIP IP address	Specify the IP address of the VoIP interface.
VoIP IP mask	Specify the IP subnet mask of the VoIP interface.
Default gateway	Specify the default gateway of the VoIP interface.
Apply	Click Apply to save the changes in this screen.
Cancel	Click Cancel to start configuring the screen again.
Refresh	Click Refresh to update this screen.
First/ Second/ Third DNS server	Specify the first/second/third DNS server address that the VoIP interface uses.
Apply	Click Apply to save the changes in this screen.
Cancel	Click Cancel to start configuring the screen again.

18.3.2 RTP Interface Screen

Click **VoIP > IP Setup > RTP Interface** to configure settings for the RTP interface managed by the IES.

Figure 237 VoIP > IP Setup > RTP interface

The screenshot displays the 'VoIP IP Setup' configuration page, specifically the 'RTP interface' tab. The page includes a 'VoIP IP Setup' header and two tabs: 'VoIP interface' and 'RTP interface'. The 'RTP interface' tab is active, showing the following configuration fields:

- DHCP Operation:** Includes 'Release' and 'Renew' buttons.
- DHCP mode:** A dropdown menu set to 'disable'.
- Interface VLAN:** A text input field containing '2', with a range indicator '[1 ~ 4093]'.
- RTP pbit:** A text input field containing '7', with a range indicator '[0 ~ 7]'.
- RTP IP address:** A text input field containing '192.168.2.1'.
- RTP IP mask:** A text input field containing '24', with a range indicator '[1 ~ 30]'.
- Default gateway:** A text input field containing '192.168.2.254'.

At the bottom of the form, there are three buttons: 'Apply', 'Cancel', and 'Refresh'.

The following table describes the labels in this screen.

Table 185 VoIP > IP Setup > RTP Interface

LABEL	DESCRIPTION
DHCP Operation	Specify the DHCP operations on the RTP interface. release : release the dynamic IP address renew : renew the dynamic IP address
DHCP mode	Select the DHCP status (enable or disable) on the RTP interface.
Interface VLAN	Specify the VLAN ID of the RTP interface.
RTP pbit	Specify the priority bit of the RTP interface.
RTP IP address	Specify the IP address of the RTP interface.
RTP IP mask	Specify the IP subnet mask of the RTP interface.
Default gateway	Specify the default gateway of the RTP interface.
Apply	Click Apply to save the changes in this screen.
Cancel	Click Cancel to start configuring the screen again.
Refresh	Click Refresh to update this screen.

18.4 VoIP Key Pattern Screen

This is available when using SIP firmware. Click **VoIP > Key Pattern** to configure key pattern profiles. A key pattern profile is a set of telephone key-presses that allow users to access a variety of features such as call hold, call transfer, and so on.

Note: Before a user can access a feature, you must enable it in the SIP call service profile (see [Section 13.11 on page 200](#)).

Figure 238 VoIP > Key Pattern

Key Pattern Setup

Name

Service Type Pattern

clir

dndoff

dndon

Index	Name	Select
1	DEFVAL	☐
2	test	☐

The following table describes the labels in this screen.

Table 186 VoIP > Key Pattern

LABEL	DESCRIPTION
Name	Enter a name for this key pattern profile (up to 31 ASCII characters; spaces are not allowed).
Service Type	These fields control the telephone keys a user presses to access a particular service. Characters are limited to the numerals 0~9, the pound (#) and asterisk (*).
clir	Enter the sequence of keys the user presses to restrict his/her phone number by not sending caller ID information (1~7 characters).
dndoff	Enter the sequence of keys the user presses to turn off Do Not Disturb (1~7 characters).
dndon	Enter the sequence of keys the user presses to turn on Do Not Disturb (1~7 characters).
Apply	Click Apply to save the changes in this screen.
New	While you are modifying a profile, you can click New to start configuring a fresh profile without saving your changes.
Index	This is an incremental number indicating the order in which the profiles were created.
Name	This is the name of the profile.
Select	Select the profile you wish to modify or delete.
Modify	Select a profile and click this to edit its configuration.
Delete	Select a profile and click this to delete the profile. Once deleted, information cannot be retrieved.

18.5 VoIP Line Info Screen

This is available when using SIP firmware. Click **VoIP > Line Info** to view detailed VoIP port statistics.

Figure 239 VoIP > Line Info

Line Information

Slot **2** Port **1** **Load**

sipLocalUri	sip:@0.0.0.0
sipRemoteUri	
rtpTxCodecType	
rtpRxCodecType	
rtpTxPayloadType	0
rtpRxPayloadType	0
rtpLocalIp	0.0.0.0
rtpRemoteIp	0.0.0.0
rtpLocalPort	0
rtpRemotePort	0

Refresh

The following table describes labels in this example.

Table 187 VoIP > Line Info

LABEL	DESCRIPTION
Slot, Port	Use the drop-down list boxes to select a port on a VOP line card.
Load	Click Load to display the port's detailed statistics.
sipLocalUri	This is the Universal Resource Indicator of the port. If a local URI is "aaa@bbb", "aaa" is the telephone number configured for the port, and "bbb" is the domain name of the SIP server.
sipRemoteUri	This shows the URI of the remote VoIP device (the person at the other end of the line).
rtpTxCodecType	This shows the voice codec used for transmitting data.
rtpRxCodecType	This shows the voice codec used for receiving data.
rtpTxPayloadType	This shows the voice codec currently used for transmitting voice on this port. The supported codecs can be configured in each DSP profile. The value displayed here depends on the result of the codec negotiation between the system and the remote VoIP device. Possible values are: G711a: 0 G711µ: 8 G723: 4 G729: 18 T.38: 32 G726-16: 96 G726-24: 97 G726-32: 98 G726-40: 99
rtpRxPayloadType	This shows the voice codec currently used for receiving voice on this port. The supported codecs can be configured in each DSP profile. The value displayed here depends on the result of the codec negotiation between the system and the remote VoIP device. Possible values are: G711a: 0 G711µ: 8 G723: 4 G729: 18 T.38: 32 G726-16: 96 G726-24: 97 G726-32: 98 G726-40: 99
rtpLocalIp	This is the local IP address.
rtpRemoteIp	This is the remote IP address.
rtpLocalPort	This is the local port used for SIP.

Table 187 VoIP > Line Info (continued)

LABEL	DESCRIPTION
rtpRemotePort	This is the port on the remote device used for SIP.
Refresh	Click this to update the information in this screen.

18.6 POTS Ring Screen

This is available when using SIP firmware. Click **VoIP > POTS > Ring** to set the SIP POTS ring patterns.

Figure 240 VoIP > POTS > Ring

on/off time : 100 ~ 10000 ms or 65535 indicate continuous time

Index	DEFVAL	Name	DEFVAL	on1	off1	on2	off2	on3	off3
1	☒	ETSI-dr1	☒	1000	4000				
2	☒	ETSI-dr2	☒	1000	500	1000	3500	1000	3500
3	☒	ETSI-dr3	☒	500	500	500	500	1000	3000
4	☒	ETSI-dr4	☒	500	500	1000	500	500	3000
5	☒	ETSI-dr5	☒	1000	500	500	4000		
6	☒	ETSI-dr6	☒	1000	4000				
7	☒	ETSI-dr7	☒	1000	4000				
8	☒	ETSI-dr8	☒	1000	4000				
9	☒	ETSI-dr9	☒	1000	4000				
10	☒	ETSI-dr10	☒	1000	4000				
11	☒	ETSI-dr11	☒	1000	4000				
12	☒	ETSI-dr12	☒	1000	4000				
13	☒	ETSI-dr13	☒	1000	4000				
14	☒	ETSI-dr14	☒	1000	4000				
15	☒	ETSI-dr15	☒	1000	4000				
16	☒	ETSI-dr16	☒	1000	4000				

Apply Cancel

The following table describes the labels in this screen.

Table 188 VoIP > POTS > Ring

LABEL	DESCRIPTION
Index	These are the numbers of the ring patterns.
DEFVAL	Select this to use the default ring pattern name. Clear it to be able to edit the ring pattern name.
Name	This is the name of the ring pattern. Clear the DEFVAL option to be able to configure this using 1-31 printable characters.
DEFVAL	Select this to use the default ring pattern. Clear it to be able to edit the ring pattern.
on1	This is the duration of the first ring (in milliseconds). Clear the DEFVAL option to be able to configure this as 100-10000 milliseconds. Or use 65535 to set a continuous time and have the IES ignore the following parameters.
off1	This is the length of time between the first and second ring (in milliseconds). Clear the DEFVAL option to be able to configure this as 100-10000 milliseconds. Or use 65535 to set a continuous time and have the IES ignore the following parameters.

Table 188 VoIP > POTS > Ring (continued)

LABEL	DESCRIPTION
on2	This is the duration of the second ring (in milliseconds). Clear the DEFVAL option to be able to configure this as 100-10000 milliseconds. Or use 65535 to set a continuous time and have the IES ignore the following parameters.
off2	This is the length of time between the second and third ring (in milliseconds). Clear the DEFVAL option to be able to configure this as 100-10000 milliseconds. Or use 65535 to set a continuous time and have the IES ignore the following parameters.
on3	This is the duration of the third ring (in milliseconds). Clear the DEFVAL option to be able to configure this as 100-10000 milliseconds. Or use 65535 to set a continuous time and have the IES ignore the following parameters.
off3	This is the wait time after the third ring before the first ring is sent again (in milliseconds). Clear the DEFVAL option to be able to configure this as 100-10000 milliseconds. Or use 65535 to set a continuous time and have the IES ignore the following parameters.
Apply	Click Apply to save the changes in this screen.
Cancel	Click Cancel to begin configuring the screen again.

18.7 POTS Flash Screen

Click **VoIP > POTS > Flash** to open the following screen. Use this screen to set how long (in milliseconds) a user has to press the flash key for the IES to register its use. DEFVAL uses the period defined in the country code setting.

Figure 241 VoIP > POTS > Flash

The following table describes the labels in this screen.

Table 189 VoIP > POTS > Flash

LABEL	DESCRIPTION
DEFVAL	Select this to use the flash period defined in the country code setting.
Minimum Time	If you cleared the DEFVAL option, use this field to specify a minimum number of milliseconds that the flash key has to be pressed. You can use 20~1500. Note: Setting the minimum to less than 80 ms disables flash key pulse detection.
Maximum Time	If you cleared the DEFVAL option, use this field to specify a maximum number of milliseconds for the flash key to be pressed. The valid range is from the number specified as the minimum, up to 1500.
DEFVAL	Select this to use the off time period defined in the country code setting.

Table 189 VoIP > POTS > Flash

LABEL	DESCRIPTION
Off Hook Time	Specify the off-hook detection time threshold.
Apply	Click Apply to save the changes in this screen.
Cancel	Click Cancel to begin configuring the screen again.

CHAPTER 19

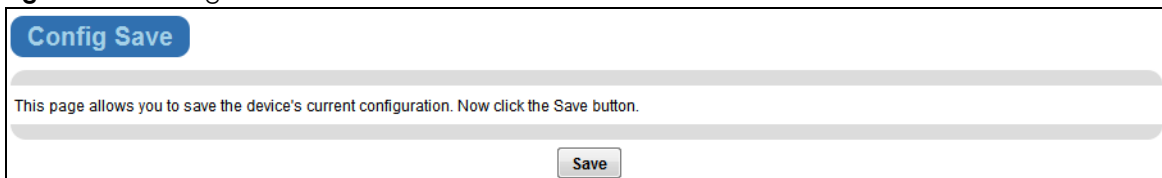
Config Save

Use this section to save changes to your system's configuration.

19.1 The Config Save Screen

Use this screen to save all configuration changes on to your IES's flash memory. If you do not use this screen, any changes you have made to the system's configuration will be lost once the IES is shut down.

Figure 242 Config Save



The following table describes the labels in this screen.

Table 190 Config Save

LABEL	DESCRIPTION
Save	Click Save to save your changes to non-volatile memory when you are done configuring. Otherwise system configuration changes will be lost if the IES is turned off or loses power.

PART III

Commands

CHAPTER 20

The CLI

This chapter introduces the command line interface (CLI).

20.1 Accessing the CLI

Use any of the following methods to access the CLI.

20.1.1 Console Port

- 1 Connect your computer to the console port on the IES using the appropriate cable.
- 2 Use terminal emulation software with the following settings:

Table 191 Default Settings for the Console Port

SETTING	DEFAULT VALUE
Terminal Emulation	VT100
Baud Rate	115200 bps
Parity	None
Number of Data Bits	8
Number of Stop Bits	1
Flow Control	None

- 3 Press [ENTER] to open the login screen.

20.1.2 Local Access by Telnet

Follow these steps to access the CLI from a computer connected to the **MGMT** port.

- 1 Connect your computer to the **MGMT** port.
- 2 Open a Telnet session to the IES's IP address. If this is your first login, use the default values.

Table 192 Default Out Of Band Management IP Address and Subnet Mask

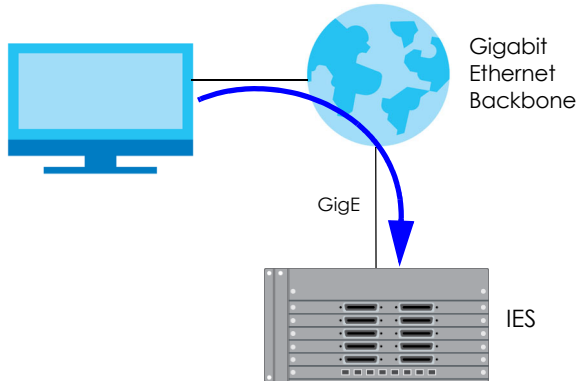
SETTING	DEFAULT VALUE
IP Address	192.168.0.1
Subnet Mask	255.255.255.0

Make sure your computer IP address is in the same subnet, unless you are accessing the IES through one or more routers.

20.1.3 Remote Access by Telnet

Figure 243 Follow these steps to access the CLI from a computer behind a VLAN-aware Ethernet switch on the active Gigabit Ethernet backbone network.

Figure 244 Remote Telnet



- 1 Configure the computer's IP address and subnet mask as 192.168.1.100 and 255.255.255.0.
- 2 Open a Telnet session to the IES's IP address.

Table 193 Default in band management IP address and subnet mask

SETTING	DEFAULT VALUE
IP Address	192.168.1.1
Subnet Mask	255.255.255.0

20.2 Logging in

Use the administrator username and password. If this is your first login, use the default values shown in the cover page of this guide.

Note: The IES automatically logs you out of the management interface after five minutes of inactivity. If this happens to you, simply log back in again.

20.3 Using Shortcuts and Getting Help

This table identifies some shortcuts in the CLI, as well as how to get help.

Table 194 CLI Shortcuts and Help

COMMAND / KEYS	DESCRIPTION
history	Displays a list of recently-used commands.
↑↓ (up/down arrow keys)	Scrolls through the list of recently-used commands. You can edit any command or press [ENTER] to run it again.
[CTRL] +Z	Returns to the previous mode. See Section 20.7 on page 309 for more information about modes.

Table 194 CLI Shortcuts and Help (continued)

COMMAND / KEYS	DESCRIPTION
[TAB]	Auto-completes the keyword you are typing if possible. For example, type <code>config</code> , and press [TAB]. The IES finishes the word <code>configure</code> .
?	Displays the keywords and/or input values that are allowed in place of the ?.
help	Displays the (full) commands that are allowed in place of <code>help</code> .

The help generally follows these syntax conventions:

- Each interface refers to a port on the IES.
- Required input values are in angle brackets `<>`; for example, `ping <ip-address>` means that you must specify an IP number for this command.
- Lists (such as `<port-list>`) consist of one or more elements separated by commas. Each element might be a single value (1, 2, 3, ...) or a range of values (1-2, 3-5, ...) separated by a dash. Use an asterisk (*) to indicate all possible elements.
- The | (bar) symbol means “or”.
- Optional fields are in square brackets []; for instance, in `snmp-server [contact <system contact>] [location <system location>]`, the `contact` and `location` fields are optional.
- The `<cr>` means press the [ENTER] key.

20.3.1 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 IES 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 IES displays a list of commands that start with the partial command.

Figure 245 Non-Unique Partial Command Example

```

ras# c [TAB]
clear      configure  copy
ras# co [TAB]
configure  copy

```

20.4 Common Command Notation

The following table describes commonly used command parameter notation.

Table 195 Common Command Notation

NOTATION	DESCRIPTION
[...]	The optional fields in a command are enclosed in square brackets [], for instance, <code>ip ping <ip-address> [<count>]</code> means that the <code>count</code> field is optional.
	The symbol means “or”.
etype	Ethernet type in hexadecimal (0000-FFFF).

Table 195 Common Command Notation

NOTATION	DESCRIPTION
<i>index</i>	This is an integer that sets the index number of a table entry. The range starts at 1. The end of the range varies by command.
<i>ip-address</i>	This represents a valid IP version four address in dotted decimal notation. 192.168.1.1 is an example.
<i>ipv6-address</i>	This represents a valid IP version six address. ::0 ~ ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
<i>mac</i>	This represents a MAC address in a0:c5:12:34:56:78 format. 00:00:00:00:00:00-FF:FF:FF:FF:FF:FF
<i>mask</i>	This represents the bit number of the subnet mask of an IP address. The range is 0 to 32 for IPv4 or 0 to 128 for IPv6. To find the bit number, convert the subnet mask to binary and add all of the 1's together. Take "255.255.255.0" for example. 255 converts to eight 1's in binary. There are three 255's, so add three eights together and you get the bit number (24).
<i>pbit</i>	This is a priority bit (0-7).
<i>port</i>	This represents the UDP or TCP port number of a service.
<i>priority</i>	The VLAN priority setting (0-7).
<i>protocol</i>	An IP protocol 0-255.
<i>slot</i>	This represents the number of an individual chassis slot where a control or line card is located. 1 is the MSC card. 2-5 are the line cards.
<i><slot>/<port></i>	This represents the number of an individual chassis slot where a line card is located and the number of a port. You can specify a single port. <i>slot</i> : 2-5 <i>port</i> : 1-N where N is the number of ports on the line card.
<i>slot/portlist</i>	This specifies DSL ports on a line card in an individual chassis slot (2-5). You can specify individual ports on the cards in different slots, for example 2/1,2/3,3/1,3/3 Use * to specify all of a line card's ports: 2/*,3/1,3/3 You can also include a range of ports: 2/1-2/12
<i>uni-vlan</i>	The VLAN ID on the UNI (User Network Interface) ports, 1-4093.
<i>pvid, vid</i>	This represents a VLAN identifier (VLAN ID). The range is [1.. 4093].
<i>vpi/vci</i>	The VPI (Virtual Path Indicator) and VCI (Virtual Channel Indicator) of an individual PVC (Permanent Virtual Circuit). The VPI setting can be 0 to 255. The VCI setting can be 32 to 65535 if the VPI is 0 or 1 to 65535 if the VPI is not 0.

20.5 Command Summary

The following table describes user-input values available in multiple commands for this feature.

Table 196 Example: user-input Values

COMMAND	DESCRIPTION
<i>vid</i>	1-4093

This section lists the commands for this feature.

Table 197 Example: Command Summary Table

COMMAND	DESCRIPTION	M	P
show vlan	Displays STPID, single VLAN tag mode and all VLAN settings.	E	3
show vlan <vid-list>	Displays the member ports of specified VLANs or all VLANs. <i>vid-list</i> : list of (1-4093), for example 1,3 or 1,3,5-21 or *	E	13
interface ge-nni <portlist>	Configures the specified Gigabit Ethernet uplink ports. You can specify a single port <1>, all ports <*> or a list of ports <1,2>. You can also include a range of ports <1-2>.	C	13
exit	Leaves the Gigabit Ethernet Gigabit Ethernet uplink port configuration.	C	13
vlan <vid>	Adds the Gigabit Ethernet uplink ports to the specified VLAN.	C	13
no vlan <vid>	Removes the Gigabit Ethernet uplink ports from the specified VLAN.	C	13

The **Table** title identifies the specific keywords that the commands share.

The **Command** column shows the syntax of the command. The syntax follows the same conventions the help ([Section 20.3 on page 302](#)) does, in addition to the following.

- *these* terms represent user-input values that are explained in more detail in the **Description** column or in the user-input value table.
- If a command is indented, users have to run it in one of the config- modes. You can identify the specific mode by looking at the last config-mode command above it.
- If a command is not indented, users have to run it in enable or config mode.

The **Description** column explains what the command does. It also identifies legal input values for user-input values, if necessary.

The **M** column helps identify the mode in which users have to run the command.

- **E**: The command is available in enable mode. It is also available in user mode if the level (**P**) is less than 13.
- **C**: The command is available in config (not indented) or one of the config- (indented) modes.

The **P** column identifies the level of the command.

20.6 Privilege Levels, Accounts and Passwords

Every command has a level (0-14). Users can run a command if the session's level is greater than or equal to the command's level. The session's level initially comes from the login account's level, though it is possible to change the session's level after logging in.

The following table summarizes the types of commands at each of these levels.

Table 198 Types of Commands at Different Levels

LEVEL	TYPES OF COMMANDS AT THIS LEVEL
0	Ping, IPv6, enable, and logout.
1	Display basic system information.
3	Display configuration or status.

Table 198 Types of Commands at Different Levels (continued)

LEVEL	TYPES OF COMMANDS AT THIS LEVEL
13	Configure features except for login accounts, login precedence, multiple logins, and administrator and enable passwords.
14	Configure login accounts, login precedence, multiple logins, and administrator and enable passwords.

The following table describes commonly used parameter notation for these commands.

Table 199 Login Account and Password Command Parameters

NOTATION	DESCRIPTION
<i>name</i>	1- 31 alphanumeric characters
<i>password</i>	Up to 31 printable characters.
<i>privilege</i>	The user privilege level. 1-14

This table summarizes the commands that manage passwords and the Privilege Levels for login accounts.

Table 200 Login Account and Password Commands Summary

COMMAND	DESCRIPTION	M	P
show logins	Displays local account information.	E	13
show logins online	Displays session information for the currently logged in users.	E	13
logins username <name> password <password>	Creates an account with the specified user name and sets the password. <i>name</i> : 1- 31 alphanumeric characters <i>password</i> : up to 31 printable characters	C	14
logins username <name> privilege <privilege>	Assigns a privilege level to the specified account. The privilege level is applied the next time the user logs in.	C	14
no logins username <name>	Removes the specified account.	C	14
show user online	Displays the online user' information.	E	3
admin-password <password> <confirm-string>	Changes the administrator password. The password and confirmation string must be exactly the same. <i>password</i> : Up to 31 printable characters. <i>confirm-string</i> : Type the password again for confirmation purpose.	C	14
password <password>	Changes the enable password of the highest privilege (enable) mode. <i>password</i> : Up to 31 printable characters.	C	14
password <password> privilege <privilege>	Sets the enable password of the specified privilege (enable) mode. Each command has a privilege level. A user can only use commands with privilege levels equal to or lower than his current privilege (enable) mode. <i>password</i> : Up to 31 printable characters. <i>privilege</i> : 1 - 14	C	14
no password privilege <privilege>	Removes the privilege (enable) mode password setting for the specified privilege level. <i>privilege</i> : 1 - 14	C	14

Table 200 Login Account and Password Commands Summary (continued)

COMMAND	DESCRIPTION	M	P
<code>privilege mode config exec command <command> level <level></code>	Configures the privilege level required for the specified command tree. config: The specific command tree is in configuration mode. exec: The specific command tree is in execution mode. <i>command</i> : The command syntax, use '*' for parameters and add quotes if it contains any spaces. <i>level</i> : 1-13	C	14
<code>no privilege</code>	Removes all command privilege configurations.	C	14

20.6.1 Command Example

This example creates a user account **tom** with a password of **0123**. The privilege level is set to 5. Then it displays all user accounts on your IES.

```

ras# config
ras(config)# logins username tom password 0123
ras(config)# logins username tom privilege 5
ras(config)# exit
ras# show logins
index status name                privilege
-----
  1    V    admin                14
  2    V    tom                  5
ras#

```

This example sets the password of enable mode to **ies7** and enable local database for user authentication. The administrator logs out and then logs in to a user account (for example, **tom**) for testing whether the enable password works.

```

ras# config
ras(config)# password ies7
ras(config)# aaa authentication enable local
ras(config)# exit
ras# exit

User name: tom

Password: ****

ras# enable
Password:
ras#

```

20.6.2 Privilege Levels for Login Accounts

Login accounts can be configured by the **admin** account or any login account with a level of 14. The **admin** account has a level of 14, so the administrator can run every command. You cannot change the privilege level of the **admin** account.

20.6.3 Privilege Levels for Sessions

The session's privilege level initially comes from the privilege level of the login account the user used to log in to the IES. After logging in, the user can use the following commands to change the session's privilege level.

20.6.3.1 enable Command

This command raises the session's privilege level to 14. It also changes the session to enable mode, if necessary. This command is available in user mode or enable mode. The IES does not have the default password for the enable mode, you have to set a password for it first.

The following command sets the enable password to **123456**.

```
ras# config
ras(config)# password 123456
ras(config)#
```

In the following example, the login user account has a privilege level of 0 but knows that the highest level of enable password is **123456**. Afterwards, the session's privilege level is 14, instead of 0, and the session changes to enable mode.

```
ras# enable
Password: 123456
ras#
```

20.6.3.2 Password Privilege Command

Use the following command to create passwords for specific privilege levels.

```
password <password> <1-14>
```

The following command sets the password for privilege level 13 to **pswd13**.

```
ras(config)# password pswd13 privilege 13
```

20.6.3.3 Enable <0-14> Command

This command raises the session's privilege level to the specified level. It also changes the session to enable mode, if the specified level is 13 or 14. This command is available in user mode or enable mode, and users have to know the password for the specified privilege level.

In the following example, the login user account has a privilege level of 0 but knows that the password for privilege level 13 is **pswd13**. Afterwards, the session's privilege level is 13, instead of 0, and the session changes to enable mode.

```
ras# enable 13
Password: pswd13
ras#
```


20.6.3.4 Disable Command

This command reduces the session's privilege level to 0. It also changes the session to user mode. This command is available in enable mode. In the following example, user **tom** changes his session privilege to 14 and then changes the privilege again to 0.

```
User name: tom

Password: *****
ras# enable 14
Password:
ras# disable
ras>
```

20.7 Command Modes

The CLI is divided into modes. Certain commands are available in certain command modes. The modes that are available depend on the session's privilege level.

20.7.1 Modes for Privilege Levels 0-12

If the session's privilege level is 0-12, the user and all of the commands are in user mode. Users do not have to change modes to run any allowed commands.

20.7.2 Modes for Privilege Levels 13-14

If the session's privilege level is 13-14, the allowed commands are in one of these modes.

Table 201 Command Modes for Privilege Levels 13-14

MODE	PROMPT	DESCRIPTION
enable	ras#	Displays current configuration, diagnostics, maintenance.
configuration	ras(config)#	Configures features other than those below.

Each command is usually in one mode. To run a particular command, you have to change to the appropriate mode. The command modes are organized like a tree, and you start at the root of the tree in enable mode. Here are some examples of how to change modes.

Table 202 Changing Between Command Modes for Privilege Levels 13-14

MODE	ENTER MODE	LEAVE MODE
enable	exit (while in configuration mode)	exit (logs you out)
configuration	configure (while in enable mode)	exit (takes you to enable mode)
DSL interface sub-commands	interface dsl <slot/portlist> (while in enable mode)	exit (takes you to configuration mode)

20.8 Dual Image Files

The IES supports dual firmware images. You can store up to two firmware files (of the same device model) on the IES. Only one firmware is used at a time. This allows immediate rollback on system boot up in case the current firmware is corrupt. By default, the switch uses firmware ras-0 while the second firmware file is named ras-1. See [Section 22.7 on page 328](#) for commands for managing firmware and for how to use FTP to upload firmware to the IES.

20.9 Dual Configuration Files

The IES also supports dual configuration files.

20.10 Saving Your Configuration

When you run a command, the IES saves any changes to its run-time memory. The IES loses these changes if it is turned off or loses power. Use the `write memory` command in enable mode to save the current configuration permanently to non-volatile memory.

```
ras# write memory
```

Note: You should save your changes after each CLI session. All unsaved configuration changes are lost once you restart the IES.

20.11 Logging Out

Enter the `exit` command in configure mode to go to mode.

Enter the `exit` command in enable mode to log out of the CLI. See [Section 20.7 on page 309](#) for more information about modes.

CHAPTER 21

Initial Setup

This chapter identifies tasks you might want to do when you first configure the IES.

21.1 Changing the Administrator Password

Note: It is recommended you change the default administrator password.

Use this command to change the administrator password.

```
admin-password <password> <confirm-password>
```

where <password> and <confirm-password> may be 1-32 alphanumeric characters long.

```
ras# configure
ras(config)# admin-password t1g2y7i9 t1g2y7i9
```

21.2 Changing the Enable Password

Note: It is recommended you change the default enable password.

Use this command to change the enable password.

```
password <password>
```

where <password> may be 1-32 alphanumeric characters long.

```
ras# configure
ras(config)# password k8s8s3dl0
```

21.3 Changing the Management IP Address

This command changes the management IP address for remote access.

```
ip inband address <ip-address>/<mask>
```

or this command changes the management IP address for local access.

```
ip outband address <ip-address>/<mask>
```

The *mask* is a number from 1 to 31.

This example changes the inband management IP address to 172.1.1.10 with subnet mask 255.255.255.0 (/24).

```
ras# configure
ras(config)# ip inband address 172.1.1.10 24
```

This example changes the out-of-band management IP address (for local access) to 172.1.1.10 with subnet mask 255.255.255.0.

```
ras# configure
ras(config)# ip outband address 172.1.1.10/24
```

Note: Afterwards, you have to use the new IP address to access the IES.

21.4 Changing the Management VLAN

This command changes the inband management VLAN IP.

```
ip inband mgmt-vlan <mgmt-vid>
```

Note: After the following example configuration, you must connect through a VLAN aware device using the proper VLAN ID in order to perform management.

This example sets the VLAN ID 3 for managing the system (the "management" or "CPU" VLAN).

```
ip inband mgmt-vlan 3
```

Note: Remote access could be affected.

21.5 Looking at Basic System Information

Here is how to display general system information about the IES.

```
ras# show system-information
      Hostname: a\n
      Location:
      Contact:
      Model: IES4105
      NNI Type: MSC1002GA
      ZyNOS version: V3.60 (ABIZ.0)b2 | 02/23/2017
      F/W size: 7347350
      MAC address: 00:13:49:AB:CD:12
      System up time: 0(days) : 22:07:21
      Bootbase version: V1.01 | 02/23/2017
      F/W build date: Jun 06 2016 16:22:45
      Hardware version:
      Serial number:
      Console baudrate: 115200 bps
      Power source: AC
      Power Module: Dual and Charge
```

21.6 Looking at the Operating Configuration

Use this command to look at the current operating configuration.

```
show running-config
```

This is illustrated in the following example.

```
ras# show running-config page
Building configuration...

Current configuration:

!Last configuration change at 12:39:28 Thu Feb 05 2037 by admin with
telnet (172.23.44.56)

logins username admin password
d4:88:dd:79:63:7c:78:11:87:92:cb:3b:c5:41:0c:21:c6:ca:ad:9a:db:90:1c:14:7c:85:46:
38:dd:19:df:db
logins username admin privilege 14
fe alarm-profile DEFVAL
exit
fe alarm-profile test-FE
exit
ge-nni alarm-profile DEFVAL
exit
ge-nni alarm-profile Test-Enet
exit
dsl line-profile test
exit
dsl alarm-profile DEFVAL
exit
dsl gbond group test
    portList 3/1,3/2
    protocol 0
exit
dsl gbond group test2
    portList 3/12,3/13
    protocol 0
exit
-- more --, next page: Space, continue: c, quit: ESC
```

21.7 Provisioning Slots

IES will detect the line card type automatically. However, a slot can be configured before a real line card is plugged in. You must configure a line card slot for appropriate type of line card before you can pre-configure the line card. Please note if a different type of line card is plugged in, all saved/pre-configured settings will be reset.

CHAPTER 22

Management

Configure the time and alarms; monitor the hardware, configure IP addresses and subnet masks; copy, erase, and display settings; configure SNMP; use FTP; configure the hostname, contact, and location settings; and set the console port's baud rate.

22.1 Alarm Commands

Use these commands to manage alarms on the IES. You can show current and historical alarms, configure alarm definitions, clear alarms, set up alarm notification severity levels for DSL and VoIP ports, and configure descriptions for the alarm inputs.

The following table describes commonly used `alarm` command parameter notation.

Table 203 Alarm Command Parameters

NOTATION	DESCRIPTION
<i>alarm</i>	A category of alarms. eqpt represents equipment alarms. dsl represents Digital Subscriber Line (DSL) alarms. enet represents Ethernet alarms. fe represents Fast Ethernet alarms. sys represents system alarms. voip represents VoIP alarms. Check the alarm definition table for allowed alarms.
<i>severity</i>	Specifies an alarm severity level (critical, major, minor, or warning).
<i>condition</i>	Specifies an alarm condition. <i>condition</i> Checks the alarm definition table for allowed conditions.
<i>month</i>	Specifies the month (1-12) in MM format.
<i>day</i>	Specifies the day (1-31) in DD format.
<i>year</i>	Specifies the year (1970-2037) in YYYY format.
<i>target</i>	Specifies where to send the alarm. snmp syslog all none 'none' disables alarm reports on this alarm condition.
<i>forward</i> <i>reverse</i>	Specifies the displaying order. forward: oldest entry displayed first reverse: latest entry displayed first
<i>detail</i>	Displays more comprehensive alarm condition descriptions.

This table describes the commands.

Table 204 Alarm Commands Summary

COMMAND	DESCRIPTION	M	P
show alarm current [severity <severity>] [alarm <alarm>] [condition <condition>] [start-date <month>/<day>/<year>] [end-date <month>/<day>/<year>] [forward reverse] [detail] [indexes]	Displays current alarms. indexes displays alarm indexes information	E	1
clear alarm current [condition <condition>] indexes <index1>/<index2>/<index3>]	Clears all clearable current alarms or alarms with the specified condition code and indexes <i>condition</i> : check for alarm definition table for allowed condition <i>index1</i> : target alarm index1, check for indexes of alarm current table <i>index2</i> : target alarm index2, check for indexes of alarm current table <i>index3</i> : target alarm index3, check for indexes of alarm current table	E	13
show alarm history [severity <severity>] [alarm <alarm>] [condition <condition>] [start-date <month>/<day>/<year>] [end-date <month>/<day>/<year>] [forward reverse] [detail]	Displays alarm history.	E	1
clear alarm history [severity <severity>] [alarm <alarm>] [condition <condition>]	Clears historical alarms with the specified severity or specified alarm or specified condition or all severities.	E	13
alarm definition alarm <alarm> condition <condition> severity <severity> [syslog-facility <facility>] [target <target>] [clearable]	Configures the specified alarm definition. <i>condition</i> : check the alarm definition table for allowed conditions or condition codes clearable: alarm is clearable	C	13
show alarm definition [alarm <alarm>] [condition <condition>] [severity <severity>] [target <target>]	Displays the alarm definition table.	E	1
show interface dsl <slot/portlist> alarm notification-severity	Displays the minimum severity level to send out alarm notifications (SNMP trap and SYSLOG) on the specified DSL ports.	E	1
interface dsl <slot/portlist>	Enters the sub-command mode for configuring the specified DSL ports.	C	13
exit	Leaves the DSL port configuration.	C	13
alarm notification-severity <severity>	Configures the minimum severity level for sending out alarm notifications (SNMP trap and SYSLOG) about the specified ports.	C	13
show interface voip <slot/portlist> alarm notification-severity	Displays the minimum severity level to send out alarm notifications (SNMP trap and SYSLOG) on the specified VoIP ports.	E	1
interface voip <slot/portlist>	Enters the sub-command mode for configuring the specified VoIP ports.	C	13
exit	Leaves the VoIP port configuration sub-command mode.	C	13
alarm notification-severity <severity>	Configures the minimum severity level for sending out alarm notifications (SNMP trap and SYSLOG).	C	13

Table 204 Alarm Commands Summary (continued)

COMMAND	DESCRIPTION	M	P
<code>show interface fe <slot/portlist> alarm notification-severity</code>	Displays the minimum severity level to send out alarm notifications (SNMP trap and SYSLOG) on the specified FE ports.	E	1
<code>interface fe <slot/portlist></code>	Enters the sub-command mode for configuring the specified FE ports.	C	13
<code>exit</code>	Leaves the FE port configuration sub-command mode.	C	13
<code>alarm notification-severity <severity></code>	Configures the minimum severity level for sending out alarm notifications (SNMP trap and SYSLOG).	C	13
<code>show interface ge <port> alarm notification-severity</code>	Displays the minimum severity level to send out alarm notifications (SNMP trap and SYSLOG) on the specified Gigabit Ethernet uplink interfaces. You can specify a single port <1>, all ports <*> or a list of ports <1,2>. You can also include a range of ports <1-2>.	E	1
<code>interface ge-nni <portlist></code>	Configures the specified Gigabit Ethernet uplink ports. You can specify a single port <1>, all ports <*> or a list of ports <1,2>. You can also include a range of ports <1-2>.	C	13
<code>exit</code>	Leaves the Gigabit Ethernet uplink port configuration.	C	13
<code>alarm notification-severity <severity></code>	Configures the minimum severity level for sending out alarm notifications (SNMP trap and SYSLOG).	C	13
<code>show interface system alarm</code>	Displays the system-wide alarm settings.	E	1
<code>interface system</code>	Enters the sub-command mode for configuring system-wide settings.	C	13
<code>exit</code>	Leaves the system-wide settings sub-command mode.	C	13
<code>alarm notification-severity <severity></code>	Configures the minimum severity level for sending out alarm notifications (SNMP trap and SYSLOG).	C	13
<code>alarm alarm-input <index> description <description></code>	Configures the alarm input description. <i>index</i> : 1-7 <i>description</i> : up to 31 printable characters	C	13
<code>no alarm alarm-input <index></code>	Loads the default alarm input description.	C	13
<code>show alarm alarm-input</code>	Displays the alarm input descriptions.	E	1
<code>alarm sys-suppress</code>	Enables alarm system suppression. This suppresses all traps except those with the "event" severity level. The IES still records all alarms and syslog (if enabled).	C	13
<code>no alarm sys-suppress</code>	Disables alarm system suppression.	C	13
<code>show alarm sys-suppress</code>	Displays the alarm system suppression setting.	E	1

Table 204 Alarm Commands Summary (continued)

COMMAND	DESCRIPTION	M	P
alarm coa issue-threshold <issue-threshold>	Configures the threshold for issuing an CPU overload alarm. <i>issue-threshold</i> : percent of CPU usage. 0 ~ 100. Set the CPU overload alarm issue threshold higher than the CPU overload alarm clear threshold.	C	13
alarm coa clear-threshold <clear-threshold>	Configures the threshold for clearing an CPU overload alarm. <i>clear-threshold</i> : percent of CPU usage. 0 ~ 100. Set the CPU overload alarm clear threshold lower than CPU overload alarm issue threshold.	C	13
alarm coa sample-seconds <seconds>	Configures the number of sample seconds used for monitoring for a CPU overload. <i>seconds</i> : 1 ~ 60	C	13
alarm coa analytic-method continuous average	Configures the method of analyzing CPU usage in monitoring for a CPU overload. <i>continuous</i> : issue a CPU overload alarm if all samples are above <issue-threshold>. Clear the CPU overload alarm if all samples are below <clear-threshold>. <i>average</i> : issue a CPU overload alarm if the average of all samples is above <issue-threshold>. Clear the CPU overload alarm if the average of all samples is below <clear-threshold>.	C	13
show alarm coa	Displays the CPU overload alarm related settings.	E	1

22.2 Date and Time Commands

Use these commands to configure the date and time settings. Besides setting the current system time and date, you can also configure daylight savings time, and the time server to use.

The following table describes commonly used parameter notation for these commands.

Table 205 Date and Time Command Parameters

NOTATION	DESCRIPTION
<i>hour</i>	Specifies the hour (0-23) in HH format.
<i>min</i>	Specifies the minute (0-59) in MM format.
<i>sec</i>	Specifies the second (0-59) in SS format.
<i>month</i>	Specifies the month (1-12) in MM format.
<i>day</i>	Specifies the day (1-31) in DD format.
<i>year</i>	Specifies the year (1970-2037) in YYYY format.

This table describes the commands.

Table 206 Date and Time Commands Summary

COMMAND	DESCRIPTION	M	P
show time	Displays the current system time and date.	E	1
time <hour>:<min>:<sec>	Sets the current system time.	C	13
time date <month>/<day>/<year>	Sets the current system date.	C	13
time server timezone <time-zone>	Selects the time difference between UTC (formerly known as GMT) and your time zone. <i>time-zone</i> : -1200-1400 in steps of 15 minutes	C	13
time daylight-saving-time	Enables daylight saving time. The current time is updated if daylight saving time has started.	C	13
no time daylight-saving-time	Disables daylight saving time.	C	13
time daylight-saving-time startdate <week> <day> <month> <o'clock>	Sets the day and time when Daylight Saving Time starts. In most parts of the United States, Daylight Saving Time starts on the second Sunday of March at 2 A.M. local time. In the European Union, Daylight Saving Time starts on the last Sunday of March at 1 A.M. GMT or UTC, so the o'clock field depends on your time zone.	C	13
time daylight-saving-time end-date <week> <day> <month> <o'clock>	Sets the day and time when Daylight Saving Time ends. In most parts of the United States, Daylight Saving Time ends on the first Sunday of November at 2 A.M. local time. In the European Union, Daylight Saving Time ends on the last Sunday of October at 1 A.M. GMT or UTC, so the o'clock field depends on your time zone.	C	13
show time server	Displays the time server settings.	E	1
time server	Has the system synchronize its time with the time server every 24 hours.	C	13
no time server	Disables synchronizing the system time with the time server.	C	13
time server type <daytime time ntp>	Sets the time server type. <i>daytime</i> : Daytime Protocol (RFC 867) <i>time</i> : Time Protocol (RFC 868) <i>ntp</i> : SNTP (RFC 2030)	C	13
time server address <ip-address> <ipv6-address>	Sets the IP address of the time server in IPv4 or IPv6 format. <i>ip-address</i> : 0.0.0.0 ~ 223.255.255.255 <i>ipv6-address</i> : 2000:: ~ 3fff:ffff:ffff:ffff:ffff:ffff:ffff:ffff	C	13
time server sync	Synchronize the current system time with time server.	C	13

22.3 Hardware Monitor Commands

Use these commands to view hardware monitor statistics and set hardware monitoring alarm limits. You can set maximum and minimum allowed speeds for individual fans, maximum and minimum allowed temperatures and voltages for individual sensors in the management card and line cards.

This table describes the commands.

Table 207 Hardware Monitor Commands Summary

COMMAND	DESCRIPTION	M	P
<code>show hw-monitor</code>	Displays the system monitor settings.	E	1
<code>show hw-monitor battery-saving</code>	Displays the battery saving configuration.	E	1
<code>show hw-monitor statistics [slot <slot>]</code>	Displays the system monitor statistics summary. <i>slot</i> : 1-5, 1 is the control card. 2-5 are the line cards.	E	1
<code>hw-monitor fan-speed-threshold <index> <high> <low></code>	Sets the high and low fan speed limits for raising an alarm on the specified fan. <i>index</i> : 1-3 <i>high</i> : 0-15000 in RPM <i>low</i> : 0-15000 in RPM	C	13
<code>hw-monitor temperature-threshold <slot> <index> <high> <low></code>	Sets the high and low temperature limits for raising an alarm on the specified module and sensor. <i>slot</i> : 1-5, 1 is the control card. 2-5 are the line cards. <i>index</i> : 1-10 <i>high</i> : -50-120 in degree Celsius <i>low</i> : -50-120 in degree Celsius	C	13
<code>hw-monitor voltage-threshold <slot> <index> <high> <low></code>	Sets the high and low voltage limits for raising an alarm on the specified module and sensor. <i>index</i> : 1-5 <i>high</i> : 0-25000 in mV <i>low</i> : 0-25000 in mV	C	13
<code>hw-monitor battery-saving <input1 input2 input3 input4></code>	Configures battery saving mode on the specified alarm input. When the specified alarm input is triggered, the IES turns off subscriber data traffic in order to support PSTN calls for as long as possible. See Section 3.6.1 on page 45 for details on the alarm inputs.	C	13
<code>no hw-monitor battery-saving</code>	Restores the battery saving configuration to the default value.	C	13

22.4 Running Configuration Commands

Use these commands to back up and restore configuration and firmware.

This table describes the commands.

Table 208 Running Configuration Commands Summary

COMMAND	DESCRIPTION	M	P
copy running-config interface dsl <slot>/<port> <slot/portlist> [<attribute> [<...>]]	Clones (copies) the attributes from the specified DSL port to other DSL ports. Optionally, copies the specified attributes from one port to other ports. Attributes are: [loopguard] [alarm] [acl] [packet-type] [smcast] [atm_vc] [vlan_transparent] [vlan_trunk] [vlan_trans_n_aggr] [vlan_tls] [qos] [igmp] [vdsl] [dhcp] [fdb] [dscp] [dot1x]	E	13
copy running-config interface fe <slot>/<port> <slot/portlist> [<attribute> [<...>]]	Clones (copies) the attributes from the specified FE port to other FE ports. Optionally, copies the specified attributes from one port to other ports. Attributes are: [loopguard] [alarm] [acl] [packet-type] [smcast] [vlan_transparent] [vlan_trunk] [vlan_trans_n_aggr] [vlan_tls] [qos] [igmp] [fe] [dhcp] [fdb] [dscp] [dot1x]	E	13
copy running-config interface ge-nni <port> <portlist> [<attribute> [<...>]]	Clones (copies) the attributes from the specified GE NNI port to other GE NNI ports. You can specify a single port <1>, all ports <*> or a list of ports <1,2>. You can also include a range of ports <1-2>. Attributes are: [acl] [alarm] [vlan_uplink] [rstp]	E	13
copy running-config interface voip <slot>/<port> <slot/portlist> [<attribute> [<...>]]	Clones (copies) the attributes from the specified VoIP port to other VoIP ports. Optionally, copies the specified attributes from one port to other ports. Attributes are: [alarm] [sip] [dsp] [pots] SIP applies when using SIP firmware.	E	13
erase running-config	Resets the IES to the factory default settings.	E	13
erase running-config interface dsl <slot/portlist> [<attribute> [<...>]]	Resets the specified DSL ports to the factory default settings on a per-port basis and optionally on a per-feature configuration basis. Attributes are: [loopguard] [alarm] [acl] [packet-type] [smcast] [atm_vc] [vlan_transparent] [vlan_trunk] [vlan_trans_n_aggr] [vlan_tls] [qos] [igmp] [vdsl] [dhcp] [fdb] [dscp] [dot1x]	E	13
erase running-config interface fe <slot/portlist> [<attribute> [<...>]]	Resets the specified FE ports to the factory default settings on a per-port basis and optionally on a per-feature configuration basis. Attributes are: [loopguard] [alarm] [acl] [packet-type] [smcast] [vlan_transparent] [vlan_trunk] [vlan_trans_n_aggr] [vlan_tls] [qos] [igmp] [fe] [dhcp] [fdb] [dscp] [dot1x]	E	13
erase running-config interface ge-nni <portlist> [<attribute> [<...>]]	Resets the specified GE NNI ports to the factory default settings on a per-port basis and optionally on a per-feature configuration basis. You can specify a single port <1>, all ports <*> or a list of ports <1,2>. You can also include a range of ports <1-2>. Attributes are: [acl] [alarm] [vlan_uplink] [rstp]	E	13
erase running-config interface voip <slot/portlist> [<attribute> [<...>]]	Resets the specified VoIP ports to the factory default settings on a per-port basis and optionally on a per-feature configuration basis. Attributes are: [alarm] [sip] [dsp] [pots] SIP applies when using SIP firmware.	E	13
erase running-config interface system [<attribute> [<...>]]	Resets the system-wide interface settings to the factory default settings. Attributes are: [acl] [alarm]	E	13

Table 208 Running Configuration Commands Summary (continued)

COMMAND	DESCRIPTION	M	P
show running-config [page]	Displays the current configuration file. This file contains the commands that change the IES's configuration from the default settings to the current configuration. Optionally, displays current operating configuration page by page.	E	13
show running-config interface dsl <slot/portlist> [<attribute> [<...>]]	Displays the current DSL configuration on a port-by-port basis. Attributes are: [loopguard] [alarm] [acl] [packet-type] [smcast] [atm_vc] [vlan_transparent] [vlan_trunk] [vlan_trans_n_aggr] [vlan_tls] [qos] [igmp] [vds1] [dhcp] [fdb] [dscp] [dot1x]	E	13
show running-config interface fe <slot/portlist> [<attribute> [<...>]]	Displays the current FE configuration on a port-by-port basis. Attributes are: [loopguard] [alarm] [acl] [packet-type] [smcast] [vlan_transparent] [vlan_trunk] [vlan_trans_n_aggr] [vlan_tls] [qos] [igmp] [fe] [dhcp] [fdb] [dscp] [dot1x]	E	13
show running-config interface voip <slot/portlist> [<attribute> [<...>]]	Displays the current VoIP configuration on a port-by-port basis. Attributes are: [alarm] [sip] [dsp] [pots] SIP applies when using SIP firmware.	E	13
show running-config interface ge-nni <portlist> [<attribute> [<...>]]	Displays the current GE NNI configuration on a port-by-port basis. You can specify a single port <1>, all ports <*> or a list of ports <1,2>. You can also include a range of ports <1-2>. Attributes are: [acl] [alarm] [vlan_uplink] [rstp]	E	13
show running-config interface system [<attribute> [<...>]]	Displays the current system-wide interface settings. Attributes are: [acl] [alarm]	E	13

22.4.1 Command Examples

This example shows the current configuration of port 1 on slot 2. Then it shows how to copy the port's configuration to port 7 on slot 2. Finally, this example also shows the configuration of port 7.

```
ras# show running-config interface dsl 2/1
Building configuration...

Current configuration:

#SLOT 2 ALC1132A-51

interface dsl 2/1
 active
 loopguard
 loopguard uni-vlan 100
 vlan transparent
exit
ras# copy running-config interface dsl 2/1 2/7
ras# show running-config interface dsl 2/7
Building configuration...

Current configuration:

#SLOT 2 ALC1132A-51

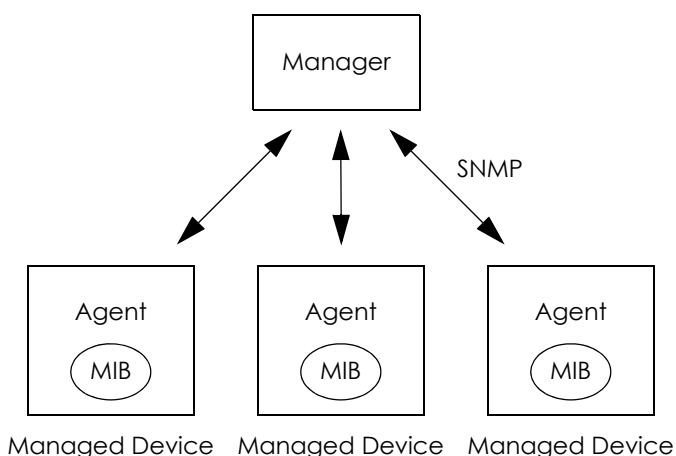
interface dsl 2/7
 active
 loopguard
 loopguard uni-vlan 100
 vlan transparent
exit
ras#
```

22.5 SNMP Server Commands

Use these commands to configure SNMP on the IES.

SNMP

Simple Network Management Protocol is a protocol used for exchanging management information between network switches. SNMP is a member of TCP/IP protocol suite. A manager station can manage and monitor the system through the network via SNMP version one (SNMPv1) and/or SNMP version 2c. The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

Figure 246 SNMP Management Model

An SNMP managed network consists of two main components: agents and a manager.

An agent is a management software module that resides in a managed switch (the system). An agent translates the local management information from the managed switch into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a switch. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

Table 209 SNMP Commands

COMMAND	DESCRIPTION
Get	Allows the manager to retrieve an object variable from the agent.
GetNext	Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
Set	Allows the manager to set values for object variables within an agent.
Trap	Used by the agent to inform the manager of some events.

Supported MIBs

MIBs let administrators collect statistics and monitor status and performance. The system supports the following MIBs:

- BRIDGE-MIB.mib
- IF-MIB.mib
- IANAIfType-MIB.mib
- INET-ADDRESS-MIB.mib

- Q-BRIDGE-MIB.mib
- RFC1155-SMI.mib
- RFC-1212.mib
- RFC1213-MIB.mib
- RFC-1215.mib
- RFC-1271.MIB
- RMON-MIB.mib
- SNMP-FRAMEWORK-MIB.mib
- SNMPv2-SMI.mib
- SNMPv2-MIB.mib
- SNMPv2-SMI.mib
- SNMPv2-TC.mib
- VDSL2_drafft06.mib
- VDSL2-LINE-MIB.mib
- VDSL2-LINE-TC-MIB.mib
- IEEE8021-PAE-MIB.mib (8021X)

The following table describes commonly used parameter notation for these commands.

Table 210 SNMP Server Command Parameters

NOTATION	DESCRIPTION
<i>property</i>	1-31 English printable characters; spaces are not allowed.

This table describes the commands.

Table 211 SNMP Server Commands Summary

COMMAND	DESCRIPTION	M	P
<code>show snmp-server</code>	Displays SNMP settings.	E	13
<code>snmpserver authfailtrap inactive</code>	Stops the SNMP agent process from generating authentication-failure traps.	C	13
<code>no snmp authfailtrap inactive</code>	Permits the SNMP agent process to generate authentication-failure traps, when setting by SNMP but the set-community on the SNMP server and manager do not match, or getting the MIB but the get-community on the SNMP server and manager do not match, or the authentication algorithm and/or password for the username in the SNMP server does not match between an SNMPv3 server and manager, or the security level for the username with security level auth priv in the SNMP server does not match between an SNMPv3 server and manager (for a username, the SNMPv3 server's security level needs to be higher than or equal to that of the SNMPv3 manager. A privacy algorithm mismatch between the SNMPv3 server and manager will not trigger an authentication-failure trap.	C	13
<code>snmp-server version</code> <code><v2c v3 v3v2c></code>	Sets the SNMP version to use for communication with the SNMP manager. v2c: v2c only v3: v3 only v3v2c: v2c and v3	C	13
<code>snmp-server get-community</code> <code><property></code>	Sets the get community. Only for SNMPv2c or lower.	C	13

Table 211 SNMP Server Commands Summary (continued)

COMMAND	DESCRIPTION	M	P
<code>snmp-server set-community <property></code>	Sets the set community. Only for SNMPv2c or lower.	C	13
<code>snmp-server trap-community <property></code>	Sets the trap community. Only for SNMPv2c or lower.	C	13
<code>snmp-server trap-destination <ip-address> <ipv6-address> [udp-port <socket-number>] [version <v1 v2c v3>] [username <name>]</code>	Sets the IP addresses of up to four SNMP managers (stations to send your SNMP traps to). You can configure up to four managers. <i>ip-address</i> : 0.0.0.0 ~ 223.255.255.255 <i>ipv6-address</i> : 2000:: ~ 3fff:ffff:ffff:ffff:ffff:ffff:ffff:ffff <i>udp-port</i> : SNMP manager UDP port <i>version</i> : SNMP version	C	13
<code>no snmp-server trap-destination <ip-address> <ipv6-address></code>	Deletes the specified SNMP manager. <i>ip-address</i> : 0.0.0.0 ~ 223.255.255.255 <i>ipv6-address</i> : 2000:: ~ 3fff:ffff:ffff:ffff:ffff:ffff:ffff:ffff	C	13
<code>snmp-server username <name> sec-level <noauth auth priv> [auth <md5 sha>] [priv <des aes>]</code>	<i>name</i> : Must match an existing account on the IES. <i>noauth</i> : Use the username as the password string sent to the SNMP manager. This is the equivalent to the Get, Set, and Trap Community in SNMPv2c. This is the lowest security level. <i>auth</i> : Implement an authentication algorithm for SNMP messages by this user. <i>priv</i> : Implement authentication and encryption for SNMP messages sent by this user. This is the highest security level. <i>md5 sha</i> : Specify MD5 or SHA authentication algorithm. <i>des aes</i> : Specify DES or AES encryption algorithm.	C	13

22.6 System Maintenance Commands

Use these commands to work with the IES firmware and configuration files, configure the hostname, contact, and location settings, and set the console port's baud rate.

You can store up to two firmware files (of the same device model) on the IES. Only one firmware is used at a time. This allows immediate rollback on system boot up in case the current firmware is corrupt. By default, the switch uses firmware `ras-0` while the second firmware file is named `ras-1`.

The IES also supports dual configuration files that you can switch between.

- Select which firmware to use during system startup using the `boot image <1|2>` command (where 1 is `ras-0` and 2 is `ras-1`).
- To specify whether to save a new firmware to `ras-0` or `ras-1` on the switch, perform firmware upgrade using the FTP commands (refer to [Section 22.7.2 on page 329](#)).
- If the IES detects that firmware boot up has failed due to an incomplete firmware upgrade (which can be caused by a power outage during upgrading), the IES automatically changes to the other firmware.

- If firmware boot up fails due to defective firmware, use the admin account to access the device through the console port and use the `ATBI` command. For example, `ATBI1` has the IES use the first firmware, `ATBI2` has it use the second.

After the system successfully boots up, use the `show boot-image` command to check which firmware image file the IES is currently using.

The following section lists the commands for this feature.

Table 212 System Maintenance Commands Summary

COMMAND	DESCRIPTION	M	P
<code>boot config</code>	Restarts the system with the current active configuration file.	E	13
<code>boot config seconds</code> <i><seconds></i>	Restarts the system with the current active configuration file, after the specified number of seconds. <i>seconds</i> : 3~2147483647 seconds	E	13
<code>no boot config</code>	Cancels a scheduled reboot.	E	13
<code>boot image <1 2></code>	Restarts the system with the specified firmware image (1: ras-0, 2: ras-1).	E	13
<code>help</code>	Displays the interactive help system.	E	1
<code>show boot-image</code>	Displays the firmware image file currently in use.	E	13
<code>show system-information</code>	Displays general system information.	E	1
<code>show version [flash]</code>	Displays the version of the currently running firmware. Optionally, display the versions of the currently installed firmware images on the flash memory.	E	1
<code>write memory</code>	Saves the current configuration in volatile memory to the configuration file currently in use.	E	13
<code>show startup-config</code>	Displays the configuration file currently in use.	E	13
<code>hostname <hostname></code>	Sets the system name for identification purposes. <i>hostname</i> : up to 31 printable characters; spaces are allowed.	C	13
<code>contact <contact></code>	Sets the contact information. <i>contact</i> : up to 31 English printable characters; spaces are allowed.	C	13
<code>location <location></code>	Sets the location information. <i>location</i> : up to 31 English printable characters; spaces are allowed.	C	13
<code>login-message</code>	Sets the login information for console, TELNET, SSH, and the Web Configurator. After the command is executed, the UI gets all characters keyed in until Ctrl+S or Ctrl+X is pressed. Ctrl+S saves the characters keyed in, while Ctrl+X drops all characters.	E	13
<code>baudrate <1 2 3 4 5></code>	Changes the console port baud rate (in bps). 1: 38400 2: 19200 3: 9600 4: 57600 5: 115200	E	1
<code>show cpu info</code>	Displays recent CPU utilization.	E	13

22.7 FTP for Configuration and Firmware Files

This section shows some examples of uploading to or downloading files from the IES using FTP commands. First, understand the filename conventions.

22.7.1 Filename Conventions

The configuration file (also known as the romfile or ROM) initially contains the factory default settings. After you customized the IES's settings, save them back to your computer under a filename of your choosing.

Table 213 Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	config	*.cfg	This is the configuration filename on the IES. Uploading the config file replaces the specified configuration file system, including your IES configurations, system-related data (including the default password), the error log and the trace log.
Firmware	ras-0 ras-1	*.bin	This is the generic name for the firmware on the IES. <code>ras-0</code> is image 1; <code>ras-1</code> is image 2.

The IES supports dual firmware images, `ras-0` and `ras-1`. It uses one firmware image at a time.

The names `ras-0` and `ras-1` are internal and not visible through FTP. You see "ras" when you type "ls" at the FTP prompt. The IES updates the backup (non-active) image when you use FTP to upload firmware to the IES. For example if the active (loaded) image is `ras-0` and you use the FTP `put` command, the IES updates `ras-1`. At the next start up the IES loads `ras-1` as the boot image and keeps `ras-0` as a backup. This ensures that the IES always has a bootable image (the backup one).

- Run the `boot image <1 | 2>` command to restart the IES with the specified firmware image (1: `ras-0`, 2: `ras-1`).
- Use FTP commands to upload firmware to the non-active image.

22.7.1.1 Example FTP Commands

Make sure you have downloaded (and unzipped) the correct model firmware and version to your computer before uploading to the device.

Be sure to upload the correct model firmware as uploading the wrong model firmware may damage your device.

```
ftp> put firmware.bin ras
```

This is a sample FTP session showing the transfer of the computer file `firmware.bin` to the IES.

```
ftp> get config config.cfg
```

This is a sample FTP session saving the current configuration to a file called "config.cfg" on your computer.

If your (T)FTP client does not allow you to have a destination filename different than the source, you will need to rename them as the IES only recognizes "config" and "ras". Be sure you keep unaltered copies of all files for later use.

22.7.2 FTP Command Line Procedure

- 1 Launch the FTP client on your computer.
- 2 Enter `open`, followed by a space and the IP address of your IES.
- 3 Press [ENTER] when prompted for a username.
- 4 Enter your password as requested (the default is "1234").
- 5 Enter `bin` to set transfer mode to binary.
- 6 Use `put` to transfer files from the computer to the IES, for example, `put firmware.bin ras` transfers the firmware on your computer (`firmware.bin`) to the IES and uses it to replace the non-active image. Similarly, `put config.cfg config` transfers the configuration file on your computer (`config.cfg`) to the IES and renames it to "config". Likewise `get config config.cfg` transfers the configuration file on the IES to your computer and renames it to "`config.cfg`". See [Table 213 on page 328](#) for more information on filename conventions.
- 7 Enter `quit` to exit the ftp prompt.

22.8 AAA Commands

Use these commands to configure authentication, authorization and accounting on the IES.

Authentication, Authorization, Accounting (AAA)

Authentication is the process of determining who a user is and validating access to the system. The system can authenticate users who try to log in based on user accounts configured on the system itself. The system can also use an external authentication server to authenticate a large number of users.

Authorization is the process of determining what a user is allowed to do. Different user accounts may have higher or lower privilege levels associated with them. For example, user A may have the right to create new login accounts on the system but user B cannot. The system can authorize users based on user accounts configured on the system itself or it can use an external server to authorize a large number of users.

Accounting is the process of recording what a user is doing. The system can use an external server to track when users log in, log out, execute commands and so on. Accounting can also record system related actions such as boot up and shut down times of the system.

The external servers that perform authentication, authorization and accounting functions are known as AAA servers. The system supports RADIUS (Remote Authentication Dial-In User Service) and TACACS+

(Terminal Access Controller Access-Control System Plus) as external authentication and accounting servers. The system supports TACACS+ as external authorization server only.

Local User Accounts

By storing user profiles locally on the IES, your IES is able to authenticate and authorize users without interacting with a network authentication server. However, there is a limit on the number of users you may authenticate in this way.

RADIUS and TACACS+

RADIUS and TACACS+ are security protocols used to authenticate users by means of an external server instead of (or in addition to) an internal device user database that is limited to the memory capacity of the device. In essence, RADIUS and TACACS+ authentication both allow you to validate an unlimited number of users from a central location.

The following table describes some key differences between RADIUS and TACACS+.

Table 214 RADIUS vs. TACACS+

	RADIUS	TACACS+
Transport Protocol	UDP (User Datagram Protocol)	TCP (Transmission Control Protocol)
Encryption	Encrypts the password sent for authentication.	All communication between the IES and the TACACS+ server is encrypted.

22.8.1 AAA Command Summary

The following section lists the commands for this feature.

Table 215 aaa command summary

COMMAND	DESCRIPTION	M	P
<code>aaa server authentication radius index <1 2></code>	Configures an entry for RADIUS authentication server settings.	C	13
<code>address <ip-address></code>	Sets the specified RADIUS server's IP address.	C	13
<code>port <1-65535></code>	Sets the specified RADIUS server's port number for recording events.	C	13
<code>secret <secret></code>	Sets a secret password shared with the specified RADIUS server. <i>secret</i> : 1~31 printable characters	C	13
<code>aaa server authentication radius mode <index-priority round-robin></code>	Specifies how the IES decides which authentication server to use if you configure multiple servers. <i>index-priority</i> : The IES tries to authenticate with the first configured authentication server. If the server does not respond, then the IES tries to authenticate with the second authentication server. <i>round-robin</i> : The IES alternates between authentication servers that it sends authentication requests to.	C	13

Table 215 aaa command summary (continued)

COMMAND	DESCRIPTION	M	P
aaa server authentication radius timeout <timeout>	Sets the timeout interval in seconds that the IES waits for the authentication response from the server. If you are using index priority and you are using two sets then the timeout value is divided between the two servers. For example, if you set the timeout value to 30 seconds, the IES waits for a response from first server for 15 seconds and then tries the second server. Default value is 30 seconds. <i>timeout: 1 ~ 300</i>	C	13
no aaa server authentication radius index <1 2>	Clears the specified authentication server entry's settings.	C	13
no aaa server authentication radius mode	Resets the authentication server's mode to the default.	C	13
no aaa server authentication radius timeout	Resets the timeout value to the default.	C	13
show aaa server authentication radius	Displays all RADIUS authentication server settings.	E	3
aaa server accounting radius index <1 2>	Configures an entry of RADIUS accounting server settings.	C	13
address <ip-address>	Sets the accounting server's IP address.	C	13
port <1-65535>	Sets the accounting server's port number for recording events.	C	13
secret <secret>	Sets a secret password shared with the accounting server. <i>secret: 1~31 printable characters</i>	C	13
aaa server accounting radius mode <index-priority round-robin>	Specifies how the IES decides which accounting server to use if you configure multiple servers. <i>index-priority:</i> The IES tries to send logs to the first configured accounting server. If the accounting server does not respond, then the IES tries to send logs to the second accounting server. <i>round-robin:</i> The IES alternates the sending of logs between the configured accounting server settings.	C	13
aaa server accounting radius timeout <seconds>	Sets the timeout interval in seconds that the IES waits for the accounting response from the server. If you are using index priority and you are using two sets then the timeout value is divided between the two servers. For example, if you set the timeout value to 30 seconds, the IES waits for a response from first server for 15 seconds and then tries the second server. Default value is 30 seconds. <i>timeout: 1 ~ 60</i>	C	13
no aaa server accounting radius index <1 2>	Clears the specified accounting server's settings.	C	13
aaa server authentication tacacas+ index <1 2>	Configures an entry for TACACS+ authentication server settings.	C	13
address <ip-address>	Sets the specified TACACS+ server entry's IP address.	C	13
port <1-65535>	Sets the specified TACACS+ server entry's TCP port number for recording events.	C	13
secret <secret>	Sets a secret password shared with the specified TACACS+ server. <i>secret: 1~32 printable characters</i>	C	13

Table 215 aaa command summary (continued)

COMMAND	DESCRIPTION	M	P
aaa server authentication tacacas+ mode <index- priority round-robin>	Specifies how the IES decides which TACACS+ authentication server to use if you configure multiple servers. index-priority: The IES tries to authenticate with the first configured authentication server. If the server does not respond, then the IES tries to authenticate with the second authentication server. round-robin: The IES alternates between authentication servers that it sends authentication requests to.	C	13
aaa server authentication tacacas+ timeout <timeout>	Sets the timeout interval in seconds that the IES waits for the authentication response from the TACACS+ server. If you are using index priority and you are using two sets then the timeout value is divided between the two servers. For example, if you set the timeout value to 30 seconds, the IES waits for a response from first server for 15 seconds and then tries the second server. Default value is 30 seconds. timeout: 1 ~ 300	C	13
no aaa server authentication tacacas+ index <1 2>	Clears the specified authentication server entry's settings.	C	13
no aaa server authentication tacacas+ mode	Resets the authentication server's mode to the default.	C	13
no aaa server authentication tacacas+ timeout	Resets the timeout value to the default.	C	13
show aaa server authentication tacacas+	Displays all TACACS+ authentication server settings.	E	3
aaa server accounting tacacas+ index <1 2>	Configures an entry of TACACS+ accounting server settings.	C	13
address <ip-address>	Sets the accounting server's IP address.	C	13
port <1-65535>	Sets the accounting server's port number for recording events.	C	13
secret <secret>	Sets a secret password shared with the accounting server. secret: 1~31 printable characters	C	13
aaa server accounting tacacas+ mode <index-priority round- robin>	Specifies how the IES decides which accounting server to use if you configure multiple servers. index-priority: The IES tries to send logs to the first configured accounting server. If the accounting server does not respond, then the IES tries to send logs to the second accounting server. round-robin: The IES alternates the sending of logs between the configured accounting server settings.	C	13
aaa server accounting tacacas+ timeout <seconds>	Sets the timeout interval in seconds that the IES waits for the accounting response from the server. If you are using index priority and you are using two sets then the timeout value is divided between the two servers. For example, if you set the timeout value to 30 seconds, the IES waits for a response from first server for 15 seconds and then tries the second server. Default value is 30 seconds. timeout: 1 ~ 60	C	13
no aaa server accounting tacacas+ index <1 2>	Clears the specified accounting server's settings.	C	13
no aaa server accounting tacacas+ mode	Resets the accounting server's index-priority or round-robin mode to the default.	C	13

Table 215 aaa command summary (continued)

COMMAND	DESCRIPTION	M	P
no aaa server accounting tacacs+ timeout	Resets the timeout value to the default.	C	13
show aaa server accounting tacacs+	Displays all TACACS+ accounting server settings.	E	3
aaa server authorization tacacs+ index <1-2>	Configures an entry of TACACS+ authorization server settings.	C	13
address <ip-address>	Sets the authorization server's IP address.	C	13
port <1-65535>	Sets the authorization server's port.	C	13
secret <secret>	Sets a secret password shared with the authorization server. <i>secret</i> : 1~31 printable characters	C	13
aaa server authorization tacacs+ mode <index- priority round-robin>	Specifies how the IES decides which TACACS+ authorization server to choose if you configure multiple servers. <i>index-priority</i> : The IES tries to send authorization requests to the first configured authorization server. If the authorization server does not respond, then the IES tries to send requests to the second authorization server. <i>round-robin</i> : The IES alternates the sending of logs between the configured authorization server settings.	C	13
aaa server authorization tacacs+ timeout <timeout>	Sets the timeout interval in seconds that the IES waits for the authentication response from the TACACS+ server. If you are using index priority and you are using two sets then the timeout value is divided between the two servers. For example, if you set the timeout value to 30 seconds, the IES waits for a response from first server for 15 seconds and then tries the second server. Default value is 30 seconds. <i>timeout</i> : 1 ~ 300	C	13
no aaa server authorization tacacs+ index <index>	Clears the specified TACACS+ authorization server's settings.	C	13
no aaa server authorization tacacs+ mode	Resets the TACACS+ authorization mode to the default.	C	13
no aaa server authorization tacacs+ timeout	Resets the TACACS+ timeout value to the default.	C	13
show aaa server authorization tacacs+	Displays all TACACS+ authorization server settings.	E	3
aaa authentication enable <method> [<method>...]	Sets the authentication methods to authenticate users' access privilege levels and sets the order. If the IES fails to get a request response in time through the first method, the IES uses the second method. <i>method</i> : local, radius or tacacs+	C	13
aaa authentication login <method> [<method> ...]	Sets the authentication methods to authenticate user login and the order for using them. <i>method</i> : local, radius or tacacs+	C	13
show aaa authentication	Displays the enable and login authentication method settings.	E	3
no aaa authentication	Resets both the enable and login authentication method settings to their defaults.	C	13
no aaa authentication enable	Resets the enable authentication method settings to the default.	C	13
no aaa authentication login	Resets the login authentication method settings to the default.	C	13

Table 215 aaa command summary (continued)

COMMAND	DESCRIPTION	M	P
aaa accounting update period <period>	Sets how often the IES sends an update to the accounting server. This is only valid if you set the start-stop option using the aaa accounting exec command. <i>period</i> : 1 ~ 2147483647 in minutes, default is 1 minute	C	13
aaa accounting system <method>	Sets the accounting method used for recording the following system events: system boots up, system shuts down, system accounting is enabled, system accounting is disabled. <i>method</i> : radius Or tacacs+	C	13
aaa accounting exec <start-stop stop-only> <method>	Sets the mode and accounting method used for recording administrator's login and logout events via the console port, Telnet or SSH. <i>start-stop</i> : to have the system send information to the accounting server when a user begins a session, during a user's session (if it lasts past the "update period"), and when a user ends a session. <i>stop-only</i> : to have the system send information to the accounting server only when a user ends a session. <i>method</i> : radius Or tacacs+	C	13
aaa accounting command privilege <privilege> stop-only tacacs+	Sets the accounting method used for recording information when commands of the specified privilege level and higher are executed on the system. <i>privilege</i> : 1-14 Note: TACACS+ is the only method for recording the "commands" type of events.	C	13
show aaa accounting	Displays accounting settings.	E	3
no aaa accounting update period	Resets the update interval for accounting to the default value.	C	13
no aaa accounting system	Disables accounting for system type events, such as system boots up and system shuts down.	C	13
no aaa accounting exec	Disables accounting for exec type events, such as recording administrator's login and logout events via the console port, Telnet or SSH.	C	13
no aaa accounting command	Disables accounting for command type events.	C	13
no aaa accounting	Resets all accounting settings to their defaults.	C	13

Table 215 aaa command summary (continued)

COMMAND	DESCRIPTION	M	P
aaa authorization privilege <privilege> <mode>	Sets the authorization mode for the specified command privilege level. Every command belongs to a privilege. Authorization happens when a user executes a command matching the specified privilege. For example, to allow only one user "A" to use the multicast commands, you can configure this system so all the <code>igmp-mld</code> commands require a specific privilege level (ex. 12) and set the authorization method for this privilege level to <code>tacacs+</code>. Then you set the command shell set configured in the TACACS+ server to only give user "A" access to multicast commands. <i>privilege: 1-14</i> <i>mode: 1-5</i> 1: none: to have no authorization 2: local: to have the system use its local database. This is the default value. 3: tacacs+: to have the system use a remote TACACS+ server. 4: tacacs+ then none: to have the system use a remote TACACS+ server and if the TACACS+ server does not respond, the system has no authorization. 5: tacacs+ then local: to have the system use remote TACACS+ server and if the TACACS+ server does not respond, use its local database.	C	13
show aaa authorization	Displays authorization method and privilege mappings.	E	3
no aaa authorization	Resets the authorization mode and privilege mappings to the defaults.	C	13

22.8.2 Command Examples

This example displays how to set the authentication methods for login first to use RADIUS server and second to use the IES's local database. Then it displays the current authentication method settings.

```

sysname# configure
sysname(config)# aaa authentication login radius local
sysname(config)# exit
sysname# show aaa authentication
login type method :
method1 method2 method3
-----
radius local

enable type method :
method1 method2
-----
local

```

This example displays how to set the authorization method to "tacacs+ then local" for privilege 12 and then displays the settings.

```

sysname# configure
sysname(config)# aaa authorization privilege 12 3
sysname(config)# exit
sysname# show aaa authorization
Privilege  Mode
-----
      1  local
      2  local
      3  local
      4  local
      5  local
      6  local
      7  local
      8  local
      9  local
     10  local
     11  local
     12  tacacs+ then local
     13  local
     14  local

```

This example displays how to set:

- 1 Accounting method to "radius" for recording system-type events.
- 2 Accounting method to "tacacs+" for recording command-type events with privilege 12.
- 3 Update interval to 3 minutes.

Finally, it displays the settings.

```

sysname# config
sysname(config)# aaa accounting system radius
sysname(config)# aaa accounting command privilege 12 tacacs+
sysname(config)# aaa accounting update period 3
sysname(config)# exit
sysname# show aaa accounting
accounting update timeout: 3 minutes
accounting system:
  method
  -----
  radius

accounting exec:
  method  mode
  -----  -----
  radius  start-stop

accounting commands:
  privilege
  -----
  12

```

22.9 Performance Management

Use these commands for performance management.

22.9.1 Performance Management Commands Summary

The following table describes commonly used parameter notation for these commands.

Table 216 performance management command parameters

NOTATION	DESCRIPTION
<i>alarm-profile</i>	The name of an alarm profile. Use up to 31 printable characters.
<i>portlist</i>	The number of uplink ports, 1-2. You can use 1,2, 1~2 or * to specify all the ports.
<i>threshold</i>	0 ~ 18446744073709551615. An alarm is triggered if this number is exceeded.

This table describes the commands.

Table 217 performance management commands summary

COMMAND	DESCRIPTION	M	P
ge-nni alarm-profile <alarm-profile>	Enters the sub-command mode for configuring a GE port alarm profile.	C	13
exit	Leaves the GE port alarm profile configuration sub-command mode.	C	13
15min-txoctets-threshold <threshold>	Configures the number of octets of Ethernet frames allowed to transmit in any 15-minute period.	C	13
15min-txpkts-threshold <threshold>	Configures the number of packets allowed to transmit in any 15-minute period.	C	13
15min-txbcastpkts-threshold <threshold>	Configures the number of broadcast packets allowed to transmit in any 15-minute period.	C	13
15min-txmcastpkts-threshold <threshold>	Configures the number of multicast packets allowed to transmit in any 15-minute period.	C	13
15min-rxoctets-threshold <threshold>	Configures the number of octets of Ethernet frames allowed to receive in any 15-minute period.	C	13
15min-rxpkts-threshold <threshold>	Configures the number of packets allowed to receive in any 15-minute period.	C	13
15min-rxbcastpkts-threshold <threshold>	Configures the number of broadcast packets allowed to receive in any 15-minute period.	C	13
15min-rxmcastpkts-threshold <threshold>	Configures the number of multicast packets allowed to receive in any 15-minute period.	C	13
15min-rxcrc-threshold <threshold>	Configures the number of CRC (Cyclical Redundancy Check) alignment errors allowed to occur in any 15-minute period.	C	13
15min-rxunder-threshold <threshold>	Configures the number of packets that were too small allowed to receive in any 15-minute period.	C	13
15min-rxover-threshold <threshold>	Configures the number of packets that were too big allowed to receive in any 15-minute period.	C	13
15min-rxfrag-threshold <threshold>	Configures the number of fragmented frames allowed to receive in any 15-minute period.	C	13

Table 217 performance management commands summary (continued)

COMMAND	DESCRIPTION	M	P
15min-collision-threshold <threshold>	Configures the number of frames for which transmission failed due to excessive collisions allowed to receive or transmit in any 15-minute period. Excessive collision is defined as the number of maximum collisions before the retransmission count is reset.	C	13
15min-64octets-threshold <threshold>	Configures the number of frames 64 octets or less in length allowed to receive or transmit in any 15-minute period.	C	13
15min-127octets-threshold <threshold>	Configures the number of frames 65 to 127 octets in length allowed to receive or transmit in any 15-minute period.	C	13
15min-255octets-threshold <threshold>	Configures the number of frames 128 to 255 octets in length allowed to receive or transmit in any 15-minute period.	C	13
15min-511octets-threshold <threshold>	Configures the number of frames 256 to 511 octets in length allowed to receive or transmit in any 15-minute period.	C	13
15min-1023octets-threshold <threshold>	Configures the number of frames 512 to 1023 octets in length allowed to receive or transmit in any 15-minute period.	C	13
15min-1518octets-threshold <threshold>	Configures the number of frames 1024 to 1518 octets in length allowed to receive or transmit in any 15-minute period.	C	13
15min-1522octets-threshold <threshold>	Configures the number of frames 1519 to 1522 octets in length allowed to receive or transmit in any 15-minute period.	C	13
no ge-nni alarm-profile <alarm-profile>	Deletes the specified Gigabit Ethernet (GE) port alarm profile.	C	13
show ge-nni alarm-profile [alarm-profile]	Displays all or the specified GE port alarm profile.	E	13
interface ge-nni <portlist>	Enters the sub-command mode for configuring the specified GE ports.	C	13
alarm-profile <alarm-profile>	Applies the specified alarm profile to the ports.	C	13
clear interface ge-nni <portlist> performance	Clears current, historical 15-minutes and historical 1-day Ethernet line status on the specified GE ports.	E	13
show interface ge-nni <portlist> performance <current 15-min 1-day>	Displays current, historical 15-minutes and historical 1-day Ethernet line status on the specified GE ports.	E	13
dsl alarm-profile <alarm-profile>	Enters the sub-command mode for configuring a DSL port alarm profile.	C	13
exit	Leaves the DSL port alarm profile configuration sub-command mode.	C	13
15min-txBytes-threshold <threshold>	Configures the number of octets allowed to transmit in any 15-minute period.	C	13
15min-txPkts-threshold <threshold>	Configures the number of packets allowed to transmit in any 15-minute period.	C	13
15min-txUnicastPkts-threshold <threshold>	Configures the number of unicast packets allowed to transmit in any 15-minute period.	C	13
15min-txMulticastPkts-threshold <threshold>	Configures the number of multicast packets allowed to transmit in any 15-minute period.	C	13
15min-txBroadcastPkts-threshold <threshold>	Configures the number of broadcast packets allowed to transmit in any 15-minute period.	C	13
15min-txDiscardPkts-threshold <threshold>	Configures the number of transmitted discard packets allowed in any 15-minute period.	C	13

Table 217 performance management commands summary (continued)

COMMAND	DESCRIPTION	M	P
15min-rxBytes-threshold <threshold>	Configures the number of octets of Ethernet frames allowed to receive in any 15-minute period.	C	13
15min-rxPkts-threshold <threshold>	Configures the number of packets allowed to receive in any 15-minute period.	C	13
15min-rxUnicastPkts-threshold <threshold>	Configures the number of unicast packets allowed to receive in any 15-minute period.	C	13
15min-rxMulticastPkts-threshold <threshold>	Configures the number of multicast packets allowed to receive in any 15-minute period.	C	13
15min-rxBroadcastPkts-threshold <threshold>	Configures the number of broadcast packets allowed to receive in any 15-minute period.	C	13
15min-rxDiscardPkts-threshold <threshold>	Configures the number of discard packets allowed to receive in any 15-minute period.	C	13
no dsl alarm-profile <alarm-profile>	Deletes the specified DSL port alarm profile.	C	13
show dsl alarm-profile [alarm-profile]	Displays all or the specified DSL port alarm profile.	E	13
interface dsl <portlist>	Enters the sub-command mode for configuring the specified DSL ports.	C	13
alarm-profile <alarm-profile>	Applies the specified alarm profile to the ports.	C	13
clear interface dsl <portlist> performance	Clears current, historical 15-minutes and historical 1-day line status on the specified DSL ports.	E	13
show interface dsl <portlist> performance <current 15-min 1-day>	Displays current, historical 15-minutes and historical 1-day line status on the specified DSL ports.	E	13
fe alarm-profile <alarm-profile>	Enters the sub-command mode for configuring a FE port alarm profile.	C	13
exit	Leaves the DSL port alarm profile configuration sub-command mode.	C	13
15min-txoctets-threshold <threshold>	Configures the number of octets of Ethernet frames allowed to transmit in any 15-minute period.	C	13
15min-txpKts-threshold <threshold>	Configures the number of packets allowed to transmit in any 15-minute period.	C	13
15min-txbcastpkts-threshold <threshold>	Configures the number of broadcast packets allowed to transmit in any 15-minute period.	C	13
15min-txmcastpkts-threshold <threshold>	Configures the number of multicast packets allowed to transmit in any 15-minute period.	C	13
15min-rxoctets-threshold <threshold>	Configures the number of octets of Ethernet frames allowed to receive in any 15-minute period.	C	13
15min-rxpKts-threshold <threshold>	Configures the number of packets allowed to receive in any 15-minute period.	C	13
15min-rxbcastpkts-threshold <threshold>	Configures the number of broadcast packets allowed to receive in any 15-minute period.	C	13
15min-rxmcastpkts-threshold <threshold>	Configures the number of multicast packets allowed to receive in any 15-minute period.	C	13
15min-rxcrc-threshold <threshold>	Configures the number of CRC (Cyclical Redundancy Check) alignment errors allowed to occur in any 15-minute period.	C	13

Table 217 performance management commands summary (continued)

COMMAND	DESCRIPTION	M	P
15min-rxunder-threshold <threshold>	Configures the number of packets that were too small allowed to receive in any 15-minute period.	C	13
15min-rxover-threshold <threshold>	Configures the number of packets that were too big allowed to receive in any 15-minute period.	C	13
15min-rxfrag-threshold <threshold>	Configures the number of fragmented frames allowed to receive in any 15-minute period.	C	13
15min-collision-threshold <threshold>	Configures the number of frames for which transmission failed due to excessive collisions allowed to receive or transmit in any 15-minute period. Excessive collision is defined as the number of maximum collisions before the retransmission count is reset.	C	13
15min-64octets-threshold <threshold>	Configures the number of frames 64 octets or less in length allowed to receive or transmit in any 15-minute period.	C	13
15min-127octets-threshold <threshold>	Configures the number of frames 65 to 127 octets in length allowed to receive or transmit in any 15-minute period.	C	13
15min-255octets-threshold <threshold>	Configures the number of frames 128 to 255 octets in length allowed to receive or transmit in any 15-minute period.	C	13
15min-511octets-threshold <threshold>	Configures the number of frames 256 to 511 octets in length allowed to receive or transmit in any 15-minute period.	C	13
15min-1023octets-threshold <threshold>	Configures the number of frames 512 to 1023 octets in length allowed to receive or transmit in any 15-minute period.	C	13
15min-1518octets-threshold <threshold>	Configures the number of frames 1024 to 1518 octets in length allowed to receive or transmit in any 15-minute period.	C	13
no fe alarm-profile <alarm-profile>	Deletes the specified Fast Ethernet (FE) port alarm profile.	C	13
show fe alarm-profile [alarm-profile]	Displays all or the specified FE port alarm profile.	E	13
interface fe <portlist>	Enters the sub-command mode for configuring the specified FE ports.	C	13
alarm-profile <alarm-profile>	Applies the specified alarm profile to the ports.	C	13
clear interface fe <portlist> performance	Clears current, historical 15-minutes and historical 1-day Ethernet line status on the specified FE ports.	E	13
show interface fe <portlist> performance <current 15-min 1-day>	Displays current, historical 15-minutes and historical 1-day Ethernet line status on the specified FE ports.	E	13
no voip alarm-profile <alarm-profile>	Deletes the specified VoIP alarm profile.	C	13
show voip alarm-profile [alarm-profile]	Displays all or the specified VoIP alarm profile.	E	13
voip alarm-profile <alarm-profile>	Enters the sub-command mode for configuring the specified VoIP alarm profile.	C	13
exit	Leaves the sub-command mode.	C	13
15min-rtpelapse-threshold <threshold>	Configures the accumulated time of RTP sessions allowed in any 15-minute period. In other words, this is the amount of audio transmission time allowed within 15 minutes.	C	13
15min-rtptxbytes-threshold <threshold>	Configures the accumulated number of bytes of RTP packets that can be transmitted in any 15-minute period.	C	13

Table 217 performance management commands summary (continued)

COMMAND	DESCRIPTION	M	P
15min-rtprxbytes-threshold <threshold>	Configures the accumulated number of bytes of RTP packets that can be received in any 15-minute period.	C	13
15min-rtptxpks-threshold <threshold>	Configures the number of RTP packets that can be transmitted in any 15-minute period.	C	13
15min-rtprxpks-threshold <threshold>	Configures the number of RTP packets that can be received in any 15-minute period.	C	13
15min-rtptxlostpkts-threshold <threshold>	Configures the number of RTP packets that can be lost during transmission in any 15-minute period.	C	13
15min-rtprxlostpkts-threshold <threshold>	Configures the number of RTP packets that can be failed to be received by the IES in any 15-minute period.	C	13
interface voip <slot/portlist>	Configures specified VoIP UNI ports.	C	13
alarm-profile <alarm-profile>	Configures the referenced VoIP alarm profile to specified UNI ports.	C	13
clear interface voip <slot/portlist> performance	Clears VoIP performance statistics for the specified ports.	E	13
show interface voip <slot/portlist> performance <current 15-min 1-day>	Displays VoIP performance statistics for the specified ports currently, in the most recent 15-minute, or in the past one day time segment.	E	13

22.9.2 Command Examples

This example first shows how to configure a performance management alarm profile named **Alarm1**. Then allow 1234 packets to receive in a 15-minute period. Finally, apply the alarm profile **Alarm1** to GE port 1.

```

ras# config
ras(config)# ge-nni alarm-profile Alarm1
ras(config-Gsx-alm-profile-Alarm1)# 15min-rxPkts-threshold 1234
ras(config-Gsx-alm-profile-Alarm1)#exit
ras# config
ras# (config)# interface-ge-nni-1
ras(config-interface-ge-nni-1)# alarm-profile Alarm1

```

22.10 Remote Management

Use these commands to specify remote hosts that can access the IES for management.

22.10.1 Remote Management Commands Summary

The following table describes commonly used parameter notation for these commands.

Table 218 remote management command parameters

NOTATION	DESCRIPTION
<i>index</i>	The index number of a trusted host entry, 1~16. You can specify a single entry <1>, all entries <*> or a list of entries <1,3>. You can also include a range of entries <1-5>.
<i>ip-address</i>	An IPv4 IP address, 0.0.0.0 ~ 223.255.255.255
<i>ipv6-address</i>	An IPv6 IP address, :: ~ ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

This table describes the commands.

Table 219 remote management command summary

COMMAND	DESCRIPTION	M	P
show remote-management	Displays all IPv4 trusted host information.	E	13
remote-management <index>	Enters the sub-command mode for configuring the specified IPv4 trusted host entry.	C	13
exit	Leaves the IPv4 trusted host configuration sub-command mode.	C	13
active	Enables the IPv4 trusted host entry.	C	13
no active	Disables the IPv4 trusted host entry.	C	13
start-addr <ip-address> end-addr <ip-address>	Configures a range of trusted hosts with the starting and ending IPv4 IP addresses. Setting both the starting and ending addresses to 0.0.0.0 removes the trusted host limitation. That is, any host can access the IES.	C	13
service <[icmp] [telnet] [ftp] [snmp] [web] [https] [ssh] [voip]>	Allows the trusted host to access the IES through the specified services.	C	13
no service <[icmp] [telnet] [ftp] [snmp] [web] [https] [ssh] [voip]>	Stops the trusted host from accessing the IES through the specified services.	C	13
show remote-management ipv6	Displays all IPv6 trusted host information.	E	13
remote-management ipv6 <index>	Enters the sub-command mode for configuring the specified IPv6 trusted host entry.	C	13
exit	Leaves the IPv6 trusted host configuration sub-command mode.	C	13
active	Enables the IPv6 trusted host entry.	C	13
no active	Disables the IPv6 trusted host entry.	C	13
address <ipv6-address> mask <mask>	Configures a trusted host with its IPv6 IP address and the prefix length. <i>mask</i> : 0 ~ 128, 0 means any hosts.	C	13
service <[icmp] [telnet] [ftp] [snmp] [ssh] [web] [https]>	Allows the trusted host to access the IES through the specified services.	C	13
no service <[icmp] [telnet] [ftp] [snmp] [ssh] [web] [https]>	Stops the trusted host from accessing the IES through the specified services.	C	13

22.10.2 Command Examples

This example allows computers in subnet 172.16.37.0/255 to access the IES through any service except SNMP, allows the computer at 192.168.10.1 to access the IES only through SNMP, and prevents other computers from accessing the IES at all.

```

ras# config
ras(config)# remote-management 1
ras(config-remote-management-1)# start-addr 172.16.37.0 end-addr
--> 172.16.37.255
ras(config-remote-management-1)# service icmp telnet ftp ssh
ras(config-remote-management-1)# exit
ras# config
ras(config)# remote-management 2
ras(config-remote-management-2)# start-addr 192.168.10.1 end-addr
--> 192.168.10.1
ras(config-remote-management-2)# service snmp
ras(config-remote-management-2)# exit
ras(config)# exit
ras#

```

22.11 Syslog

The syslog protocol allows devices to send event notification messages across an IP network to syslog servers that collect the event messages. A syslog-enabled device can generate a syslog message and send it to a syslog server.

Syslog is defined in RFC 3164. The RFC defines the packet format, content and system log related information of syslog messages. Each syslog message has a facility and severity level. The syslog facility identifies a file in the syslog server. Refer to the documentation of your syslog program for details.

22.11.1 Syslog Commands Summary

Use these commands to configure the device's system logging settings and to configure the external syslog server entries.

Table 220 Syslog Server Commands

COMMAND	DESCRIPTION	M	P
show syslog	Displays the syslog settings.	E	13
syslog	Enables the syslog client.	C	13
syslog server <index> address <ip-address> <ipv6-address>	Configures the IP addresses of the syslog servers. <i>index</i> : 1-4 <i>ip-address</i> : 0.0.0.0-223.255.255.255 <i>ipv6-address</i> : :: ~ ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff	C	13
no syslog	Disables the syslog client.	C	13
no syslog server <index>	Loads the default syslog server setting. <i>index</i> : 1-4	C	13

CHAPTER 23

Line Card Management

Use these commands to enable, disable, reset, or display status information about line cards.

23.1 Line Card Management Commands Summary

This table describes the commands.

Table 221 Line Card Management Commands Summary

COMMAND	DESCRIPTION	M	P
<code>lcman slot <slot> provision-type <card type></code>	Configures the line card type of the specified slot. After you provision the slot for a type of line card, you can only use that type of line card in the slot. <i>slot</i> : slot number 2 ~ 5 <i>card type</i> : card type <code>alc</code> (ADSL2+), <code>v1c</code> (VDSL2), or <code>vop</code> (VoIP)	C	13
<code>lcman disable <slot></code>	Disables the line card in the specified slot.	E	13
<code>lcman enable <slot></code>	Enables the line card in the specified slot.	E	13
<code>lcman reset slot <slot></code>	Resets the line card in the specified slot.	E	13
<code>show lcman</code>	Displays the status of the installed line cards. Optionally, displays the information of specified installed line card.	E	13

23.1.1 Command Examples

This example shows how to check all card states and activate a card

- 1 Display all line cards' status.
- 2 Activate (provision) slot 3 where an ADSL card is installed.

3 Display the line card status again. Note that the line card's state will go to "Init" and then "Active".

```

ras# show lcman
f/w version: V3.60(ABIZ.0)b2
id state      card type      provision type      uptime heat vol mon
--
1 Active      MSC1002GA      -                  1:21:13:50      - - -
2 Active      VOP1164A-61   VOP1164A-61       1:21:12:35      - - -
3 Idle        ALC1132A-51   -                  - - -
4 Active      VLC1124A-51   VLC1124A-51       1:21:12:13      - - -
ras# config
ras(config)# lcman slot 3 provision-type alc
ras(config)# exit
ras# show lcman
f/w version: V3.60(ABIZ.0)b2
id state      card type      provision type      uptime heat vol mon
--
1 Active      MSC1002GA      -                  1:21:13:50      - - -
2 Active      VOP1164A-61   VOP1164A-61       1:21:12:35      - - -
3 Init        ALC1132A-51   ALC1132A-51       - - -
4 Active      VLC1124A-51   VLC1124A-51       1:21:12:13      - - -

```

CHAPTER 24

Switch Features

24.1 ACL Commands

Use these commands to configure and apply Access Control List (ACL) profiles on the IES.

An ACL (Access Control List) profile allows the system to classify and perform actions on the incoming traffic. Each ACL profile consists of a rule and an action. ACL profiles let you configure filters to drop, limit, or modify (QoS fields) specific types of traffic. You can apply the ACL profiles to individual uplink interfaces, DSL ports, or the whole system.

Applying ACL Profiles

Rules applied to an individual port take priority over rules applied to the whole system. The priority of the rules for an individual port is not guaranteed, and the priority of the rules for whole system is not guaranteed.

This table describes the commands.

Table 222 ACL Commands Summary

COMMAND	DESCRIPTION	M	P
show interface system acl	Displays ACL rules applied to the whole system.	E	13
interface system	Enters the sub-command mode for configuring system-wide settings.	C	13
exit	Leaves the system-wide settings sub-command mode.	C	13
acl <acl-profile>	Uses the specified ACL profile for the system.	C	13
no acl <acl-profile>	Do not use the specified ACL profile for the system.	C	13
show interface ge-nni <portlist> acl	Displays ACL settings for the specified Gigabit Ethernet uplink interfaces. You can specify a single port <1>, all ports <*> or a list of ports <1,2>. You can also include a range of ports <1-2>.	E	13
interface ge-nni <portlist>	Enters the sub-command mode for configuring the specified Gigabit Ethernet uplink interfaces. You can specify a single port <1>, all ports <*> or a list of ports <1,2>. You can also include a range of ports <1-2>.	C	13
exit	Leaves the Gigabit Ethernet uplink port configuration.	C	13
acl <acl-profile>	Uses the specified ACL profile for the ports.	C	13
no acl <acl-profile>	Do not use the specified ACL profile for the ports.	C	13
show interface dsl <slot/ portlist> acl	Displays ACL settings for the specified DSL ports.	E	13
show interface fe <slot/portlist> packet-type	Displays packet type filtering settings for the specified FE ports.	E	13
interface dsl <slot/portlist>	Enters the sub-command mode for configuring the specified DSL ports.	C	13
exit	Leaves the DSL port configuration.	C	13
acl <acl-profile>	Uses the specified ACL profile for the ports.	C	13

Table 222 ACL Commands Summary (continued)

COMMAND	DESCRIPTION	M	P
<code>no acl <acl-profile></code>	Do not use the specified ACL profile for the ports.	C	13
<code>packet-type <uni-vlan> pppoe-only</code>	Configures packet type filtering for the specified UNI VLAN as PPPoE only. <i>uni-vlan</i> : 1-4093	C	13
<code>packet-type <uni-vlan> drop <packet-type-list></code>	Configures packet type filtering for the specified UNI VLAN to drop the specified packet types. <i>uni-vlan</i> : 1-4093 <i>packet-type-list</i> : list of pppoe, arp, ip, netbios, eapol, dhcp, and igmp; for example, ip, arp, pppoe, netbios	C	13
<code>no packet-type <uni-vlan></code>	Removes all packet type filtering for the specified UNI VLAN. In other words, accept all packet types. <i>uni-vlan</i> : 1-4093	C	13
<code>show interface fe <slot/portlist> acl</code>	Displays ACL settings for the specified FE ports.	E	13
<code>show interface fe <slot/portlist> packet-type</code>	Displays packet type filtering settings for the specified FE ports.	E	13
<code>interface fe <slot/portlist></code>	Enters the sub-command mode for configuring the specified FE ports.	C	13
<code>exit</code>	Leaves the FE port configuration.	C	13
<code>acl <acl-profile></code>	Uses the specified ACL profile for the ports.	C	13
<code>no acl <acl-profile></code>	Do not use the specified ACL profile for the ports.	C	13
<code>packet-type <uni-vlan> pppoe-only</code>	Configures packet type filtering for the specified UNI VLAN as PPPoE only. <i>uni-vlan</i> : 1-4093	C	13
<code>packet-type <uni-vlan> drop <packet-type-list></code>	Configures packet type filtering for the specified UNI VLAN to drop the specified packet types. <i>uni-vlan</i> : 1-4093 <i>packet-type-list</i> : list of pppoe, arp, ip, netbios, eapol, dhcp, and igmp; for example, ip, arp, pppoe, netbios	C	13
<code>no packet-type <uni-vlan></code>	Removes all packet type filtering for the specified UNI VLAN. In other words, accept all packet types. <i>uni-vlan</i> : 1-4093	C	13
<code>acl-profile <name></code>	Creates an ACL profile and enters the sub-command mode for configuring it. <i>name</i> : up to 31 printable characters	C	13
Use the following sub-commands to set the rules for the ACL profile.			
<code>ether-type <etype></code>	Specifies an Ethernet type. <i>etype</i> : Ethernet type in hexadecimal (0000-FFFF).	C	13
<code>source-mac <mac></code>	Specifies a source MAC.	C	13
<code>dest-mac <mac></code>	Specifies a destination MAC.	C	13
<code>source-oui <oui></code>	Specifies a source MAC Organization Unit Identifier (OUI). <i>oui</i> : 00:00:00-FF:FF:FF	C	13
<code>dest-oui <oui></code>	Specifies a destination MAC Organization Unit Identifier (OUI).	C	13

Table 222 ACL Commands Summary (continued)

COMMAND	DESCRIPTION	M	P
inner-vlan <vid>	Specifies an inner VLAN ID.	C	13
outer-vlan <vid>	Specifies an outer VLAN ID.	C	13
inner-pbit <pbit>	Specifies an inner VLAN priority bit. <i>pbit</i> : 0-7	C	13
outer-pbit <pbit>	Specifies an outer VLAN priority bit.	C	13
source-ip range <ip>/<mask>	Specifies a source IP range. <i>mask</i> : 16-32	C	13
dest-ip range <ip>/<mask>	Specifies a destination IP range.	C	13
source-ip <ip>	Specifies a source IP address.	C	13
dest-ip <ip>	Specifies a destination IP address.	C	13
protocol <protocol>	Specifies an IP protocol. <i>protocol</i> : 0-255	C	13
ip-precedence <precedence>	Specifies an IP precedence. <i>precedence</i> : 0-7	C	13
dscp <dscp>	Specifies an IP DSCP. <i>dscp</i> : 0-63	C	13
source-ipv6 <ipv6>	Specifies a source IPv6 address.	C	13
dest-ipv6 <ipv6>	Specifies a destination IPv6 address.	C	13
next-header <next-header>	Specifies an IPv6 next header. <i>next-header</i> : 0 ~ 255	C	13
traffic-class <traffic-class>	Specifies an IPv6 traffic class. <i>traffic-class</i> : 0 ~ 255	C	13
source-l4-port range <start-port> <end-port>	Specifies a layer 4 source port range. <i>start-port</i> : 0-65535 <i>end-port</i> : 0-65535	C	13
dest-l4-port range <start-port> <end-port>	Specifies a layer 4 destination port range.	C	13
source-l4-port <port>	Specifies a layer 4 source port. <i>port</i> : 0-65535	C	13
dest-l4-port <port>	Specifies an layer 4 destination port.	C	13
no change-qos	Disables changing the QoS level of matched packets.	C	13
no ether-type	Removes the Ethernet type from the profile.	C	13
no source-mac	Removes the source MAC from the profile.	C	13
no dest-mac	Removes the destination MAC from the profile.	C	13
no source-oui	Removes the source MAC OUI from the profile.	C	13
no dest-oui	Removes the destination MAC OUI from the profile.	C	13
no inner-vlan	Removes the inner VLAN ID from the profile.	C	13
no outer-vlan	Removes the outer VLAN ID from the profile.	C	13
no inner-pbit	Removes the inner VLAN priority bit from the profile.	C	13

Table 222 ACL Commands Summary (continued)

COMMAND	DESCRIPTION	M	P
no outer-pbit	Removes the outer VLAN priority bit from the profile.	C	13
no source-ip	Removes the source IP address or IP address range from the profile.	C	13
no dest-ip	Removes the destination IP address or IP address range from the profile.	C	13
no protocol	Removes the IP protocol from the profile.	C	13
no ip-precedence	Removes the IP precedence from the profile.	C	13
no dscp	Removes the IP DSCP from the profile.	C	13
no source-ipv6	Removes the source IPv6 address from the profile.	C	13
no dest-ipv6	Removes the destination IPv6 address from the profile.	C	13
no next-header	Removes the IPv6 next header from the profile.	C	13
no traffic-class	Removes the IPv6 traffic class from the profile.	C	13
no source-l4-port	Removes the source L4 port or L4 port range from the profile.	C	13
no dest-l4-port	Removes the destination L4 port or L4 port range from the profile.	C	13
Use the following sub-commands to set the actions for the ACL profile.			
change-qos <queue-id>	Changes the QoS level of matched packets. <i>queue-id</i> : 0-7 7:highest priority 0:lowest priority	C	13
drop	Discards packets that match the profile.	C	13
no drop	Disables dropping of matching packets.	C	13
rate-limit <rate-limit>	Limits the receiving rate for packets that match the profile. <i>rate-limit</i> : 32-100000 in kbps	C	13
no rate-limit	Disables rate limiting for matching packets.	C	13
change-inner-pbit <pbit>	Changes the inner VLAN inner priority bit of matching packets to the specified one.	C	13
no change-inner-pbit	Disables changing the inner VLAN inner priority bit of matching packets.	C	13
change-outer-pbit <pbit>	Changes the outer VLAN outer priority bit of matching packets.	C	13
no change-outer-pbit	Disables changing the outer VLAN outer priority bit of matching packets.	C	13
change-dscp <dscp>	Changes the IP DSCP of matching packets to the specified one. <i>dscp</i> : 0-63	C	13
no change-dscp	Disables changing the IP DSCP of matching packets.	C	13
change-traffic-class <traffic-class>	Changes the IPv6 traffic class of matching packets. <i>traffic-class</i> : 0 ~ 255	C	13
no change-traffic-class	Disables changing the IPv6 traffic class of matching packets.	C	13
exit	Leaves the ACL rule editing sub-command mode.	C	13
no acl-profile <name>	Removes the specified ACL profile.	C	13
show acl-rule [name]	Displays the specified ACL profile's settings.	E	13

Table 222 ACL Commands Summary (continued)

COMMAND	DESCRIPTION	M	P
<code>acl-profile field-priority</code> <code><index> <priority></code>	Configures the ACL field priority. <i>index</i> : 1~24 for field index. index 1: source MAC index 2: destination MAC index 3: source OUI index 4: destination OUI index 5: source IP address index 6: source IP range index 7: destination IP address index 8: destination IP range index 9: source IPv6 address index 10: destination IPv6 address index 11: source layer 4 port index 12: source layer 4 port range index 13: destination layer 4 port index 14: destination layer 4 port range index 15: outer VLAN index 16: inner VLAN index 17: outer priority bit index 18: inner priority bit index 19: Ether type index 20: next header index 22: traffic class index 23: DSCP index 24: protocol <i>priority</i> : 1~ff for field priority in hexadecimal	C	13
<code>no acl field-priority</code>	Resets the ACL field priority table.	C	13
<code>show acl field-priority</code>	Displays the ACL field priority table.	E	13

There are still some ACL commands related to multicast application. Please refer to [Table 238 on page 373](#) or search “acl multicast” directly.

24.1.1 Command Examples

Note: Before you can use an interface, you have to activate (provision) the corresponding slot. See [Section 23.1.1 on page 344](#) for how to activate a slot.

This example shows how to create an ACL profile named **EXAMPLE** to prioritize specific traffic. This example classifies SMTP packets (port **25** is the most common port used by SMTP) sending from a host with an IP address **192.168.1.100** and then sends the matched packets to queue **1**.

```

ras# config
ras(config)# acl-profile EXAMPLE
ras(config-acl-profile-EXAMPLE)# source-ip 192.168.1.100
ras(config-acl-profile-EXAMPLE)# source-l4-port range 25 26
ras(config-acl-profile-EXAMPLE)# change-qos 1
ras(config-acl-profile-EXAMPLE)# exit
ras(config)# exit
ras# write memory
saving configuration to flash...
ras#

```

24.2 Broadcast Storm Commands

Use these commands to limit the number of broadcast, multicast and destination lookup failure (DLF) packets (unknown unicast and multicast packets) the IES receives per second on the ports. When the number of broadcast, multicast and/or DLF packets reaches the maximum allowed per second, the IES discards subsequent packets. Enable this feature to reduce broadcast, multicast and/or DLF packets in your network. You can specify limits for DLF and broadcast packets.

The following table describes commonly used parameter notation for these commands.

Table 223 Broadcast Storm Command Parameters

NOTATION	DESCRIPTION
<i>rate</i>	2-100000 in kbps

The following section lists the commands for this feature.

Table 224 Broadcast Storm Commands Summary

COMMAND	DESCRIPTION	M	P
show storm-control	Displays the rate limits set for broadcast and DLF packets.	E	13
storm-control broadcast <rate>	Sets the rate limit for broadcast packets on the IES.	C	13
storm-control dlf <rate>	Sets the rate limit for DLF packets on the IES.	C	13

24.3 Daisy Chain Commands

Use the `daisychain` commands to set the IES to use one Gigabit Ethernet NNI as a downlink to connect to another daisy chained IES. The other Gigabit Ethernet uplink port connects to the Ethernet backbone. This is also called subtending. The daisy chain switch mode is recommended for use in a network topology that does not have loops. When you daisy chain multiple IESs, all except the last one in the chain must have daisy chain enabled.

You can enable daisy chain on one Gigabit Ethernet uplink port at a time. When you enable daisy chain, the daisy chain-enabled port serves as the subtending port (connect it to the downlink device). The IES treats a daisy chain-enabled Gigabit Ethernet uplink port as a downlink and follows the port

isolation setting. Daisy chain mode with port isolation enabled blocks direct communications between subscriber ports on an individual IES and the subscriber ports of the daisy chained IESs.

The following section lists the commands for this feature.

Table 225 Daisy Chain Commands Summary

COMMAND	DESCRIPTION	M	P
show daisychain	Displays the current daisy chain settings and status.	E	13
interface ge-nni <portlist>	Configures the specified Gigabit Ethernet uplink port. You can specify a single port <1> or <2>.	C	13
exit	Leaves the Gigabit Ethernet uplink port configuration.	C	13
daisychain	Enables daisy chain on the specified Gigabit Ethernet uplink port.	C	13
no daisychain	Disables daisy chain on the specified Gigabit Ethernet uplink port.	C	13

24.4 Forwarding Database Commands

Use these commands to configure the forwarding database settings and display the forwarding database address table. You can set the aging time, flush the address table, show the learned entries count, display the address table, display the entries for specific ports, UNI VLANs, untagged UNI VLANs, set the maximum number of MAC entries for specific ports, configure a static unicast MAC entry on a specific port and the VLAN it must use, and allow only static or static and dynamic MAC addresses on a specific port.

This table describes the commands.

Table 226 Forwarding Database Commands Summary

COMMAND	DESCRIPTION	M	P
fdb aging-time <aging-time>	Sets the forwarding database aging time in seconds. <i>aging-time</i> : 10-3600 in seconds	C	13
show fdb aging-time	Displays the forwarding database aging time.	E	13
fdb disable-anti-spoofing	Turns off MAC spoofing protection. The IES issues an alarm and an SNMP trap when it learns a MAC address on a second UNI port. The IES still forwards packets from other ports destined for the spoofed MAC to the later UNI port.	C	13
fdb disable-spoofing-action	Turns off anti-spoofing action so the IES does not shut down UNI ports upon which it detects spoofing.	C	13
no fdb disable-anti-spoofing	Turns on MAC spoofing protection. The IES issues an alarm and an SNMP trap when it learns a MAC address on a second UNI port. The subscriber device with a spoofed MAC cannot send packets to other ports. If anti-spoofing action is also turned on, anti-spoofing deactivates the second UNI port upon which it detects a MAC address.	C	13
no fdb disable-spoofing-action	Turns on anti-spoofing action so the IES deactivates UNI ports upon which it detects MAC address spoofing. For DSL ports, use the <code>interface dsl <slot/portlist></code> and <code>active</code> commands to re-activate the UNI port. Note: Anti-spoofing must also be enabled for this to take effect.	C	13

Table 226 Forwarding Database Commands Summary (continued)

COMMAND	DESCRIPTION	M	P
show fdb spoofing	Displays whether anti-spoofing is enabled or disabled.	E	13
show fdb spoofing-action	Displays whether anti-spoofing action is enabled or disabled.	E	13
no fdb address-table	Flushes the forwarding database address table.	E	13
no fdb address-table interface <slot/portlist>	Flushes the forwarding database address table for the specified ports.	E	13
no fdb address-table interface ge-nni <portlist>	Flushes the forwarding database address table for the specified Gigabit Ethernet uplink ports.	E	13
show fdb address-table count	Displays the number of learned entries in the forwarding database table.	E	13
show fdb address-table count <uni-vlan list>	Displays the number of learned entries in the forwarding database table for the specified UNI VLANs.	E	13
show fdb address-table count uni-untag	Displays the number of learned entries in the forwarding database table for untagged UNI VLANs.	E	13
show fdb address-table all	Displays all the learned entries in the forwarding database table.	E	1
show fdb address-table vlan <uni-vlan list>	Displays the forwarding database address table for the specified UNI VLANs. <i>uni-vlan list</i> : list of (1-4093)	E	1
show fdb address-table uni-untag	Displays the forwarding database table address table for untagged UNI VLANs.	E	1
show interface dsl <slot/portlist> fdb address-table	Displays the forwarding database address table for the specified ports.	E	13
show interface fe <slot/portlist> fdb address-table	Displays the forwarding database address table for the specified ports.	E	13
interface dsl <slot/portlist>	Configures the specified DSL ports.	C	13
fdb max-count <max-count>	Configures the maximum number of forwarding database MAC entries for the specified ports.	C	13
fdb uni-vlan-max-count <max-count> uni-vlan <uni-vlan>	Configures the maximum number of forwarding database MAC entries for the specified UNI VLAN on the specified ports. <i>mac-count</i> : 1 ~ 32 <i>uni-vlan</i> : 1 ~ 4093	C	13
no fdb uni-vlan-max-count <uni-vlan>	Removes the maximum number of forwarding database MAC entries limitation for the specified UNI VLAN on the specified ports.	C	13

Table 226 Forwarding Database Commands Summary (continued)

COMMAND	DESCRIPTION	M	P
<code>fdb mac <mac> [vlan <vlan>]</code>	Configures a static MAC entry on the specified ports. You can also specify the VLAN it must use. <i>mac</i>: unicast MAC address <i>vlan</i>: 1 ~ 4093 VLAN mode <vlan> ----- Trunk uni-vlan uni-vid Trunk uni-untag svlan Trunk etype(S) svlan Trunk etype(S+C) cvlan Translation uni-vid Transparent not supported TLS not supported	C	13
<code>no fdb mac <mac> [vlan <vlan>]</code>	Removes a static MAC entry from the specified ports. <i>mac</i>: unicast MAC address <i>vlan</i>: 1 ~ 4093 VLAN mode <vlan> ----- Trunk uni-vlan uni-vid Trunk uni-untag svlan Trunk etype(S) svlan Trunk etype(S+C) cvlan Translation uni-vid Transparent not supported TLS not supported	C	13
<code>fdb static-mac-only</code>	Allows only static MAC addresses.	C	13
<code>no fdb static-mac-only</code>	Allows both static and dynamic MAC addresses.	C	13
<code>interface fe <slot/portlist></code>	Configures the specified FE ports.	C	13
<code>fdb max-count <max-count></code>	Configures the maximum number of forwarding database MAC entries for the specified ports.	C	13
<code>fdb uni-vlan-max-count <max-count> uni-vlan <uni-vlan></code>	Configures the maximum number of forwarding database MAC entries for the specified UNI VLAN on the specified ports. <i>mac-count</i>: 1 ~ 32 <i>uni-vlan</i>: 1 ~ 4093	C	13
<code>no fdb uni-vlan-max-count <uni-vlan></code>	Removes the maximum number of forwarding database MAC entries limitation for the specified UNI VLAN on the specified ports.	C	13

Table 226 Forwarding Database Commands Summary (continued)

COMMAND	DESCRIPTION	M	P
<code>fdb mac <mac> [vlan <vlan>]</code>	Configures a static MAC entry on the specified ports. You can also specify the VLAN it must use. <i>mac</i>: unicast MAC address <i>vlan</i>: 1 ~ 4093 VLAN mode <vlan> ----- Trunk uni-vlan uni-vid Trunk uni-untag svlan Trunk etype(S) svlan Trunk etype(S+C) cvlan Translation uni-vid Transparent not supported TLS not supported	C	13
<code>no fdb mac <mac> [vlan <vlan>]</code>	Removes a static MAC entry from the specified ports. <i>mac</i>: unicast MAC address <i>vlan</i>: 1 ~ 4093 VLAN mode <vlan> ----- Trunk uni-vlan uni-vid Trunk uni-untag svlan Trunk etype(S) svlan Trunk etype(S+C) cvlan Translation uni-vid Transparent not supported TLS not supported	C	13
<code>fdb static-mac-only</code>	Allows only static MAC addresses.	C	13
<code>no fdb static-mac-only</code>	Allows both static and dynamic MAC addresses.	C	13
<code>show interface dsl <slot/portlist> fdb</code>	Displays the forwarding database settings and maximum MAC entry counts for the specified DSL ports.	E	13
<code>show interface fe <slot/portlist> fdb</code>	Displays the forwarding database settings and maximum MAC entry counts for the specified FE ports.	E	13

24.5 GE Uplink Commands

Use these commands to configure the Gigabit Ethernet uplink ports.

This table describes the commands.

Table 227 GE Uplink Commands Summary

COMMAND	DESCRIPTION	M	P
<code>show interface ge-nni <portlist></code>	Displays the configuration of the specified Gigabit Ethernet uplink ports. You can specify a single port <1>, all ports <*> or a list of ports <1,2>. You can also include a range of ports <1-2>.	E	13
<code>interface ge-nni <portlist></code>	Configures the specified Gigabit Ethernet uplink ports. You can specify a single port <1>, all ports <*> or a list of ports <1,2>. You can also include a range of ports <1-2>.	C	13
<code>exit</code>	Leaves the Gigabit Ethernet uplink port configuration.	C	13
<code>inactive</code>	Disables the Gigabit Ethernet uplink ports.	C	13
<code>no inactive</code>	Enables the Gigabit Ethernet uplink ports.	C	13
<code>name <port-name-string></code>	Sets a name of up to 31 printable characters for the Gigabit Ethernet uplink ports.	C	13
<code>no name</code>	Resets the name of the port to the default.	C	13
<code>speed-duplex auto 10-half 10-full 100-half 100-full 1000-full 1000-fiber</code>	Configures the Gigabit Ethernet port's speed and duplex mode. The default is auto. auto: auto negotiation 10-half: fixed to 10Base-T half duplex 10-full: fixed to 10Base-T full duplex 100-half: fixed to 100Base-TX half duplex 100-full: fixed to 100Base-TX full duplex 1000-full: fixed to 1000Base-T full duplex 1000-fiber: fixed to 1000Base-X full duplex	C	13
<code>no speed-duplex</code>	Resets the Gigabit Ethernet port's speed and duplex mode to the default.	C	13
<code>clear interface ge-nni <portlist> performance</code>	Clears the current or historical 15-minutes and 1-day interface status for the specified Gigabit Ethernet uplink ports. You can specify a single port <1>, all ports <*> or a list of ports <1,2>. You can also include a range of ports <1-2>.	E	13
<code>clear interface ge-nni <portlist> statistics</code>	Clears packet statistics for the specified port. You can specify a single port <1>, all ports <*> or a list of ports <1,2>. You can also include a range of ports <1-2>.	E	13
<code>show interface ge-nni <portlist> statistics</code>	Displays packet statistics for the specified port. You can specify a single port <1>, all ports <*> or a list of ports <1,2>. You can also include a range of ports <1-2>.	E	13
<code>show interface ge-nni <portlist> status</code>	Displays the current interface status for the specified ports. You can specify a single port <1>, all ports <*> or a list of ports <1,2>. You can also include a range of ports <1-2>.	E	13
<code>show interface ge-nni <portlist> performance current 15-min 1-day</code>	Displays the current or historical 15-minutes and 1-day interface status for the specified Gigabit Ethernet uplink ports. You can specify a single port <1>, all ports <*> or a list of ports <1,2>. You can also include a range of ports <1-2>.	E	13
<code>show interface ge-nni <portlist> ddmi</code>	Displays current DDMI (Digital Diagnostics Monitoring Interface) status on the specified ports. You can specify a single port <1>, all ports <*> or a list of ports <1,2>. You can also include a range of ports <1-2>.	E	13

24.6 Link Aggregation Commands

Use these commands to configure the IEEE 802.3ad link aggregation settings for the Gigabit Ethernet (GE) uplink ports. Use Link Aggregate Control Protocol (LACP) to have the IES dynamically create and manage the trunk group.

This table describes the commands.

Table 228 Link Aggregation Commands Summary

COMMAND	DESCRIPTION	M	P
<code>show dot3ad</code>	Displays the current link aggregation mode and status.	E	13
<code>dot3ad static lacp</code>	Configures and enables the Gigabit Ethernet uplink ports' IEEE 802.3ad mode. <i>static</i> : statically aggregate the GE ports <i>lacp</i> : have LACP aggregate and control the GE ports	C	13
<code>no dot3ad</code>	Turns off link aggregation.	C	13
<code>dot3ad lacp-priority <priority></code>	Configures the LACP system priority. <i>priority</i> : 0~65535. Default 0. The switch with the lowest system priority (and lowest port number if system priority is the same) becomes the LACP "server". The LACP "server" controls the operation of LACP setup. Enter a number to set the priority of an active port using Link Aggregate Control Protocol (LACP). The smaller the number, the higher the priority level.	C	13
<code>no dot3ad lacp-priority</code>	Resets the LACP priority to the default value.	C	13
<code>dot3ad lacp-timeout long short</code>	Configures the LACP status packet exchange interval. Set either <i>short</i> (1 second) or <i>long</i> (30 seconds). Default <i>long</i> . Timeout is the time interval between the individual port exchanges of LACP packets in order to check that the peer port in the trunk group is still up. If a port does not respond after three tries, it is deemed to be "down" and removed from the trunk. Set a short timeout (one second) for busy trunked links to remove disabled ports from the trunk group as soon as possible.	C	13
<code>no dot3ad lacp-timeout</code>	Resets the LACP timeout to the default value.	C	13
<code>dot3ad load-distribution <field-combination></code>	Specifies which packet fields the load sharing mechanism uses. <i>field-combination</i> : can be one of the following values: <i>src-mac</i> : Distributes the traffic load based on the source MAC address of the incoming packets. <i>dst-mac</i> : Distributes the traffic load based on the destination MAC address of the incoming packets. <i>src-dst-mac</i> : Distributes the traffic load based on both the source and destination MAC address of the incoming packets. <i>src-ip</i> : Distributes the traffic load based on the source IP address of the incoming packets. <i>dst-ip</i> : Distributes the traffic load based on the destination IP address of the incoming packets. <i>src-dst-ip</i> : Distributes the traffic load based on both the source and destination IP address of the incoming packets. <i>src-dst-ipmac</i> : Distributes the traffic load based on both the source and destination IP and MAC address of the incoming packets.	C	13

24.7 Loop Guard Commands

Use these commands to configure the IES to guard against loops on the edge of your network. Loop guard allows you to configure the IES to shut down a port if it detects that packets sent out on that port loop back to the IES. While Spanning Tree Protocol (STP) can help prevent loops in the core of your network, it cannot prevent loops that occur on the edge of your network.

Loop guard handles loop problems on the edge of your network. This can occur when a port is connected to a IES that is in a loop state. Loop state occurs as a result of human error. It happens when two ports on a switch are connected with the same cable. When a switch in loop state sends out broadcast messages the messages loop back to the switch and are re-broadcast again and again causing a broadcast storm.

If a switch (not in loop state) connects to a switch in loop state, then it will be affected by the switch in loop state in the following way:

- It will receive broadcast messages sent out from the switch in loop state.
- It will receive its own broadcast messages that it sends out as they loop back. It will then re-broadcast those messages again.

The loop guard feature checks to see if a loop guard enabled port is connected to a switch in loop state. This is accomplished by periodically sending a probe packet and seeing if the packet returns on the same port. If this is the case, the IES will shut down the port connected to the switch in loop state.

Loop guard can be enabled on xDSL and FE ports.

Note: After resolving the loop problem on your network use the commands to re-activate the disabled port.

This table describes the commands.

Table 229 Loop Guard Commands Summary

COMMAND	DESCRIPTION	M	P
<code>show interface dsl <slot/portlist> loopguard</code>	Displays whether loop guard is enabled or disabled and packet statistics on the specified DSL ports.	E	1
<code>show interface dsl <slot/portlist> loopguard policy</code>	Displays the loop guard policy on the specified DSL ports.	E	1
<code>show interface dsl <slot/portlist> loopguard recover-time</code>	Displays the recover time for the dynamic loopguard policy on the specified DSL ports.	E	1
<code>clear interface dsl <slot/portlist> loopguard</code>	Clears loop guard statistics (packet counter) on the specified DSL ports.	E	13
<code>show interface dsl <slot/portlist> loopguard uni-vlan</code>	Displays the unicast VLAN tag that the specified DSL ports use for the loop guard detection packets.	E	1
<code>interface dsl <slot/portlist></code>	Enters the sub-command mode for configuring the specified DSL ports.	C	13
<code>active</code>	Enables the specified ports on the IES. Use this to manually re-activate a port disabled by loop guard.	C	13
<code>loopguard</code>	Enables loop guard.	C	13

Table 229 Loop Guard Commands Summary (continued)

COMMAND	DESCRIPTION	M	P
loopguard policy fix dynamic	Sets which action to take when a loop condition is detected on one of the specified DSL ports. fix: shut down the port, you need to enable the port by command dynamic: shutdown the port, and recover it after the recover time	C	13
loopguard recover-time <time>	Configures the recover time for the dynamic loop guard policy. time: 60-600 in seconds	C	13
loopguard uni-vlan <vid> [pbit <pbit>]	Tells the IES what VID (and optionally IEEE 802.1p priority bit) to look for to detect loopguard packets. Detecting the loopguard packets fails if the VLAN mode you configured (through vlan trunk for example) does not match the loopguard VID. vid: 1 ~ 4093 pbit: 0~7, default 6	C	13
no loopguard uni-vlan	Removes the VID and IEEE 802.1p priority bit settings that the IES uses to detect loopguard packets.	C	13
no loopguard	Disables loop guard.	C	13
show interface fe <slot/ portlist> loopguard	Displays whether loop guard is enabled or disabled and packet statistics on the specified FE ports.	E	1
show interface fe <slot/ portlist> loopguard policy	Displays the loop guard policy on the specified FE ports.	E	1
show interface fe <slot/ portlist> loopguard recover- time	Displays the recover time for the dynamic loopguard policy on the specified FE ports.	E	1
clear interface fe <slot/ portlist> loopguard	Clears loop guard statistics (packet counters) on the specified FE ports.	E	13
show interface fe <slot/ portlist> loopguard uni-vlan	Displays the unicast VLAN tag that the specified FE ports use for the loop guard detection packets.	E	1
interface fe <slot/portlist>	Enters the sub-command mode for configuring the specified FE ports.	C	13
active	Enables the specified ports on the IES. Use this to manually re-activate a port disabled by loop guard.	C	13
loopguard	Enables loop guard.	C	13
loopguard policy fix dynamic	Sets which action to take when a loop condition is detected on one of the specified FE ports. fix: shut down the port, you need to enable the port by command dynamic: shutdown the port, and recover it after the recover time	C	13
loopguard recover-time <time>	Configures the recover time for the dynamic loop guard policy. time: 60-600 in seconds	C	13
loopguard uni-vlan <vid> [pbit <pbit>]	Tells the IES what VID (and optionally IEEE 802.1p priority bit) to look for to detect loopguard packets. Detecting the loopguard packets fails if the VLAN mode you configured (through vlan trunk for example) does not match the loopguard VID. vid: 1 ~ 4093 pbit: 0~7, default 6	C	13

Table 229 Loop Guard Commands Summary (continued)

COMMAND	DESCRIPTION	M	P
no loopguard uni-vlan	Removes the VID and IEEE 802.1p priority bit settings that the IES uses to detect loopguard packets.	C	13
no loopguard	Disables loop guard.	C	13

24.7.1 Command Examples

This example shows port 1 on slot 2 is disabled, then enables the port and loop guard on it as well. It also sets the IES to shut down port 1 if it detects a loop on it on VLAN 100 and wait 300 seconds before reactivating it. This example also shows whether the port has linked up with the connected CPE port, loop guard status, sending and receiving packet statistics, and the date and time this port was last shut down.

```

ras# show interface dsl 2/1 config
slot port enable          name
-----
 2    1    -
template mapping
slot port          line-template          alarm-template
-----
 2    1    DEFVAL          DEFVAL
ras# config
ras(config)# interface dsl 2/1
ras(config-interface-dsl-2/1)# active
ras(config-interface-dsl-2/1)# loopguard
ras(config-interface-dsl-2/1)# loopguard policy dynamic
ras(config-interface-dsl-2/1)# loopguard uni-vlan 100
ras(config-interface-dsl-2/1)# loopguard recover-time 300
ras(config-interface-dsl-2/1)# exit
ras(config)# exit
ras# show interface dsl 2/1 loopguard
LoopGuard Status: Enable
Port  Port      LoopGuard  Total      Total      Bad      Shutdown
No   Status      Status      TxPkts     RxPkts     Pkts     Time
-----
2/1  Inactive      Enable       0          0          0      00:00:00 Thu. Jan. 01, 197
ras#

```

24.8 Port Isolation Commands

Use these commands for isolating subscriber ports. Isolation blocks communications between subscriber ports. You do not need to configure the VLAN to isolate subscribers. If you do not block communications between subscriber ports, you can use isolation VLAN block communications between subscribers in different VLANs.

This table describes the commands.

Table 230 Port Isolation Commands Summary

COMMAND	DESCRIPTION	M	P
isolation inactive	Allows communications between subscriber ports.	C	13
no isolation inactive	Blocks communications between subscriber ports.	C	13

Table 230 Port Isolation Commands Summary (continued)

COMMAND	DESCRIPTION	M	P
<code>isolation vlan <vid></code>	Adds an isolated VLAN. <i>vid:</i> 1-4093	C	13
<code>no isolation vlan <vid></code>	Removes an isolated VLAN. <i>vid:</i> 1-4093	C	13
<code>show isolation</code>	Displays the isolation settings between subscriber ports.	E	13

24.9 RSTP Commands

Use these commands to configure the IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) settings for the Gigabit Ethernet (GE) uplink ports. Use RSTP to detect and break network loops and provide backup links for the IES's GE uplink ports.

This table describes the commands.

Table 231 RSTP Commands Summary

COMMAND	DESCRIPTION	M	P
<code>show rstp</code>	Displays the current RSTP settings and status.	E	13
<code>rstp priority <priority></code>	Configures the RSTP bridge priority of the IES. The switch with the highest priority (lowest numeric value) becomes the RSTP root switch. If all switches have the same priority, the switch with the lowest MAC address becomes the root switch. <i>priority:</i> 0~61440 in steps of 4096 (0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344 or 61440) default: 61440	C	13
<code>no rstp priority</code>	Resets the RSTP priority to the default value.	C	13
<code>rstp timer hellotime <hellotime> maxage <maxage> fwdelay <forward delay></code>	Configures the RSTP bridge timer. <i>hellotime:</i> The time interval (1-10 seconds) between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. If an RSTP-aware device does not get a Hello BPDU after three Hello Times pass (or the Max Age), the device assumes that the link to the neighboring bridge is down. <i>maxage:</i> The maximum time (4-30 seconds) the IES can wait without receiving a BPDU before attempting to reconfigure. <i>forward delay:</i> The maximum time (4-30 seconds) the IES waits before changing states. This delay gives other switches time to receive information about topology changes before the IES starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. $\text{maxage} > (2 \times (\text{hellotime} + 1))$ $\text{maxage} < (2 \times (\text{fwdelay} - 1))$ defaults: <i>hellotime:</i> 2, <i>maxage:</i> 20, <i>forward delay:</i> 15	C	13
<code>no rstp timer</code>	Resets the RSTP bridge timer to the default value.	C	13

Table 231 RSTP Commands Summary (continued)

COMMAND	DESCRIPTION	M	P
<code>interface ge-nni <portlist></code>	Configures the specified Gigabit Ethernet uplink ports. You can specify a single port <1>, all ports <*> or a list of ports <1,2>. You can also include a range of ports <1-2>.	C	13
<code>exit</code>	Leaves the Gigabit Ethernet uplink port configuration.	C	13
<code>rstp</code>	Enables RSTP on the specified Gigabit Ethernet uplink port.	C	13
<code>no rstp</code>	Disables RSTP on the specified Gigabit Ethernet uplink port.	C	13
<code>rstp pathcost <path-cost></code>	Configures the Gigabit Ethernet uplink port RSTP path cost in the spanning tree. A smaller number means a lower path cost. For paths with the same priority, the switch will select the lower numbered interface first. <i>path-cost</i> : 1~65535, default is 4	C	13
<code>no rstp pathcost</code>	Resets the Gigabit Ethernet uplink port RSTP pathcost to the default value.	C	13
<code>rstp priority <priority></code>	Configures the Gigabit Ethernet uplink port RSTP priority in the spanning tree. When a loop occurs and two root ports have the same cost, the port with higher priority (lower numerical value) becomes the root port and the other port becomes an alternate port. For ports with the same priority, the switch will select the lower numbered interface first. <i>priority</i> : 0~240 in steps of 16, default is 128	C	13
<code>no rstp priority</code>	Resets the Gigabit Ethernet uplink port RSTP priority to the default value.	C	13
<code>show interface ge-nni <portlist> rstp</code>	Displays the RSTP configuration for the specified Gigabit Ethernet uplink ports. You can specify a single port <1>, all ports <*> or a list of ports <1,2>. You can also include a range of ports <1-2>.	E	13

24.10 Mirror Commands

Use these commands to copy a traffic flow for one or more ports to a monitor port so that you can examine the traffic on the monitor port without interference.

24.10.1 Mirror Commands Summary

The following table describes commonly used parameter notation for these commands.

Table 232 mirror command parameters

NOTATION	DESCRIPTION
<i>slot</i>	This is the number of a slot (2-5).
<i>srcport</i>	This is the number of a DSL port (1-32) from which traffic flow is copied.
<i>dstport</i>	This is the number of a DSL port (1-32) to which traffic flow is copied.
<i>mode</i>	This is what traffic the port mirroring applies, for incoming (ingress), outgoing (egress) or both incoming and outgoing (both) traffic.
<i>port</i>	This is an uplink GE port, 1-2.
<i>vpi/vci</i>	The VPI (Virtual Path Indicator) and VCI (Virtual Channel Indicator) of an individual PVC (Permanent Virtual Circuit). The VPI setting can be 0 to 255. The VCI setting can be 32 to 65535.

The following section lists the commands for this feature.

Table 233 mirror command summary

COMMAND	DESCRIPTION	M	P
mirror interface ge-nni <srcport> interface ge-nni <dstport> mode <mode>	Mirrors the specified traffic from an uplink GE port to another. <i>srcport</i> : This is the number of an uplink GE port (1-2) from which traffic flow is copied. <i>dstport</i> : This is the number of another uplink GE port (1-2) to which traffic flow is copied.	C	13
show mirror	Displays all port mirroring settings.	E	3
no mirror interface ge-nni <port>	Disables port mirroring on the specified uplink GE port.	C	13
no mirror interface fe <slot/srcport>	Disables port mirroring on the specified DSL port.	C	13
show mirror interface ge-nni <port>	Displays the port mirroring settings for the specified uplink GE port.	E	3
show mirror interface fe <slot/srcport>	Displays the port mirroring settings for the specified DSL port.	E	3

24.10.2 Command Examples

This example enables port mirroring and copies outgoing traffic from DSL slot 2 port 1 to uplink GE port 1.

```
sysname# configure
sysname(config)# mirror interface dsl 2/1 interface ge-nni 1 mode egress
sysname(config)# exit
sysname#
```

CHAPTER 25

ADSL

Use these commands to configure ATM virtual circuits (VCs) on DSL ports. You can then use the commands in other chapters to apply settings like QoS, Transparent LAN Service (VLAN TLS), VLAN translation and aggregation, transparent VLAN, and VLAN trunking to the virtual circuits.

ATM

Asynchronous Transfer Mode (ATM) is a networking technology that provides high-speed data transfer. ATM uses fixed-size packets of information called cells. With ATM, a high QoS (Quality of Service) can be guaranteed.

Permanent Virtual Circuits

A Permanent Virtual Circuit (PVC) is a logical point-to-point circuit between sites. PVCs are low-delay circuits because routing decisions do not need to be made along the way. Permanent means that the circuit is pre-programmed by the carrier as a path through the network. It does not need to be set up or torn down for each session. PVCs are also called virtual channels.

The system can handle multiple IEEE 802.1p priority queues on a single PVC. You can also define up to eight PVCs on a DSL port and use them for different services or levels of service. You set the PVID that is assigned to untagged frames received on each channel. You also set an IEEE 802.1p priority for each of the PVIDs. In this way you can assign different priorities to different channels (and consequently the services that get carried on them or the subscribers that use them).

For example, you want to give high priority to voice service on one of the ADSL ports. First configure a static VLAN on the system for voice on the port. Then do the following:

- Configure a channel on the port for voice service.
- Set the channel to use the PVID of the static VLAN you configured.
- Assign the channel a high priority.

LLC

LLC is a type of encapsulation where one VC (Virtual Circuit) carries multiple protocols with each packet header containing protocol identifying information. Despite the extra bandwidth and processing overhead, this method may be advantageous if it is not practical to have a separate VC for each carried protocol, for example, if charging heavily depends on the number of simultaneous VCs.

VC Mux

VC Mux is a type of encapsulation where, by prior mutual agreement, each protocol is assigned to a specific virtual circuit, for example, VC1 carries IP, VC2 carries IPX, and so on. VC-based multiplexing may be dominant in environments where dynamic creation of large numbers of ATM VCs is fast and economical.

25.1 ATM VC Commands Summary

This table describes the commands.

Table 234 ATM VC Commands Summary

COMMAND	DESCRIPTION	M	P
<code>show interface dsl <slot/portlist> atm-vc</code>	Displays the ATM VC configuration on the specified DSL ports.	E	13
<code>interface dsl <slot/portlist></code>	Enters the sub-command mode for configuring the specified DSL ports.	C	13
<code>exit</code>	Leaves the DSL port configuration.	C	13
<code>atm-vc <vpi/vci> llc vc priority <priority> [mvlan]</code>	Adds or configures the specified ATM VC on the DSL ports. llc: LLC encapsulation vc: VC-MUX encapsulation mvlan: Include this to have the specified ATM VC join MVLAN.	C	13
<code>atm-vc <vpi/vci> llc vc priority <priority> pvid <vlan> pri <pbit> [mvlan]</code>	Adds or configures the specified ATM VC and adds the VC to VLAN trunk untagged mode. vpi: 0-255 vci: 32-65535 llc: LLC encapsulation vc: VC-MUX encapsulation priority: 0-7 vlan: 1-4093 pbit: 0-7 mvlan: join MVLAN or not Note: Only <priority>, <vlan>, and <pbit> can be modified.	C	13
<code>no atm-vc <vpi>/<vci></code>	Removes the specified ATM VC from the DSL ports.	C	13

CHAPTER 26

DHCP

Use these commands to configure DHCP settings including enabling or disabling transparent DHCP on specific VLANs; configure DHCP L2 Agent settings including options 18, 37, and 82 for specific VLANs, configuring DHCP snooping database overflow handling; enabling, disabling, and displaying DHCP snooping IP-MAC binding for specific DSL ports.

DHCP Relay Agent Information Option

The system can add information to DHCP requests that it relays to a DHCP server. This helps provide authentication about the source of the requests. You can also specify additional information for the system to add to the DHCP requests that it relays to the DHCP server. Please refer to RFC 3046 for more details. The DHCP relay agent information feature adds an Agent Information field to the option 18, 37, or 82 field of the DHCP headers of client TCP/IP configuration request frames that the IES relays to a DHCP server.

The following table describes commonly used parameter notation for these commands.

Table 235 DHCP Command Parameters

NOTATION	DESCRIPTION
<i>info</i>	The option 18 circuit ID, option 37 remote ID, or option 82 circuit ID format. It can use the following components: special characters except % => ~`!@#\$%^&*()-=_+{}<>?,./ %%: equals character % %0x00-%0xFF: represents byte value %pname: configured port name %pid: port index %chvpi: channel VPI %chvci: channel VCI %chid: channel ID, UNI VLAN for Ethernet, VPI.VCI for ATM %slotid: slot index of the logic port %svlan: SVLAN ID which DHCP client runs on %cvlan: CVLAN ID which DHCP client runs on %hname: host device name %cmac1: MAC address of a DHCP client, in XX:XX:XX:XX:XX:XX format where X=0-F %cmac2: MAC address of a DHCP client in XXXXXXXXXXXX format where X=0-F %cmac3: MAC address of a DHCP client in Bytes %dmac1: MAC address of the host device in XX:XX:XX:XX:XX:XX format where X=0-F %dmac2: MAC address of the host device in XXXXXXXXXXXX format where X=0-F %dmac3: MAC address of host device in Bytes %phtype: ATM: atm Ethernet: eth %hmodel: model name of the host device %fwid: host device firmware ID %blank: blank character

This table describes the commands.

Table 236 DHCP Commands Summary

COMMAND	DESCRIPTION	M	P
<code>dhcp transparent vlan <vid></code>	Enables transparent DHCP packets to have the IES bypass all DHCP packets (Discover, Offer, Request, ACK) on the specified VLAN. The IES does not check and record any information for DHCP packets. DHCP transparent and L2 Agent cannot be enabled at the same time in a VLAN.	C	13
<code>no dhcp transparent vlan <vid></code>	Disables transparent DHCP packets on the specified VLAN.	C	13
<code>dhcp l2agent vlan <vid></code>	Enables DHCP L2 Agent to have the IES only accept DHCP requests on the specified VLAN from the downlink network. Other DHCP packets, such as DHCP Offer, will be dropped. This can help prevent Denial-Of-Service (DOS) attacks through DHCP. DHCP transparent and L2 Agent cannot be enabled at the same time in a VLAN.	C	13

Table 236 DHCP Commands Summary (continued)

COMMAND	DESCRIPTION	M	P
no dhcp l2agent vlan <vid>	Disables DHCP L2 Agent on the specified VLAN.	C	13
dhcp l2agent vlan <vid> ldra	Enables DHCP L2 Agent Lightweight DHCPv6 Relay Agent (LDRA) function on the specified VLAN. Lightweight DHCPv6 Relay Agent (LDRA) adds information to client DHCPv6 requests before forwarding them to the DHCPv6 server. Use it to add information such as this system's host name and the slot, subscriber port, and PVC from which the request was received.	C	13
no dhcp l2agent vlan <vid> ldra	Disables DHCP L2 Agent LDRA function on the specified VLAN. This has the system forward DHCPv6 requests for a VLAN without adding information.	C	13
dhcp l2agent opt18-interface-id vlan <vid> option-info <info>	Configures the DHCP L2 Agent option 18 interface ID format on the specified VLAN. Option 18 is required for LDRA. Specify the Interface ID information to add to the client DHCPv6 requests forwarded for a VLAN to identify the interface which received the client message.	C	13
no dhcp l2agent opt18-interface-id vlan <vid>	Disables the DHCP L2 Agent option 18 interface ID on the specified VLAN.	C	13
dhcp l2agent opt37-remote-id vlan <vid> option-info <info>	Configures the DHCP L2 Agent option 37 remote ID format on the specified VLAN. The required option 18 can only add up to 127 characters of information about the DHCPv6 requests forwarded for this VLAN. Use option 37 if you need to add extra information beyond what you configure for option 18. Option 37 (Remote ID Info) is the DHCPv6 equivalent for the Dynamic Host Configuration Protocol for IPv4 (DHCPv4) Relay Agent Option's Remote-ID suboption.	C	13
no dhcp l2agent opt37-remote-id vlan <vid>	Disables the DHCP L2 Agent option 37 remote ID on the specified VLAN.	C	13
dhcp l2agent opt82-circuit-id vlan <vid> option-info <info>	Configures the DHCP L2 Agent option 82 circuit ID format on the specified VLAN. Use this command to have the IES add the originating port numbers to DHCP requests in the specified VLAN. <i>info</i> : up to 127 ASCII characters of additional information for the IES to add to the DHCP requests that it relays to a DHCP server. See Table 235 on page 367 for more information.	C	13
no dhcp l2agent opt82-circuit-id vlan <vid>	Disables the DHCP L2 Agent option 82 circuit ID on the specified VLAN.	C	13
dhcp l2agent opt82-remote-id vlan <vid> option-info <info>	Configures the DHCP L2 Agent option 82 remote ID format on the specified VLAN. Use this command to have the IES add the remote ID to DHCP requests in the specified VLAN. <i>info</i> : up to 127 ASCII characters of additional information for the IES to add to the DHCP requests that it relays to a DHCP server. See Table 235 on page 367 for more information.	C	13
no dhcp l2agent opt82-remote-id vlan <vid>	Disables the DHCP L2 Agent option 82 remote ID on the specified VLAN.	C	13
show dhcp vlan <vid>	Displays the DHCP L2 Agent settings (on the specified VLAN). <i>vid</i> : 1-4093 or * for all VLANs	E	13

Table 236 DHCP Commands Summary (continued)

COMMAND	DESCRIPTION	M	P
dhcp l2agent snooping max-lease overflow-mode deny-new- lease deny-oldest-lease	Configures the DHCP snooping database overflow handling mode. deny-new-lease: a new lease is denied deny-oldest-lease: the oldest lease is removed	C	13
interface dsl <slot/portlist>	Enters the sub-command mode for configuring the specified DSL ports.	C	13
dhcp l2agent snooping ip-mac-binding	Enables IP-MAC binding on the specified DSL ports.	C	13
no dhcp l2agent snooping ip-mac-binding	Disables DHCP snooping IP-MAC binding on the specified DSL ports.	C	13
dhcp l2agent snooping max-lease <lease-count>	Configures the DHCP Snooping database max lease count for the specified DSL ports. lease-count: 1-32	C	13
show interface dsl <slot/portlist> dhcp l2agent snooping ip-mac-binding	Displays the DHCP snooping IP to MAC binding on the specified DSL ports.	E	13
show interface dsl <slot/portlist> dhcp l2agent snooping max-lease	Displays the DHCP snooping maximum lease and overflow mode on the specified DSL ports.	E	13
no interface dsl <slot/portlist> dhcp l2agent snooping database	Flushes the DHCP snooping database on the specified DSL ports.	E	13
show interface dsl <slot/portlist> dhcp l2agent snooping database	Displays the DHCP snooping database for the specified DSL ports.	E	13
show interface dsl <slot/portlist> dhcp l2agent snooping statistics	Displays DHCP snooping packet statistics for the specified DSL ports.	E	13
clear interface dsl <slot/portlist> dhcp l2agent snooping statistics	Clears the DHCP snooping packet statistics for the specified DSL ports.	E	13
interface fe <slot/portlist>	Enters the sub-command mode for configuring the specified FE ports.	C	13
dhcp l2agent snooping ip-mac-binding	Enables DHCP snooping IP-MAC binding on the specified FE ports.	C	13
no dhcp l2agent snooping ip-mac-binding	Disables DHCP snooping IP-MAC binding on the specified FE ports.	C	13
dhcp l2agent snooping max-lease <lease-count>	Configures the DHCP snooping database max lease count for the specified FE ports. lease-count: 1-32	C	13
show interface fe <slot/portlist> dhcp l2agent snooping ip-mac-binding	Displays the DHCP snooping IP to MAC binding on the specified FE ports.	E	13
show interface fe <slot/portlist> dhcp l2agent snooping max-lease	Displays the DHCP snooping maximum lease and overflow mode on the specified FE ports.	E	13
no interface fe <slot/portlist> dhcp l2agent snooping database	Flushes the DHCP snooping database on the specified FE ports.	E	13
show interface fe <slot/portlist> dhcp l2agent snooping database	Displays the DHCP snooping database for the specified FE ports.	E	13

Table 236 DHCP Commands Summary (continued)

COMMAND	DESCRIPTION	M	P
<code>show interface fe <slot/portlist> dhcp l2agent snooping statistics</code>	Displays DHCP snooping packet statistics for the specified FE ports.	E	13
<code>clear interface fe <slot/ portlist> dhcp l2agent snooping statistics</code>	Clears the DHCP snooping packet statistics for the specified FE ports.	E	13

26.1 Command Examples

You do not want the IES handle and record any DHCP packets on VLAN 100. This example shows how to enable transparent DHCP on VLAN 100. Before this, you have to make sure DHCP L2 Agent is disabled on the VLAN. You can use the `show dhcp vlan *` command to check this. If DHCP L2 Agent is enabled, the system will also display an error when you enable transparent VLAN on the same VLAN.

```

ras# show dhcp vlan *
vid transparent l2agent LDRA option82subopt1 option82subopt2 option18 option37
-----
100      -          V      -      -      -      -      -
option82subopt1(Circuit ID) info
-----

option82subopt2(Remote ID) info
-----

option18(Interface ID) info
-----

option37(Remote ID) info
-----

ras# config
ras(config)# dhcp transparent vlan 100
Error: cannot enable both transparent and L2 agent.
ras(config)# no dhcp l2agent vlan 100
ras(config)# dhcp transparent vlan 100
ras(config)#

```

This example shows how to enable DHCP L2 Agent on VLAN 200 and then configure DHCP option 18 to add this system's model name, the slot, subscriber port, and SVLAN ID from which the request was received.

```

ras# config
ras(config)# dhcp l2agent vlan 200
ras(config)# dhcp l2agent opt18-interface-id vlan 200 option-info %hmodel%slotid%pid%svlan
ras(config)# exit
ras# show dhcp vlan 200
vid transparent l2agent LDRA option82subopt1 option82subopt2 option18 option37
-----
200      -      V      -      -      -      V      -
option82subopt1(Circuit ID) info
-----

option82subopt2(Remote ID) info
-----

option18(Interface ID) info
-----
%hmodel%slotid%pid%svlan
option37(Remote ID) info
-----
ras#

```

This example shows how to enable IP-MAC binding on DSL port **1** on the line card in slot 2, set the DHCP snooping database max lease count to **10**, and display the DHCP snooping database and DHCP snooping packet statistics. Do not forget to activate (provision) the corresponding slot before using the interface. See [Section 23.1.1 on page 344](#) for more information.

```

ras# config
ras(config)# interface dsl 2/1
ras(config-interface-dsl-2/1)# dhcp l2agent snooping ip-mac-binding
ras(config-interface-dsl-2/1)# dhcp l2agent snooping max-lease 10
ras(config-interface-dsl-2/1)# exit
ras(config)# exit
ras# show interface dsl 2/1 dhcp l2agent snooping database
slot: 2  port: 1  overflow: 0
idx      mac                      ipv4/ipv6                      vid
-----
ras# show interface dsl 2/1 dhcp l2agent snooping statistics
slot: 2  port: 1  overflow: 0
dhcpv4 discover      offer  request      ack  release
-----
0      0      0      0      0
dhcpv6 solicit advertise request      reply      renew      rebind      release
-----
0      0      0      0      0      0      0
dhcpv6 relay-forward relay-reply
-----
0      0
ras#

```

CHAPTER 27

Multicast

27.1 IGMP/MLD Commands

Use these commands to configure IGMP settings and display statistics.

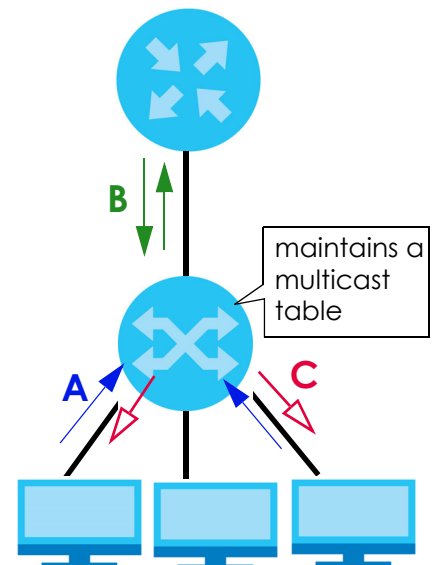
Note: At the time of writing Multicast Listener Discovery (MLD) is for future expansion.

IGMP

- IGMP (Internet Group Management Protocol) - This is a protocol used to establish membership in a multicast group.
- IP Multicast Addresses - In IPv4, a multicast address allows a device to send packets to a specific group of hosts (multicast group) in a different sub-network. A multicast IP address represents a traffic receiving group, not individual receiving devices. IP addresses in the Class D range (224.0.0.0 to 239.255.255.255) are used for IP multicasting. Certain IP multicast numbers are reserved by IANA for special purposes (see the IANA web site for more information).

In IPv6, multicast addresses provide the same functionality as IPv4 broadcast addresses. Broadcasting is not supported in IPv6. A multicast address allows a host to send packets to all hosts in a multicast group.

- IGMP join/leave reports (**A**) - An IGMP join report is sent from a host when it wants to be a member of a multicast group. When the host doesn't want to be a member of a multicast group any more, it sends an IGMP leave report.
- IGMP query and report (**B**) - A router sends an IGMP query to its downlink switches to ask a multicast group member list (also called multicast table). Then the switches that received the IGMP query send the list to the router.
- IGMP snooping - This feature groups multicast traffic (**C**) and only forwards a group's traffic to ports that are members of that group. Without IGMP snooping, a switch does not understand multicast and will broadcast multicast traffic to all the ports in a network. IGMP snooping generates no additional network traffic, allowing you to significantly reduce multicast traffic passing through your switch.
- IGMP Proxy - To allow better network performance, you can use IGMP proxy instead of a multicast routing protocol in a simple tree network topology. In IGMP proxy, only necessary IGMP join/leave reports are forwarded to its uplink router. This can significantly reduce the upstream multicast traffic to the aggregated device.



Note: The IES does not allow a subscriber port to send multicast traffic (except static multicast traffic) to an uplink port. Only the uplink port can forward multicast traffic to the subscriber ports.

- IGMP Snooping and Proxy Note - The IES acts as an IGMPv3 client host for an edge IGMPv3 multicast router and as a IGMPv2/v3 router for IGMPv2/v3 client hosts (subscribers). The IES can recognize IGMPv3 protocol messages and forward them towards the IGMP multicast router. It does not support full-featured IGMPv3 functions like source IP address control specified in RFC 3376.
- Multicast VLAN - This allows one single multicast VLAN to be shared among different subscriber VLANs on the network. This improves bandwidth utilization by reducing multicast traffic in the subscriber VLANs and simplifies multicast group management.
- IGMP group limit - This feature limits the number of multicast groups a port is allowed to join.
- IGMP fast leave - The IES removes a port from the multicast table immediately when an IGMP leave report is received on the port.
- The IES does not respond to IGMP join and leave messages on the upstream interface. The system only responds to IGMP query messages on the upstream interface on the Multicast VLAN.
- The IES only sends IGMP query messages to the hosts that are members of the Multicast VLAN.

Multicast Listener Discovery

The Multicast Listener Discovery (MLD) protocol (defined in RFC 2710) is derived from IPv4's Internet Group Management Protocol version 2 (IGMPv2). MLD uses ICMPv6 message types, rather than IGMP message types. MLDv1 is equivalent to IGMPv2 and MLDv2 is equivalent to IGMPv3.

MLD allows an IPv6 switch or router to discover the presence of MLD hosts who wish to receive multicast packets and the IP addresses of multicast groups the hosts want to join on its network.

MLD snooping and MLD proxy are analogous to IGMP snooping and IGMP proxy in IPv4.

MLD filtering controls which multicast groups a port can join.

An MLD Report message is equivalent to an IGMP Report message, and a MLD Done message is equivalent to an IGMP Leave message.

The following table describes commonly used parameter notation for these commands.

Table 237 IGMP/MLD Command Parameters

NOTATION	DESCRIPTION
<i>mvid</i>	This represents a Multicast VLAN identifier. The range is [1.. 4093].
<i>profile-name</i>	Up to 31 printable characters.

This table describes the commands.

Table 238 IGMP/MLD Commands Summary

COMMAND	DESCRIPTION	M	P
<code>igmp-mld transparent</code>	Enables IGMP/MLD packet transparency. IGMP/MLD transparent, snooping, proxy, and proxy-reporting can not enabled at the same time.	C	13
<code>no igmp-mld transparent</code>	Disables IGMP/MLD packet transparency.	C	13
<code>igmp-mld snooping</code>	Enables IGMP/MLD snooping. IGMP/MLD transparent, snooping, proxy, and proxy-reporting can not enabled at the same time.	C	13
<code>no igmp-mld snooping</code>	Disables IGMP/MLD snooping.	C	13
<code>igmp-mld proxy</code>	Enables IGMP/MLD proxy. IGMP/MLD transparent, snooping, proxy, and proxy-reporting can not enabled at the same time.	C	13
<code>no igmp-mld proxy</code>	Disables IGMP/MLD proxy.	C	13

Table 238 IGMP/MLD Commands Summary (continued)

COMMAND	DESCRIPTION	M	P
igmp-mld proxy-reporting	Enables IGMP/MLD proxy reporting. IGMP/MLD transparent, snooping, proxy, and proxy-reporting can not enabled at the same time.	C	13
no igmp-mld proxy-reporting	Disables IGMP/MLD proxy reporting.	C	13
igmp-mld version igmpv2 igmpv3 mldv1 mldv2 igmpv2 +mldv1 igmpv2+mldv2 igmpv3+mldv1 igmpv3+mldv2	Sets the IGMP/MLD protocol version. igmpv2: IGMP version 2 igmpv3: IGMP version 3 mldv1: MLD version 1 mldv2: MLD version 2	C	13
igmp-mld leave-mode fast- leave last-member-query	Sets the IGMP/MLD leave message handling mode. fast-leave: leaves the joined group immediately last-member-query: sends a specific Query to check if any hosts are still members	C	13
igmp-mld last-member-query timer query-interval <interval> robustness <robustness>	Configures last member query timers. interval: 100-1000 in ms, in step of 100 robustness: 1-5	C	13
igmp-mld general-query timer query-interval <interval> robustness <robustness> max- response-time <max-response- time>	Configures general query timers. interval: 10-300 in seconds robustness: 1-5 max-response-time: 1-10 in seconds	C	13
igmp-mld pbit <pbit>	Configures priority bit in proxy mode.	C	13
show igmp-mld	Displays IGMP/MLD settings.	E	13
igmp-mld group-privilege-profile <profile-name> index <index>	Configures a group privilege entry for the specified group privilege profile. index: the entry index 1-16	C	13
group-range <start-ip> <end- ip>	Configures the group range. start-ip: 224.0.0.0-239.255.255.255 for IPv4 or ff00:: ~ ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff for IPv6 end-ip: 224.0.0.0-239.255.255.255 for IPv4 or ff00:: ~ ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff for IPv6	C	13
privilege permit	Enables permit privilege for the groups.	C	13
privilege forbid	Enables forbid privilege for the groups.	C	13
privilege preview <length> <interval> <count> <reset>	Enables preview privilege for the group and configures the preview parameters. length: 10-300 in seconds interval: 10-300 in seconds count: 1-10 reset: 30-86400 in seconds	C	13
bandwidth <bandwidth>	Configures channel bandwidth for each group. bandwidth: 0-100 in Mbps	C	13

Table 238 IGMP/MLD Commands Summary (continued)

COMMAND	DESCRIPTION	M	P
no igmp-mld group-privilege-profile <i><profile-name></i> index <i><index></i>	Removes an entry from the specified group privilege profile. <i>index</i> : the entry index 1-16	C	13
no igmp-mld group-privilege-profile <i><profile-name></i>	Removes the specified group privilege profile.	C	13
show igmp-mld group-privilege-profile [<i><profile-name></i>]	Displays the contents of all privilege profiles or the specified privilege profile.	E	13
igmp-mld mvlan <i><mvid></i> [tr101-fw]	Enables the specified MVLAN. Without specifying tr101-fw, the IES changes the MVLAN VID of IGMP/MLD reports to this VID if the group address matches one of the group ranges configured in the MVLAN mapping table. <i>mvid</i> : 1 ~ 4093 tr101-fw: this optional configuration enables transparent forwarding of IGMP/MLD messages on this VLAN. This is available in TR-101 mode only.	C	13
no igmp-mld mvlan <i><mvid></i>	Disables the specified MVLAN.	C	13
show igmp-mld mvlan [<i><mvid></i>]	Displays the settings of all MVLAN or the specified MVLAN.	E	13
igmp-mld mvlan-table <i><mvid></i> index <i><index></i>	Configures an entry for the specified MVLAN mapping table for N:1 VLAN mapping (in TR-101 mode only). The MVLAN table is not editable when tr101-fw is specified for the MVLAN. <i>mvid</i> : 1 ~ 4093 <i>index</i> : the entry index 1 ~ 16	C	13
group-range <i><start-ip></i> <i><end-ip></i>	Configures the group range, TR-101 mode only. <i>start-ip</i> : 224.0.0.0 ~ 239.255.255.255 ff00::: ~ ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff <i>end-ip</i> : 224.0.0.0 ~ 239.255.255.255 ff00::~ ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff	C	13
no igmp-mld mvlan-table <i><mvid></i> index <i><index></i>	Removes an entry from the specified MVLAN mapping table, TR-101 mode only. <i>mvid</i> : 1 ~ 4093 <i>index</i> : the entry index 1 ~ 16	C	13
no igmp-mld mvlan-table <i><mvid></i>	Removes the specified MVLAN mapping table, TR-101 mode only. <i>mvid</i> : 1 ~ 4093	C	13
interface dsl <i><slot/portlist></i>	Enters the sub-command mode for configuring the specified DSL ports.	C	13
igmp-mld mvlan <i><mvid></i> [uni-vlan <i><uni-vid></i>]	Adds the specified DSL ports to an MVLAN. Specify uni-vlan to tag the egress packets with the specified uni-vlan.	C	13
igmp-mld mvlan <i><mvid></i> untag	Adds the specified DSL ports to an MVLAN and sends the egress packets out untagged.	C	13
no igmp-mld mvlan <i><mvid></i>	Removes the specified DSL port from an MVLAN.	C	13
igmp-mld max-group <i><max-group-cnt></i>	Configures the maximum group counts on the specified DSL ports. <i>max-group-cnt</i> : 1-16	C	13
igmp-mld group-privilege	Enables group privilege checking on the specified DSL ports.	C	13

Table 238 IGMP/MLD Commands Summary (continued)

COMMAND	DESCRIPTION	M	P
no igmp-mld group-privilege	Disables group privilege checking on the specified DSL ports.	C	13
igmp-mld cac bandwidth <bandwidth>	Enables multicast bandwidth CAC control and configures the maximum multicast bandwidth. <i>bandwidth</i> : 0-100 in Mbps	C	13
no igmp-mld cac	Disables multicast bandwidth CAC control.	C	13
igmp-mld group-privilege-profile <group-privilege-profile>	Applies the group privilege profile to the specified DSL ports. <i>group-privilege-profile</i> : up to 31 printable characters	C	13
no igmp-mld group-privilege-profile <group-privilege-profile>	Removes the group privilege profile from the specified DSL ports.	C	13
interface fe <slot/portlist>	Enters the sub-command mode for configuring the specified FE ports.	C	13
igmp-mld mvlan <mvid> [uni-vlan <uni-vid>]	Adds the specified FE ports to an MVLAN. Specify uni-vlan to tag the egress packets with the specified uni-vlan.	C	13
igmp-mld mvlan <mvid> untag	Adds the specified FE ports to an MVLAN and sends the egress packets out untagged.	C	13
igmp-mld mvlan <mvid> transparent	Adds the specified UNI port to an MVLAN. Binds MVLAN with transparent VLAN model and no multicast group created by JOIN report.	C	13
no igmp-mld mvlan <mvid>	Removes the specified FE port from an MVLAN.	C	13
igmp-mld max-group <max-group-cnt>	Configures the maximum group counts on the specified FE ports. <i>max-group-cnt</i> : 1-16	C	13
igmp-mld group-privilege	Enables group privilege checking on the specified FE ports.	C	13
no igmp-mld group-privilege	Disables group privilege checking on the specified FE ports.	C	13
igmp-mld cac bandwidth <bandwidth>	Enables multicast bandwidth CAC control and configures the maximum multicast bandwidth. <i>bandwidth</i> : 0-100 in Mbps	C	13
no igmp-mld cac	Disables multicast bandwidth CAC control.	C	13
igmp-mld group-privilege-profile <group-privilege-profile>	Applies the group privilege profile to the specified FE ports. <i>group-privilege-profile</i> : up to 31 printable characters	C	13
no igmp-mld group-privilege-profile <group-privilege-profile>	Removes the group privilege profile from the specified FE ports.	C	13
show interface dsl <slot/portlist> igmp-mld	Displays IGMP/MLD settings on the specified DSL ports.	E	13
show interface fe <slot/portlist> igmp-mld	Displays IGMP/MLD settings on the specified FE ports.	E	13
show igmp-mld group	Displays all joined multicast groups.	E	13
show igmp-mld statistics	Displays IGMP/MLD packet statistics.	E	13
clear igmp-mld statistics	Clears IGMP/MLD packet statistics.	E	13
show interface dsl <slot/portlist> igmp-mld group	Displays joined multicast groups on the specified DSL ports.	E	13

Table 238 IGMP/MLD Commands Summary (continued)

COMMAND	DESCRIPTION	M	P
<code>clear interface dsl <slot/ portlist> igmp-mld statistics</code>	Clears IGMP/MLD packet statistics on the specified DSL ports.	E	13
<code>show interface dsl <slot/ portlist> igmp-mld statistics</code>	Displays IGMP/MLD packet statistics on the specified DSL ports.	E	13
<code>show interface dsl <slot/ portlist> igmp-mld log</code>	Displays the IGMP/MLD program log for the specified DSL ports.	E	13
<code>clear interface dsl <slot/ portlist> igmp-mld log</code>	Clears the IGMP/MLD program log for the specified DSL ports.	E	13
<code>show interface fe <slot/portlist> igmp-mld group</code>	Displays joined multicast groups on the specified FE ports.	E	13
<code>clear interface fe <slot/ portlist> igmp-mld statistics</code>	Clears IGMP/MLD packet statistics on the specified FE ports.	E	13
<code>show interface fe <slot/portlist> igmp-mld statistics</code>	Displays IGMP/MLD packet statistics on the specified FE ports.	E	13
<code>show interface fe <slot/portlist> igmp-mld log</code>	Displays the IGMP/MLD program log for the specified FE ports.	E	13
<code>clear interface fe <slot/ portlist> igmp-mld log</code>	Clears the IGMP/MLD program log for the specified FE ports.	E	13
<code>acl multicast unsolicited</code>	Forwards unknown multicast packets.	C	13
<code>acl multicast upstream inactive</code>	Drops multicast packets from the upstream direction.	C	13
<code>no acl multicast unsolicited</code>	Drops unknown multicast packets.	C	13
<code>no acl multicast upstream inactive</code>	Forwards multicast packets from the upstream direction.	C	13
<code>show acl multicast</code>	Displays ACL settings for multicast packets.	E	13

27.1.1 Command Examples

Note: Before you can use an interface, you have to activate (provision) the corresponding slot. See [Section 23.1.1 on page 344](#) for how to activate a slot.

This example shows how to enable IGMP snooping on the IES with the following settings:

- IGMP version 3
- leave message handling mode: fast-leave
- last member query timer: 200 ms, robustness 1
- general query timer: 60 seconds, robustness 1 and 5 seconds for the maximum response time

Finally, it displays the IGMP/MLD settings so you can check them.

```
ras# config
ras(config)# igmp-mld snooping
ras(config)# igmp-mld version igmpv3
ras(config)# igmp-mld leave-mode fast-leave
ras(config)# igmp-mld last-member-query timer query-interval 200 robustness 1
ras(config)# igmp-mld general-query timer query-interval 60 robustness 1 max-response-time 5
ras(config)# exit
ras# show igmp-mld
mode:snooping
version:igmpv3
leavemode:fast-leave

general query timer:
  interval:60 (sec)
  robustness:1
  max response time:5 (sec)

last member query timer:
  interval:200(ms)
  robustness:1

ras#
```

This example shows the ACL multicast settings, and how to drop unknown multicast packets and forward multicast packets from DSL subscribers.

```
ras# show acl multicast
The multicast packets from upstream direction for IPv4 : drop
The multicast packets from upstream direction for IPv6 : drop
The unknown multicast packets for IPv4 : forward
The unknown multicast packets for IPv6 : forward
ras# config
ras(config)# no acl multicast upstream inactive
ras(config)# no acl multicast unsolicited
ras(config)# exit
ras# show acl multicast
The multicast packets from upstream direction for IPv4 : forward
The multicast packets from upstream direction for IPv6 : forward
The unknown multicast packets for IPv4 : drop
The unknown multicast packets for IPv6 : drop
ras#
```

CHAPTER 28

Static Multicast Commands

Use these commands to configure static multicast settings.

28.1 Static Multicast Commands Summary

Use static multicast to allow incoming frames based on the VLAN ID and multicast MAC addresses that you specify.

The following table describes commonly used parameter notation for these commands.

Table 239 Static multicast command parameters

NOTATION	DESCRIPTION
<i>uni-vlan</i>	The VLAN ID on the UNI (User Network Interface) ports, 1-4093.
<i>mac</i>	This is a static multicast MAC address (01:00:5e:00:00:00 ~ 01:00:5e:7f:ff:ff) which identifies the multicast group.

This table describes the commands.

Table 240 Static multicast commands summary

COMMAND	DESCRIPTION	M	P
<code>interface dsl <slot/portlist></code>	Enters the sub-command mode for configuring the specified DSL ports.	C	13
<code>smcast <mac> uni-vlan <uni-vid></code>	Configures a static multicast group and the VLAN ID that incoming frames from the multicast group must be tagged with. Note: Make sure the VLAN is configured in VLAN Trunk or VLAN Translation mode before using this command.	C	13
<code>smcast <mac> uni-untag</code>	Configures a static multicast group with no VLAN tagged. That is, the ports only accept untagged frames from the multicast group.	C	13
<code>no smcast <mac></code>	Removes the specified static multicast group.	C	13
<code>show interface dsl <slot/portlist> smcast</code>	Displays static multicast settings on the specified DSL ports.	E	13
<code>interface fe <slot/portlist></code>	Enters the sub-command mode for configuring the specified FE ports.	C	13
<code>smcast <mac> uni-vlan <uni-vid></code>	Configures a static multicast group and the VLAN ID that incoming frames from the multicast group must be tagged with. Note: Make sure the VLAN is configured in VLAN Trunk or VLAN Translation mode before using this command.	C	13
<code>smcast <mac> uni-untag</code>	Configures a static multicast group for traffic without a VLAN tag. That is, the ports only accept untagged frames from the multicast group.	C	13

Table 240 Static multicast commands summary (continued)

COMMAND	DESCRIPTION	M	P
<code>no smcast <mac></code>	Removes the specified static multicast group.	C	13
<code>show interface fe <slot/portlist> smcast</code>	Displays static multicast settings on the specified FE ports.	E	13

28.1.1 Command Examples

This example cross-connects untagged packets sent from DSL slot 2 port 1 to the specified S VLAN 100 on uplink ports. This example also sets the DSL port to only accept multicast frames of group 01:00:55:aa:bb:cc with no VLAN tag.

```
sysname# config
sysname(config)# interface dsl 2/1
sysname(config-interface-dsl-2/1)# vlan trunk uni-untag svlan 100 spbit 1
sysname(config-interface-dsl-2/1)# smcast 01:00:55:aa:bb:cc uni-untag
```

This example shows how to have the IES change VLAN 10 tagged frames received on DSL slot 2 port 1 to VLAN 20 tagged frames. This example also sets the DSL port to only accept multicast frames of group 01:00:11:00:00:01 with VLAN 10 tags.

```
sysname# config
sysname(config)# interface dsl 2/1
sysname(config-interface-dsl-2/1)# vlan translation uni-vlan 10 svlan 20
sysname(config-interface-dsl-2/1)# smcast 01:00:11:00:00:01 uni-vlan 10
```


CHAPTER 29

IP

Use these commands to configure the system and management IP addresses and subnet masks.

29.1 IP Commands Summary

This table describes the commands.

Table 241 IP Commands Summary

COMMAND	DESCRIPTION	M	P
show ip arp	Displays the ARP table.	E	1
no arp	Flushes the ARP table entries.	E	13
show ip	Displays interface IP settings.	E	1
show ip inband-mode	Displays the DHCP settings of the inband management (MGMT port) interface.	E	1
ip inband address <ip-address>/<mask>	Sets the inband management (MGMT port) interface's IP address and subnet mask. Disables the DHCP client function if it is enabled.	C	13
ip inband address <ip-address>/<mask> [mgmt-vlan <mgmt-vid>] [pbit <pbit>] [default-gateway <default-gateway-ip-address>]	Sets the inband management (MGMT port) interface's IP address and subnet mask with management VLAN, management priority bit, and default gateway. Disables the DHCP client function if it is enabled. <i>ip-address</i> : 0.0.0.1-223.255.255.255 <i>mask</i> : 1-30 <i>mgmt-vid</i> : 1-4093 <i>pbit</i> : 0-7 <i>default-gateway-ip-address</i> : 1.0.0.0-223.255.255.255	C	13
ip inband address dhcp	Sets the inband management (MGMT port) interface to be a DHCP client.	C	13
ip inband address dhcp enable release renew	Controls the DHCP client function on the inband management (MGMT port) interface. <i>enable</i> : turn the DHCP client function on. <i>release</i> : release the dynamic IP address. <i>renew</i> : renew the dynamic IP address	C	13
ip inband mgmt-vlan <mgmt-vid> [pbit <pbit>]	Sets the inband management VLAN and priority bit. <i>mgmt-vid</i> : 1-4093 <i>pbit</i> : 0-7, default 7	C	13
ip inband default-gateway <ip-address>	Sets the default gateway's IP address.	C	13

Table 241 IP Commands Summary (continued)

COMMAND	DESCRIPTION	M	P
no ip inband	Sets the inband management IP address and subnet mask to the default values. The default value is 192.168.1.1	C	13
ip outband address <ip-address>/<mask>	Sets the management IP address and subnet mask for the out-of-band management port. <i>ip-address</i> : 0.0.0.1 ~ 223.255.255.255 <i>mask</i> : 0-32	C	13
no ip outband	Sets the management IP address and subnet mask for the out-of-band management port to the default values. The default value is 192.168.0.1	C	13
ping <ip-address> [voip rtp] [size <size>] [-t]	Sends Ping packets to the specified Ethernet device. <i>ip-address</i> : 0.0.0.0 ~ 223.255.255.255, a domain-name is permitted for a VOIP interface <i>voip</i> : ping via VoIP interface <i>rtp</i> : ping via RTP interface <i>size</i> : 0-1472 <i>-t</i> : ping continuously until Ctrl-C is pressed	E	1
show ip statistics	Displays interface statistics.	E	1

CHAPTER 30

IPv6

Use these commands to configure IPv6 settings.

IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to 3.4×10^{38} IP addresses.

The 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address `2001:0db8:1a2b:0015:0000:0000:1a2f:0000`.

IPv6 addresses can be abbreviated in two ways:

- Leading zeros in a block can be omitted. So `2001:0db8:1a2b:0015:0000:0000:1a2f:0000` can be written as `2001:db8:1a2b:15:0:0:1a2f:0`.
- Any number of consecutive blocks of zeros can be replaced by a double colon. A double colon can only appear once in an IPv6 address. So `2001:0db8:0000:0000:1a2f:0000:0000:0015` can be written as `2001:0db8::1a2f:0000:0000:0015`, `2001:0db8:0000:0000:1a2f::0015`, `2001:db8::1a2f:0:0:15` or `2001:db8:0:0:1a2f::15`.

IPv6 Prefix and Prefix Length

Similar to an IPv4 subnet mask, IPv6 uses an address prefix to represent the network address. An IPv6 prefix length specifies how many most significant bits (start from the left) in the address compose the network address. The prefix length is written as "/x" where x is a number. For example,

```
2001:db8:1a2b:15::1a2f:0/32
```

means that the first 32 bits (`2001:db8`) is the subnet prefix.

IPv6 Subnet Masking

Both an IPv6 address and IPv6 subnet mask compose of 128-bit binary digits, which are divided into eight 16-bit blocks and written in hexadecimal notation. Hexadecimal uses four bits for each character (1 ~ 10, A ~ F). Each block's 16 bits are then represented by four hexadecimal characters. For example, `FFFF:FFFF:FFFF:FFFF:FC00:0000:0000:0000`.

The first 48 bits of the IPv6 subnet mask are for Internet routing or fixed for local address, the 49th to the 64th bits are for subnetting and the last 64 bits are for interface identifying. The 16 binary digits for subnetting allows an organization to set up to 65,535 individual subnets.

Interface ID

In IPv6, an interface ID is a 64-bit identifier. It identifies a physical interface (for example, an Ethernet port) or a virtual interface (for example, the management IP address for a VLAN). One interface should have a unique interface ID.

Link-local Address

A link-local address uniquely identifies a device on the local network (the LAN). It is similar to a "private IP address" in IPv4. You can have the same link-local address on multiple interfaces on a device. A link-local unicast address has a predefined prefix of $\text{fe80}::/10$. The link-local unicast address format is as follows.

Table 242 Link-local Unicast Address Format

1111 1110 10	0	Interface ID
10 bits	54 bits	64 bits

Global Address

A global address uniquely identifies a device on the Internet. It is similar to a "public IP address" in IPv4. A global unicast address starts with a 2 or 3. The global address format as follows.

Table 243 Global Address Format

001	Global ID	Subnet ID	Interface ID
3 bits	45 bits	16 bits	64 bits

The global ID is the network identifier or prefix of the address and is used for routing. This may be assigned by service providers.

The subnet ID is a number that identifies the subnet of a site.

Multicast Address

In IPv6, multicast addresses provide the same functionality as IPv4 broadcast addresses. Broadcasting is not supported in IPv6. A multicast address allows a host to send packets to all hosts in a multicast group.

Multicast scope allows you to determine the size of the multicast group. A multicast address has a predefined prefix of $\text{ff00}::/8$. The following table describes some of the predefined multicast addresses.

Table 244 Predefined Multicast Address

MULTICAST ADDRESS	DESCRIPTION
$\text{FF01}::0:0:0:0:0:0:1$	All hosts on a local node.
$\text{FF01}::0:0:0:0:0:0:2$	All routers on a local node.
$\text{FF02}::0:0:0:0:0:0:1$	All hosts on a local connected link.
$\text{FF02}::0:0:0:0:0:0:2$	All routers on a local connected link.
$\text{FF05}::0:0:0:0:0:0:2$	All routers on a local site.
$\text{FF05}::0:0:0:0:0:0:1:3$	All DHCP servers on a local site.

The following table describes the multicast addresses which are reserved and cannot be assigned to a multicast group.

Table 245 Reserved Multicast Address

MULTICAST ADDRESS
FF00:0:0:0:0:0:0:0
FF01:0:0:0:0:0:0:0
FF02:0:0:0:0:0:0:0
FF03:0:0:0:0:0:0:0
FF04:0:0:0:0:0:0:0
FF05:0:0:0:0:0:0:0
FF06:0:0:0:0:0:0:0
FF07:0:0:0:0:0:0:0
FF08:0:0:0:0:0:0:0
FF09:0:0:0:0:0:0:0
FF0A:0:0:0:0:0:0:0
FF0B:0:0:0:0:0:0:0
FF0C:0:0:0:0:0:0:0
FF0D:0:0:0:0:0:0:0
FF0E:0:0:0:0:0:0:0
FF0F:0:0:0:0:0:0:0

Loopback

A loopback address (0:0:0:0:0:0:1 or ::1) allows a host to send packets to itself. It is similar to "127.0.0.1" in IPv4.

Unspecified

An unspecified address (0:0:0:0:0:0:0 or ::) is used as the source address when a device does not have its own address. It is similar to "0.0.0.0" in IPv4.

EUI-64

The EUI-64 (Extended Unique Identifier) defined by the IEEE (Institute of Electrical and Electronics Engineers) is an interface ID format designed to adapt with IPv6. It is derived from the 48-bit (6-byte) Ethernet MAC address as shown next. EUI-64 inserts the hex digits `FFFE` between the third and fourth bytes of the MAC address and complements the seventh bit of the first byte of the MAC address. See the following example.

Table 246

MAC	00	:	13	:	49	:	12	:	34	:	56

Table 247

EUI-64	02	:	13	:	49	:	FF	:	FE	:	12	:	34	:	56

Stateless Autoconfiguration

With stateless autoconfiguration in IPv6, addresses can be uniquely and automatically generated. Unlike DHCPv6 (Dynamic Host Configuration Protocol version six) which is used in IPv6 stateful autoconfiguration, the owner and status of addresses don't need to be maintained by a DHCP server. Every IPv6 device is able to generate its own and unique IP address automatically when IPv6 is initiated on its interface. It combines the prefix and the interface ID (generated from its own Ethernet MAC address, see [Interface ID](#) and [EUI-64](#)) to form a complete IPv6 address.

When IPv6 is enabled on a device, its interface automatically generates a link-local address (beginning with `fe80`).

When the interface is connected to a network with a router and the `ipv6 address autoconfig` command is issued on the IES, it generates ²another address which combines its interface ID and global and subnet information advertised from the router. This is a routable global IP address.

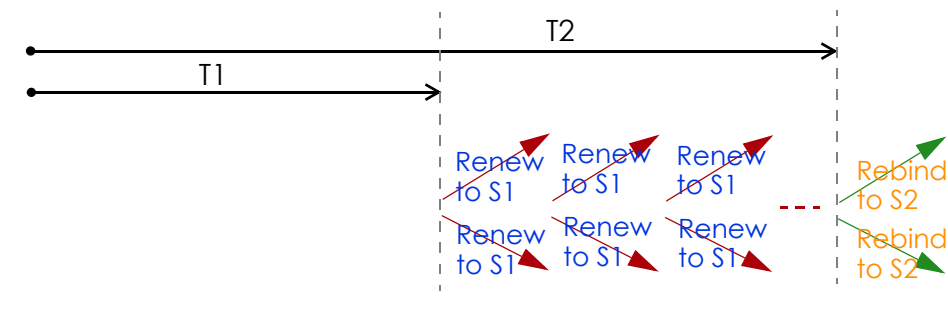
DHCPv6

The Dynamic Host Configuration Protocol for IPv6 (DHCPv6, RFC 3315) is a server-client protocol that allows a DHCP server to assign and pass IPv6 network addresses, prefixes and other configuration information to DHCP clients. DHCPv6 servers and clients exchange DHCP messages using UDP.

Each DHCP client and server has a unique DHCP Unique Identifier (DUID), which is used for identification when they are exchanging DHCPv6 messages. The DUID is generated from the MAC address, time, vendor assigned ID and/or the vendor's private enterprise number registered with the IANA. It should not change over time even after you reboot the device.

Identity Association

An Identity Association (IA) is a collection of addresses assigned to a DHCP client, through which the server and client can manage a set of related IP addresses. Each IA must be associated with exactly one interface. The DHCP client uses the IA assigned to an interface to obtain configuration from a DHCP server for that interface. Each IA consists of a unique IAID and associated IP information. The IA type is the type of address in the IA. Each IA holds one type of address. IA_NA means an identity association for non-temporary addresses and IA_TA is an identity association for temporary addresses. An IA_NA option contains the T1 and T2 fields, but an IA_TA option does not. The DHCPv6 server uses T1 and T2 to control the time at which the client contacts with the server to extend the lifetimes on any addresses in the IA_NA before the lifetimes expire. After T1, the client sends the server (**S1**) (from which the addresses in the IA_NA were obtained) a Renew message. If the time T2 is reached and the server does not respond, the client sends a Rebind message to any available server (**S2**). For an IA_TA, the client may send a Renew or Rebind message at the client's discretion.



2. In IPv6, all network interfaces can be associated with several addresses.

DHCP Relay Agent

A DHCP relay agent is on the same network as the DHCP clients and helps forward messages between the DHCP server and clients. When a client cannot use its link-local address and a well-known multicast address to locate a DHCP server on its network, it then needs a DHCP relay agent to send a message to a DHCP server that is not attached to the same network.

The DHCP relay agent can add the remote identification (remote-ID) option and the interface-ID option to the Relay-Forward DHCPv6 messages. The remote-ID option carries a user-defined string, such as the system name. The interface-ID option provides slot number, port information and the VLAN ID to the DHCPv6 server. The remote-ID option (if any) is stripped from the Relay-Reply messages before the relay agent sends the packets to the clients. The DHCP server copies the interface-ID option from the Relay-Forward message into the Relay-Reply message and sends it to the relay agent. The interface-ID should not change even after the relay agent restarts.

ICMPv6

Internet Control Message Protocol for IPv6 (ICMPv6 or ICMP for IPv6) is defined in RFC 4443. ICMPv6 has a preceding Next Header value of 58, which is different from the value used to identify ICMP for IPv4. ICMPv6 is an integral part of IPv6. IPv6 nodes use ICMPv6 to report errors encountered in packet processing and perform other diagnostic functions, such as "ping".

Neighbor Discovery Protocol (NDP)

The Neighbor Discovery Protocol (NDP) is a protocol used to discover other IPv6 devices and track neighbor's reachability in a network. A neighbor is "reachable" means a neighbor solicitation message (from the IES) is responded with a neighbor advertisement message from the neighbor.

30.1 IPv6 Commands Summary

This table describes the commands.

Table 248 IPv6 Commands Summary

COMMAND	DESCRIPTION	M	P
<code>ip inband address ipv6 <ipv6-address>/<mask></code>	Manually configures a static in-band management IPv6 global address. <i>ipv6-address</i> : 2000:: ~ 3fff:ffff:ffff:ffff:ffff:ffff:ffff:ffff <i>mask</i> : 0 ~ 127	C	13
<code>ip inband default-gateway ipv6 <ipv6-address></code>	Manually configures a static in-band IPv6 global address for the default outgoing gateway. <i>ipv6-address</i> : 2000:: ~ 3fff:ffff:ffff:ffff:ffff:ffff:ffff:ffff	C	13
<code>no ipv6 inband</code>	Removes the manually configured in-band management IPv6 address and default gateway address.	C	13
<code>ip outband address ipv6 <ipv6-address>/<mask></code>	Manually configures a static out-of-band management IPv6 global address. <i>ipv6-address</i> : 2000:: ~ 3fff:ffff:ffff:ffff:ffff:ffff:ffff:ffff <i>mask</i> : 0 ~ 128	C	13

Table 248 IPv6 Commands Summary (continued)

COMMAND	DESCRIPTION	M	P
no ipv6 outband	Removes the manually configured out-of-band management IPv6 address and default gateway address.	C	13
ip ipv6 default-management <inband outband>	Sets whether the IES uses the in-band or out-of-band traffic flow to send packets originating from itself (such as SNMP traps) or with an unknown source.	C	13
show ip ipv6	Displays the link-local addresses the IES generated automatically. This also shows the manually configured inband/out-of-band management IPv6 address and default gateway address.	E	3
show ip ipv6 default-router	Displays IPv6 addresses of on-link routers that will help forward packets.	E	3
show ip ipv6 destination	Displays the mapping list of the next-hop address to an IPv6 destination address.	E	3
show ip ipv6 neighbor	Displays the neighbor cache, which lists the MAC addresses of the IES's interfaces and neighboring devices.	E	3
show ip ipv6 prefix	Displays the list of on-link prefixes. The prefixes are used to determine whether an IP address is on the same link as the IES or should be reached through a router. A prefix is considered to be on-link when it is assigned to an interface on a link. It's used to determine if an address is on the IES's subnet and can be reached directly without passing through a router. An on-link interface is directly connected to the IES or connected through another switch.	E	3
show ip ipv6 route	Displays the IPv6 routing table.	E	3
show ip ipv6 default-management	Displays packets' default outgoing interface.	E	3
ping ipv6 <ipv6-address> [size <size>] [-t]	Sends Ping packets to the specified Ethernet device. ipv6-address: 2000:: ~ 3fff:ffff:ffff:ffff:ffff:ffff:ffff:ffff size: 0 ~ 1472 -t: ping continuously until Ctrl-C is pressed	E	0

CHAPTER 31

MTU

Use these commands to configure the maximum transmission unit.

31.1 MTU Commands Summary

This table describes the commands.

Table 249 MTU Commands Summary

COMMAND	DESCRIPTION	M	P
mtu <mtu>	Configures the maximum transmission unit. <mtu>: 512..2000 bytes	C	13
no mtu	Loads the default MTU setting.	C	13
show mtu	Displays the maximum transmission unit setting.	E	1

CHAPTER 32

PPPoE Intermediate Agent

Use these commands to have the IES to add a vendor-specific tag to PADI (PPPoE Active Discovery Initiation) and PADR (PPPoE Active Discovery Request) packets from PPPoE clients. This tag gives a PPPoE termination server additional information (such as the port number, VLAN ID, and MAC address) that the server can use to identify and authenticate a PPPoE client. See [Section 6.7.1 on page 92](#) for details on the PPPoE intermediate agent vendor-specific tag format.

32.1 PPPoE Intermediate Agent Commands Summary

The following table describes commonly used parameter notation for these commands.

Table 250 PPPoE Intermediate Agent Command Parameters

NOTATION	DESCRIPTION
<i>info</i>	The PPPoE intermediate Agent circuit ID and remote ID. The max length of option-info converting from configuration is 63. It can use the following components: special characters except % => ~`!@#\$%^&*()-=_+{}<>?.,/ %=: equals character % %0x00-%0xFF: represents byte value %pname: configured port name %pid: port index %chvpi: channel VPI %chvci: channel VCI %chid: channel ID, UNI VLAN for Ethernet, VPI.VCI for ATM %slotid: slot index of the logic port %svlan: SVLAN ID which PPPoE client runs on %cvlan: CVLAN ID which PPPoE client runs on %hname: host device name %cmac1: MAC address of a PPPoE client, in XX:XX:XX:XX:XX:XX format where X=0-F %cmac2: MAC address of a PPPoE client in XXXXXXXXXXXX format where X=0-F %cmac3: MAC address of a PPPoE client in Bytes %dmac1: MAC address of the host device in XX:XX:XX:XX:XX:XX format where X=0-F %dmac2: MAC address of the host device in XXXXXXXXXXXX format where X=0-F %dmac3: MAC address of host device in Bytes %phtype: ATM: atm Ethernet eth %hmodel: model name of the host device %fwid: host device firmware ID %blank: blank character

This table describes the commands.

Table 251 PPPoE Intermediate Commands Summary

COMMAND	DESCRIPTION	M	P
pppoe transparent vlan <vid>	Enables PPPoE packet transparent on the specified VLAN. PPPoE transparent and intermediate agent can not be enabled at the same time in a VLAN.	C	13
no pppoe transparent vlan <vid>	Disables PPPoE packet transparent on the specified VLAN.	C	13

Table 251 PPPoE Intermediate Commands Summary (continued)

COMMAND	DESCRIPTION	M	P
<code>pppoe intermediate-agent vlan <vid></code>	Enables PPPoE intermediate agent on the specified VLAN. PPPoE transparent and intermediate agent can not be enabled at the same time in a VLAN.	C	13
<code>no pppoe intermediate-agent vlan <vid></code>	Disables PPPoE intermediate agent on the specified VLAN.	C	13
<code>pppoe intermediate-agent circuit-id vlan <vid> option-info <info></code>	Configures the PPPoE intermediate Agent circuit ID format on the specified VLAN. <i>info</i> : up to 127 ASCII characters of additional information for the IES to add to the VLAN's PPPoE packets. See Table 250 on page 391 for more information.	C	13
<code>no pppoe intermediate-agent circuit-id vlan <vid></code>	Disables PPPoE intermediate Agent circuit ID on the specified VLAN.	C	13
<code>pppoe intermediate-agent remote-id vlan <vid> info <info></code>	Configures the PPPoE intermediate Agent remote ID format on the specified VLAN. <i>info</i> : up to 127 ASCII characters of additional information for the IES to add to the VLAN's PPPoE packets. See Table 250 on page 391 for more information.	C	13
<code>no pppoe intermediate-agent remote-id vlan <vid></code>	Disables PPPoE intermediate Agent remote ID on the specified VLAN.	C	13
<code>show pppoe vlan <vid></code>	Displays the PPPoE settings on the specified VLAN.	E	13
<code>pppoe test <slot/port> svlan <svid> [cvlan <cvid>]</code>	Performs a PPPoE session test. The IES sends PPPoE frames tagged with the specified subscriber VLAN ID or double-tagged VLAN IDs to the uplink PPPoE server. Use this command to check PPPoE handshake issues.	E	13
<code>pppoe test <slot/port> uni-untag</code>	Performs a PPPoE session test. The IES sends untagged PPPoE frames to the uplink PPPoE server. Use this command to check PPPoE handshake issues.	E	13
<code>show interface dsl <slot/portlist> pppoe test</code>	Shows the PPPoE session test result on the specified DSL ports.	E	13
<code>show interface fe <slot/portlist> pppoe test</code>	Shows the PPPoE session test result on the specified FE ports.	E	13

32.1.1 Command Examples

This example enables PPPoE IA on VLAN 100 and configures the circuit ID and remote ID to carry some extra information respectively.

- circuit ID: the receiving slot and port numbers + the C VLAN for the DSL line information.

- remote ID: the receiving port number + the PPPoE client's MAC address for the subscriber line identification.

```
ras# show pppoe vlan 100
ras# config
ras(config)# pppoe intermediate-agent vlan 100
ras(config)# pppoe intermediate-agent circuit-id vlan 100 option-info %slotid%pid%cvlan
ras(config)# pppoe intermediate-agent remote-id vlan 100 info %pid%cmac1
ras(config)# exit
ras# show pppoe vlan 100
vid transparent intermediateagent Circuit ID Remote ID
-----
100      -              V              V              V
Circuit ID info
-----
%slotid%pid%cvlan
Remote ID info
-----
%pid%cmac1
ras#
```

This command tests the PPPoE session handshake between port 1 of the line card in slot 2 and the uplink PPPoE server. The result shows the IES failed to receive a PADO (PPPoE Active Discovery Offer) from the PPPoE. In this case you would check the connection between the IES and the PPPoE server.

```
ras# pppoe test 2/1 uni-untag
slot: 2 port: 1 start to PPPoE test
ras# show interface dsl 2/1 pppoe test
slot  port      status
----  -
2      1      receive PADO fail
ras#
```

CHAPTER 33

QoS

Use these commands to set up Quality of Service (QoS) through DSCP to IEEE 802.1p priority bit mapping and queuing settings.

33.1 DSCP to Priority Bit Mapping Commands

Use these commands to configure the DSCP to IEEE 802.1p priority bit mapping to allow the IES to prioritize traffic based on the incoming DSCP value according to the DSCP to IEEE 802.1p mapping table.

DiffServ is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

DSCP and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) field to replace the Type of Service (ToS) field in the IP header. The DS field contains a 6-bit DSCP field which can define up to 64 service levels and the remaining 2 bits are defined as currently unused (CU). The following figure illustrates the DS field.

Table 252 DiffServ: differentiated service field

DSCP (6 bits)	CU (2 bits)

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

The DSCP value determines the PHB (Per-Hop Behavior), that each packet gets as it is forwarded across the DiffServ network. Based on the marking rule different kinds of traffic can be marked for different priorities of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

The following section lists the commands for this feature.

Table 253 DSCP to priority bit mapping command summary

COMMAND	DESCRIPTION	M	P
dscp <dscp/priority>	Maps the specified DSCP to the specified IEEE 802.1p priority bit. <i>dscp</i> : 0-63 <i>priority</i> : 0-7	C	13
show dscp	Displays the DSCP to IEEE 802.1p priority bit mapping settings.	E	13
interface dsl <slot/portlist>	Enters the sub-command mode for configuring the specified DSL ports.	C	13
dscp active	Enables DSCP to priority bit mapping on the ports.	C	13
no dscp active	Disables DSCP to priority bit mapping on the ports.	C	13
show interface dsl <slot/portlist> dscp	Displays the status of DSCP to priority bit mapping on the specified DSL ports.	E	13
interface fe <slot/portlist>	Enters the sub-command mode for configuring the specified FE ports.	C	13
dscp active	Enables DSCP to priority bit mapping on the ports.	C	13
no dscp active	Disables DSCP to priority bit mapping on the ports.	C	13
show interface fe <slot/portlist> dscp	Displays the status of DSCP to priority bit mapping on the specified FE ports.	E	13

33.1.1 Command Examples

This example shows how to map DSCP 48 to priority 6 so the IES will map incoming packets with a DSCP value of 48 to 802.1p tag 6. The packets can safely traverse DSCP-incapable links. This example also enables DSCP to IEEE 802.1p priority mapping on DSL port 1 of the line card in slot 2.

```

ras# show dscp
DSCP to p-bit mapping table :
DSCP -> Priority : 0 -> 0
DSCP -> Priority : 1 -> 0
-----SNIP!-----
DSCP -> Priority : 48 -> 0
-----SNIP!-----
ras# config
ras(config)# dscp 48/6
ras(config)# interface dsl 2/1
ras(config-interface-dsl-2/1)# dscp active
ras(config-interface-dsl-2/1)# exit
ras(config)# show interface dsl 2/1 dscp
DSCP status : enable
ras# show dscp
DSCP to p-bit mapping table :
DSCP -> Priority : 0 -> 0
DSCP -> Priority : 1 -> 0
-----SNIP!-----
DSCP -> Priority : 48 -> 6
-----SNIP!-----
ras#

```

33.2 QoS Commands

Use these commands for configuring Quality of Service settings.

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control the use of bandwidth. Without QoS, all traffic data is equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for delay-sensitive applications such as VoIP or video-on-demand (VOD).

Configure QoS to prioritize downstream traffic in queues and fine-tune network performance.

- QoS applies only to the downstream traffic (traffic going to the subscribers).
- QoS limits the data rate of traffic flowing through the IES's physical queues.

Queuing

Queuing is used to help solve performance degradation when there is network congestion. The switch has eight physical queues, Q0 to Q7. Q7 has the highest priority and Q0 has the lowest.

Table 254 Physical Queue Priority

QUEUE	PRIORITY
Q7	8 (Highest)
Q6	7
Q5	6
Q4	5
Q3	4
Q2	3
Q1	2
Q0	1 (Lowest)

Queuing algorithms allow switches to maintain separate queues for packets from each individual source or flow and prevent a source from monopolizing the bandwidth.

- Strictly Priority Queuing (SPQ) services queues based on priority only. As traffic comes into the IES, traffic on the highest priority queue, Q7 is transmitted first. When that queue empties, traffic on the next highest-priority queue, Q6 is transmitted until Q6 empties, and then traffic is transmitted on Q5 and so on. If higher priority queues never empty, then traffic on lower priority queues never gets sent. SP does not automatically adapt to changing network requirements.
- Weighted Fair Queuing is used to guarantee each queue's minimum bandwidth based on its bandwidth weight (portion) (the number you configure in the Weight field) when there is traffic congestion. WFQ is activated only when a port has more traffic than it can handle. Queues with larger weights get more guaranteed bandwidth than queues with smaller weights. This queuing mechanism is highly efficient in that it divides any available bandwidth across the different traffic queues. The default weight for each queue is 50.
- Weighted Round Robin Scheduling (WRR) scheduling services queues of the same priority level on a rotating basis based on their queue weight. The higher a queue's weight, the more service it gets. This queuing mechanism is highly efficient in that it divides any available bandwidth across the different traffic queues and returns to queues that have not yet emptied.

The following table describes commonly used parameter notation for these commands.

Table 255 QoS Command Parameters

NOTATION	DESCRIPTION
<i>rate</i>	The maximum rate. 32-100000 in kbps. Default 100000.
<i>name</i>	Name of a profile. Use up to 31 printable characters.
<i>depth</i>	The maximum number of packets, 30-255, default 255
<i>queue-id</i>	The QoS queue. 0-7
<i>weight</i>	The weight of a Weighted Round Robin (WRR) or Weighted Fair Queueing (WFQ) queue. 1-50. Default 50.

This table describes the commands.

Table 256 QoS Commands Summary

COMMAND	DESCRIPTION	M	P
<code>qos atm vc-shaping</code>	Enables per-Virtual Circuit (VC) shaping for Asynchronous Transfer Mode (ATM) Virtual Circuits (VCs).	C	13
<code>no qos atm vc-shaping</code>	Disables per-VC shaping for ATM VC.	C	13
<code>show qos atm vc-shaping</code>	Displays per-VC shaping for ATM VC.	E	13
<code>interface dsl <slot/portlist></code>	Enters the sub-command mode for configuring the specified DSL ports.	C	13
<code>qos shaping-profile <profile-name></code>	Configures a QoS shaping profile on the specified DSL ports.	C	13
<code>qos weight-profile <profile-name></code>	Configures a Weighted Round Robin or Weighted Fair Queueing profile on the specified DSL ports.	C	13
<code>qos algorithm sp wfq sp-wfq shaping</code>	Sets which QoS algorithm to use on the specified DSL ports. sp: Strict Priority, queue7 has the highest priority wfq: Weighted Fair Queueing. sp-wfq: Strict Priority + Weighted Fair Queueing. Queues 5-0 are scheduled by WFQ first, and the output of WFQ, queue 7, and queue 6 are scheduled by Strict Priority. Queue 7 has the highest priority, and the output of WFQ has the lowest priority. shaping: Strict Priority + shaping. Every queue has its own shaping rate. After shaping, every queue is scheduled by Strict Priority. Queue 7 has the highest priority.	C	13
<code>qos max-rate <rate></code>	Configures the maximum rate.	C	13
<code>qos atm-vc <vpi>/<vci> vc-shaping-profile <profile-name></code>	Configures an ATM shaping profile on the specified ATM VCs.	C	13
<code>interface fe <slot/portlist></code>	Enters the sub-command mode for configuring the specified FE ports.	C	13
<code>qos shaping-profile <profile-name></code>	Configures a QoS shaping profile on the specified FE ports.	C	13
<code>qos weight-profile <profile-name></code>	Configures a Weighted Round Robin or Weighted Fair Queueing profile on the specified FE ports.	C	13

Table 256 QoS Commands Summary (continued)

COMMAND	DESCRIPTION	M	P
<code>qos algorithm sp wfq sp-wfq shaping</code>	Sets which QoS algorithm to use on the specified FE ports. sp: Strict Priority, queue7 has the highest priority wfq: Weighted Fair Queueing. sp-wfq: Strict Priority + Weighted Fair Queueing. Queues 5-0 are scheduled by WFQ first, and the output of WFQ, queue 7, and queue 6 are scheduled by Strict Priority. Queue 7 has the highest priority, and the output of WFQ has the lowest priority. shaping: Strict Priority + shaping. Every queue has its own shaping rate. After shaping, every queue is scheduled by Strict Priority. Queue 7 has the highest priority.	C	13
<code>qos max-rate <rate></code>	Configures the maximum rate.	C	13
<code>show interface fe <slot/portlist> qos</code>	Displays the QoS configuration for the specified FE ports.	E	13
<code>qos shaping-profile <name></code>	Enters the sub-command mode for configuring the specified shaping profile.	C	13
<code>exit</code>	Leaves the shaping profile sub-command mode.	C	13
<code>queue7 max-rate <rate> depth <depth></code>	Configures the maximum rate and maximum number of packets queue 7 allows.	C	13
<code>queue6 max-rate <rate> depth <depth></code>	Configures the maximum rate queue 6 allows.	C	13
<code>queue5 max-rate <rate> depth <depth></code>	Configures the maximum rate queue 5 allows.	C	13
<code>queue4 max-rate <rate> depth <depth></code>	Configures the maximum rate queue 4 allows.	C	13
<code>queue3 max-rate <rate> depth <depth></code>	Configures the maximum rate queue 3 allows.	C	13
<code>queue2 max-rate <rate> depth <depth></code>	Configures the maximum rate queue 2 allows.	C	13
<code>queue1 max-rate <rate> depth <depth></code>	Configures the maximum rate queue 1 allows.	C	13
<code>queue0 max-rate <rate> depth <depth></code>	Configures the maximum rate queue 0 allows.	C	13
<code>no qos shaping-profile <name></code>	Removes the specified shaping profile.	C	13
<code>show qos shaping-profile [name]</code>	Displays all shaping profiles or the specified one.	C	13
<code>qos wrr-wfq-profile <name></code>	Enters the sub-command mode for configuring the specified WRR/WFQ profile.	C	13
<code>exit</code>	Leaves the shaping profile sub-command mode.	C	13
<code>queue7 weight <weight> depth <depth></code>	Configures the weight and maximum number of packets queue 7 allows.	C	13
<code>queue6 weight <weight> depth <depth></code>	Configures the weight and maximum number of packets queue 6 allows.	C	13
<code>queue5 weight <weight> depth <depth></code>	Configures the weight and maximum number of packets queue 5 allows.	C	13

Table 256 QoS Commands Summary (continued)

COMMAND	DESCRIPTION	M	P
queue4 weight <weight> depth <depth>	Configures the weight and maximum number of packets queue 4 allows.	C	13
queue3 weight <weight> depth <depth>	Configures the weight and maximum number of packets queue 3 allows.	C	13
queue2 weight <weight> depth <depth>	Configures the weight and maximum number of packets queue 2 allows.	C	13
queue1 weight <weight> depth <depth>	Configures the weight and maximum number of packets queue 1 allows.	C	13
queue0 weight <weight> depth <depth>	Configures the weight and maximum number of packets queue 0 allows.	C	13
no qos wrr-wfq-profile <name>	Removes the specified WRR/WFQ profile.	C	13
show qos wrr-wfq-profile [name]	Displays all WRR/WFQ profiles or the specified one.	E	13
qos queue-mapping	Enters the sub-command mode for configuring priority bit (pbit) to queue mapping.	C	13
exit	Leaves the pbit to queue mapping sub-command mode.	C	13
pbit7 <queue-id>	Maps pbit 7 to the specified queue.	C	13
pbit6 <queue-id>	Maps pbit 6 to the specified queue.	C	13
pbit5 <queue-id>	Maps pbit 5 to the specified queue.	C	13
pbit4 <queue-id>	Maps pbit 4 to the specified queue.	C	13
pbit3 <queue-id>	Maps pbit 3 to the specified queue.	C	13
pbit2 <queue-id>	Maps pbit 2 to the specified queue.	C	13
pbit1 <queue-id>	Maps pbit 1 to the specified queue.	C	13
pbit0 <queue-id>	Maps pbit 0 to the specified queue.	C	13
show qos queue-mapping	Displays the pbit to queue ID mapping.	E	13
qos vc-shaping-profile <name>	Enters the sub-command mode for configuring a VC shaping profile.	C	13
exit	Leaves the VC shaping profile sub-command mode.	C	13
max-rate <rate>	Configures the maximum shaping rate.	C	13
max-queue-depth <depth>	Configures the maximum shaping rate.	C	13
no qos vc-shaping-profile <name>	Removes the specified VC shaping profile.	C	13
show qos vc-shaping-profile [name]	Displays all VC shaping profiles or the specified one.	E	13

33.2.1 Command Examples

This example shows how to map priority bits 0 and 1 to queue 2 and map priority bits 6 and 7 to queue 5. This results in strict-priority queuing QoS for traffic going out the uplink port.

```

ras# show qos queue-mapping
pri:  0  1  2  3  4  5  6  7
qid:  0  1  2  3  4  5  6  7
ras# config
ras(config)# qos queue-mapping
ras(config-QosQueueMapping)# pbit0 2
ras(config-QosQueueMapping)# pbit1 2
ras(config-QosQueueMapping)# pbit6 5
ras(config-QosQueueMapping)# pbit7 5
ras(config-QosQueueMapping)# exit
ras(config)# exit
ras# show qos queue-mapping
pri:  0  1  2  3  4  5  6  7
qid:  2  2  2  3  4  5  5  5
ras#

```

This example configures a weighted fair queuing profile with extra weight for queues 0-2 and sets slot 2's DSL port 4 to use it.

```

ras# config
ras(config)# qos wrr-wfq-profile test
ras(qos wrr-wfq-profile)# queue7 weight 50 depth 255
ras(qos wrr-wfq-profile)# queue6 weight 50 depth 255
ras(qos wrr-wfq-profile)# queue5 weight 50 depth 255
ras(qos wrr-wfq-profile)# queue4 weight 50 depth 255
ras(qos wrr-wfq-profile)# queue3 weight 50 depth 255
ras(qos wrr-wfq-profile)# queue2 weight 70 depth 255
ras(qos wrr-wfq-profile)# queue1 weight 70 depth 255
ras(qos wrr-wfq-profile)# queue0 weight 70 depth 255
ras(qos wrr-wfq-profile)# exit
ras(config)# interface dsl 2/4
ras(config-interface-dsl-2/4)# qos algorithm wfq
ras(config-interface-dsl-2/4)# qos weight-profile test
ras(config-interface-dsl-2/4)# exit
ras(config)# exit
ras#

```

This example configures a WRR-WFQ profile on all ports of the line card in slot 2 and assigns weight values (1,2,3,4,12,13,14,15) to the physical queues (0 to 7). This example also configures all the ports to use WFQ QoS algorithm with a maximum rate 50000 kbps.

```

ras# config
ras(config)# qos wrr-wfq-profile EXAMPLE
ras(config-wrr-wfq-profile-EXAMPLE)# queue7 weight 15 depth 255
ras(config-wrr-wfq-profile-EXAMPLE)# queue6 weight 14 depth 255
ras(config-wrr-wfq-profile-EXAMPLE)# queue5 weight 13 depth 255
ras(config-wrr-wfq-profile-EXAMPLE)# queue4 weight 12 depth 255
ras(config-wrr-wfq-profile-EXAMPLE)# queue3 weight 4 depth 255
ras(config-wrr-wfq-profile-EXAMPLE)# queue2 weight 3 depth 255
ras(config-wrr-wfq-profile-EXAMPLE)# queue1 weight 2 depth 255
ras(config-wrr-wfq-profile-EXAMPLE)# queue0 weight 1 depth 255
ras(config-wrr-wfq-profile-EXAMPLE)# exit
ras(config)# exit
ras# show qos wrr-wfq-profile EXAMPLE
wrr-wfq-profile Name:EXAMPLE
  queue id:      0      1      2      3      4      5      6      7
  weight:        1      2      3      4     12     13     14     15
  depth:        255     255     255     255     255     255     255     255

ras(config)# interface dsl 2/*
ras(config-interface-dsl-2/*)# qos algorithm wfq
ras(config-interface-dsl-2/*)# qos weight-profile EXAMPLE
ras(config-interface-dsl-2/*)# qos max-rate 50000
ras(config-interface-dsl-2/*)# exit

```

This example configures a shaping profile, EXAMPLE2. The maximum rate is 50000 kbps for queues 0 to 2 and 75000 kbps for queues 3 to 5. Then it assigns this profile to port 1 of the line card in slot 2. This example also shows the EXAMPLE2 QoS shaping profile's settings. Note that the default maximum rate of a port is 100000 kbps with a depth of 255 packets.

```

ras# config
ras(config)# qos shaping-profile EXAMPLE2
ras(config-shaping-profile-EXAMPLE2)# queue0 max-rate 50000 depth 255
ras(config-shaping-profile-EXAMPLE2)# queue1 max-rate 50000 depth 255
ras(config-shaping-profile-EXAMPLE2)# queue2 max-rate 50000 depth 255
ras(config-shaping-profile-EXAMPLE2)# queue3 max-rate 75000 depth 255
ras(config-shaping-profile-EXAMPLE2)# queue4 max-rate 75000 depth 255
ras(config-shaping-profile-EXAMPLE2)# queue5 max-rate 75000 depth 255
ras(config-shaping-profile-EXAMPLE2)# exit
ras(config)# interface dsl 2/1
ras(config-interface-dsl-2/1)# qos shaping-profile EXAMPLE2
ras(config-interface-dsl-2/1)# exit
ras(config)# exit
ras# show qos shaping-profile EXAMPLE2

shapingProfile Name:EXAMPLE2
  queue id:      0      1      2      3      4      5      6      7
  max rate: 50000 50000 50000 75000 75000 75000 100000 100000
  depth:      255     255     255     255     255     255     255     255
ras#

```

This example shows how to configure two VC-shaping profiles. One is EXAMPLE-50M with a maximum rate of 50000 kbps and a depth of 100 packets. The other one is EXAMPLE-75M with a maximum rate of 75000 kbps and a depth of 100 packets. This example shows the configuration result at the end.

```

ras# config
ras(config)# qos vc-shaping-profile EXAMPLE-50M
ras(config-QosVcShaping-EXAMPLE-50M)# max-rate 50000
ras(config-QosVcShaping-EXAMPLE-50M)# depth 100
ras(config-QosVcShaping-EXAMPLE-50M)# exit
ras(config)# qos vc-shaping-profile EXAMPLE-75M
ras(config-QosVcShaping-EXAMPLE-75M)# max-rate 75000
ras(config-QosVcShaping-EXAMPLE-75M)# depth 100
ras(config-QosVcShaping-EXAMPLE-75M)# exit
ras(config)# exit
ras# show qos vc-shaping-profile

VC shapingProfile Name:DEFVAL
  max rate:100000
  depth:255

VC shapingProfile Name:EXAMPLE-50M
  max rate:50000
  depth:100

VC shapingProfile Name:EXAMPLE-75M
  max rate:75000
  depth:100

ras#

```

This example shows how to enable ATM VC shaping. Then configure priorities 0, 1, 2 for ATM VC channels 0/33, 0/34 and 0/35 respectively and apply the profiles configured in the previous example to the channels on all ports of the line card in slot 2.

```

ras# config
ras(config)# qos atm vc-shaping
ras(config)# interface dsl 2/*
ras(config-interface-dsl-2/*)# atm-vc 0/33 llc priority 0
ras(config-interface-dsl-2/*)# atm-vc 0/34 llc priority 1
ras(config-interface-dsl-2/*)# atm-vc 0/35 llc priority 2
ras(config-interface-dsl-2/*)# qos atm-vc 0/33 vc-shaping-profile EXAMPLE-75M
ras(config-interface-dsl-2/*)# qos atm-vc 0/34 vc-shaping-profile EXAMPLE-50M
ras(config-interface-dsl-2/*)# qos atm-vc 0/35 vc-shaping-profile EXAMPLE-50M
ras(config-interface-dsl-2/*)# exit

```

CHAPTER 34

Static Route

Use these commands to configure static routes to tell the IES how to forward IP traffic.

The IES uses IP for communication with management computers, for example using Telnet, SSH, or SNMP. Use IP static routes to have the IES respond to remote management stations that are not reachable through the default gateway. The IES can also use static routes to send data to a server or device that is not reachable through the default gateway, for example when sending SNMP traps or using ping to test IP connectivity.

The following section lists the commands for this feature.

Table 257 Static Route Commands Summary

COMMAND	DESCRIPTION	M	P
show ip route	Displays the IP routing table.	E	13
show ip route static	Displays the static routes.	E	13
ip route <ip-address>/<mask> <next-hop-ip>	Creates a static route. If the <ip-address> <mask> already exists, the IES deletes the existing route first. <i>next-hop-ip</i> : IP address of the next device. 0.0.0.0-223.255.255.255	C	13
no ip route <ip-address>/<mask>	Removes a specified static route.	C	13

CHAPTER 35

VDSL

Use these commands to configure VDSL settings on VDSL subscriber ports.

Very High Bit Rate DSL (VDSL) is an asymmetric version of DSL that is used as the final drop from a fiber optic junction point to nearby customers. VDSL lets an apartment or office complex obtain high-bandwidth services using existing copper wires without having to replace the infrastructure with optical fiber. Like ADSL, VDSL can share the line with the telephone. VDSL2 (Very High Speed Digital Subscriber Line 2) is the second generation of the VDSL standard (which is currently denoted VDSL1). VDSL2 allows a frequency band of up to 30MHz and transmission rates of up to 100 Mbps in each direction. VDSL2 is defined in G.993.2.

Here is some background information about the key VDSL settings and features you can configure.

Power Spectrum Density

Power Spectrum Density (PSD) mask. PSD defines the distribution of a line's power in the frequency domain. A PSD mask is a template that specifies the maximum allowable PSD for a line.

Limit PSD Mask

To reduce the impact of interference and attenuation, ITU-T 993.2 specifies a PSD mask to limit the VDSL2 transmitters PSD at both downstream and upstream.

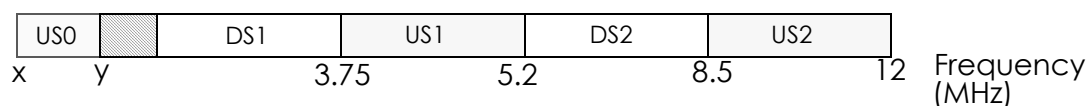
Frequency Band Plan

Each VDSL mode operates in a different frequency band allocation, resulting in different upstream and downstream speeds. Your system automatically changes the band plan based on the loop condition and loop length.

A band plan example is shown next. Band plans include an optional band (between 25 kHz and 276 kHz) controlled by "limit PSD mask".

The optional band is used for upstream transmission which is to be negotiated during line initiation. The optional band frequency (for example, **x** and **y**) varies depending on the limit PSD mask you use.

Figure 247 A Band Plan Example



A sample of optional band PSD masks and associated frequency bands used in the Device is shown next.

Table 258 Optional band PSD mask

LIMIT PSD MASK		OPTIONAL BAND FREQUENCY
nus0_d32	=	No optional band
eu32_d32	=	25-138 kHz
eu36_d48	=	25-155.25 kHz
...		

The "eu" number in the limit PSD mask is a tone index. A tone spacing, 4.3125 KHz, is used for VDSL2 profile from 8a up to 17a. So "eu32" means the optional band ending at around 138 kHz.

VDSL2 Profiles

The following table lists the supported Annex A VDSL2 profiles defined by the VDSL standard. Refer to the ITU G.993.2 specifications for more information on other profiles. The VDSL2 profiles available in an individual VDSL2 line card varies.

Table 259 Supported VDSL2 profiles (annex A)

PROFILE	8A	8B	8C	8D	12A	12B	17A
Bandwidth (MHz)	8.5	8.5	8.5	8.5	8.5	8.5	17.66
Tone	1972	1972	1972	1972	1972	1972	4096
Tone Spacing (kHz)	4.3125	4.3125	4.3125	4.3125	4.3125	4.3125	4.3125
Line Power (dBm)	+17.5	+20.5	+11.5	+14.5	+14.5	+14.5	+14.5

Configured Versus Actual Rate

You configure the maximum rate of an individual DSL port by modifying its profile or assigning a different profile to the port. However, the actual rate varies depending on factors such as transmission range and interference.

Impulse Noise Protection (INP)

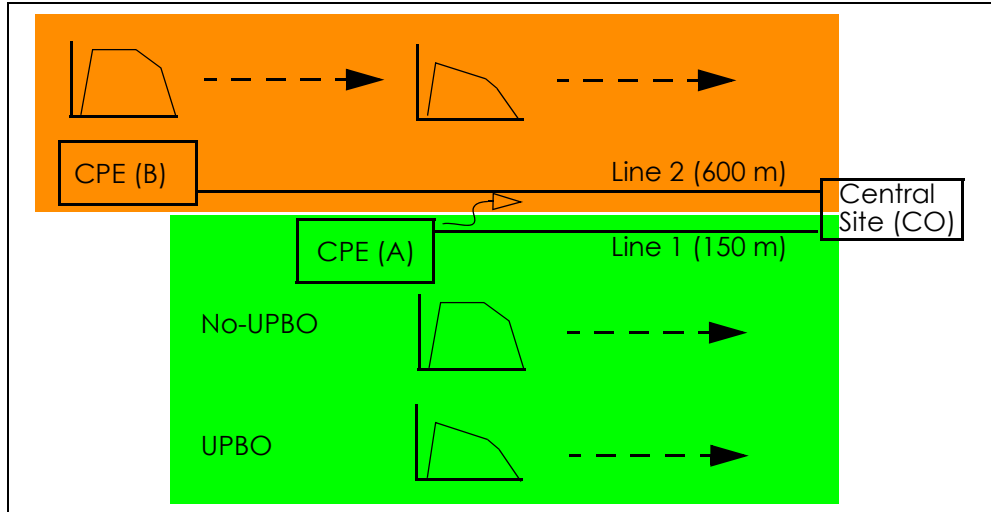
Sudden spikes in the line's noise level (external noise) can cause errors and result in lost packets. Set the impulse noise protection minimum to have a buffer to protect the DSL physical layer against impulse noise. This buffering causes a delay that reduces transfer speeds. It is recommended you use a non-zero setting for real-time traffic that has no error correction (such as video-conferencing). The number of DMT (Discrete Multi-Tone) symbols specifies the time in which errors can be completely corrected. A higher symbol value provides higher error correction capability, but it causes overhead and higher delay which may increase error rates in received multimedia data.

UPBO

In a network with varying telephone wiring lengths, the PSD on each line is different. This causes crosstalk between the lines. Enable UPBO (Upstream Power Back Off) to allow the device to adjust the transmit PSD of all lines based on a reference line length. This mitigates the upstream crosstalk on shorter loops to longer loops. It allows the switch to provide better service in a network environment with telephone wiring of varying lengths.

An example is shown below. **Line 1** and **Line 2** are in the same cable binder. Crosstalk occurs when the signal flows and is near to **CPE (A)**'s location. Besides, higher **Line 1** PSD causes higher interference to the **Line 2**. **CO** receives signal with higher attenuation. With UPBO enabled on the **CPE (A)**, it decreases the PSD level and reduces the crosstalk impact on long loops.

Figure 248 UPBO Resolves Upstream Far-End Crosstalk



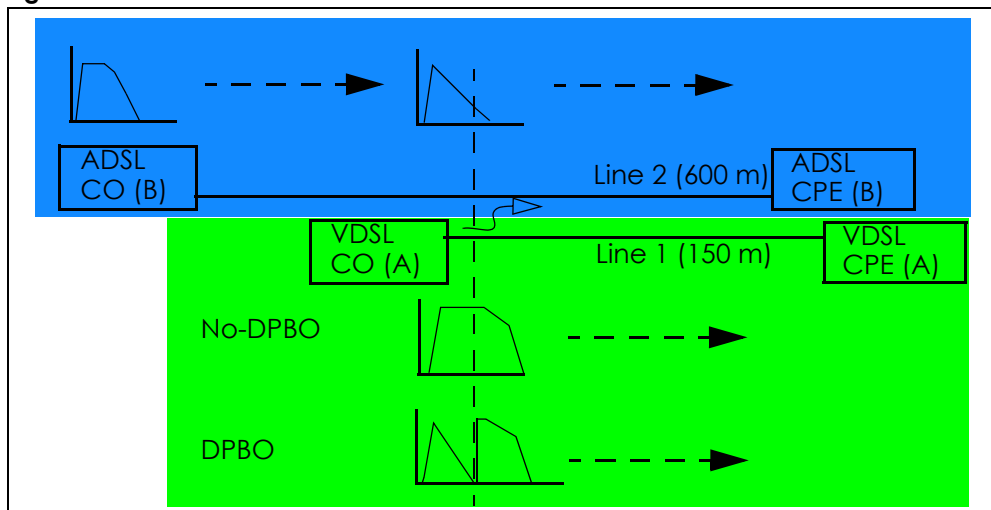
DPBO

VDSL signals may interfere with other services (such as ISDN, ADSL or ADSL2 provided by other devices) on the same bundle of lines due to downstream far-end crosstalk. DPBO (Downstream Power Back Off) can reduce performance degradation by changing the PSD level on the IES at the street cabinet level.

ISDN in Europe uses a frequency range of up to 80 kHz, while ISDN in Japan uses a frequency range of up to 640 kHz. ADSL utilizes the 1.1 MHz band. Both ADSL2 and ADSL 2+ utilize the 2.2 MHz band.

An example is shown next. VDSL **Line 1** and ADSL **Line 2** are in the same binder. Crosstalk occurs when the ADSL signal flows from **CO (B)** and is near to **CO (A)**'s location. Besides, higher **Line 1** PSD causes higher interference to the **Line 2**. **CPE (B)** receives signal with higher attenuation. With DPBO enabled on the **CO (A)**, it decreases the PSD level and reduces the crosstalk impact on other service lines.

Figure 249 DPBO Resolves Downstream Far-End Crosstalk



UPBO/DPBO Electrical Length

The distance between a cabinet and the central office is an important parameter of DPBO settings as mentioned in [Section on page 406](#). The electrical length is used instead of the real physical distance according to G.997.1 format. Depending on the cable type, the line used and physical line length, you can calculate the electrical length (in dB). For example, if the distance is 1 kilometer and you use 24 AWG cable type, the electrical length 20.5 dB is recommended.

The following table displays the calculation from a real length to an electrical length.

Table 260 Real length to electrical length

CABLE TYPE	REAL LENGTH TO ELECTRICAL LENGTH	A	B	C
22 AWG	=16.2*(cable length in kilometer)	0	0	0
24 AWG	=20.5*(cable length in kilometer)	0	1	0
26 AWG	=25.8*(cable length in kilometer)	0	1.0039065	-0.0039065

Rate Adaption

Rate adaption is the ability of a device to adjust from the configured transmission rate to the attainable transmission rate automatically depending on the line quality. The VDSL transmission rate then stays at the new rate or adjusts if line quality improves or deteriorates.

The switch determines line quality using the Signal-to-Noise Ratio (SNR). SNR is the ratio of the amplitude of the actual signal to the amplitude of noise signals at a given point in time. A low SNR indicates poor line quality.

RFI (Radio Frequency Interference)

RFI is induced noise on the lines by surrounding radio frequency electromagnetic radiation from sources such as AM and HAM radio stations. Since VDSL uses a much larger frequency range that overlaps with other radio frequency systems, signals from VDSL lines and other radio systems interfere with each other. To avoid performance degradation due to RFI, set the switch to not transmit VDSL signals in the RFI band defined by the regulatory bodies (ETSI and ANSI). You can also configure your own RFI bands on the system.

Downstream and Upstream

Downstream refers to traffic going out from the line card to the subscriber's DSL modem or router. Upstream refers to traffic coming into the line card from the subscriber's DSL modem or router.

DSL Profiles

A DSL profile is a table that contains a list of pre-configured DSL settings. Each DSL port has one (and only one) profile assigned to it at any given time. You can configure multiple profiles, including profiles for troubleshooting. Profiles allow you to configure DSL ports efficiently. You can configure many DSL ports with the same profile, thus removing the need to configure the settings of each DSL port one-by-one. You can also change an individual DSL port's settings by assigning it a different profile.

For example, you could set up different profiles for different kinds of accounts (for example, economy, standard and premium). Assign the appropriate profile to an DSL port and it takes care of a large part of

the port's configuration. You still get to individually enable or disable each port and configure port specific settings. See the chapter on profiles for how to configure DSL profiles.

Alarm Profiles

Alarm profiles define DSL port alarm thresholds. The system sends an alarm trap and generates a syslog entry when the thresholds of the alarm profile are exceeded. See the chapter on profiles for how to configure alarm profiles.

Latency Delay

Latency delay is the number of milliseconds of interleave delay. Interleave delay determines the size of a single block of data to be interleaved (assembled) and then transmitted. Use interleave delay when transmission error correction (Reed- Solomon) is necessary due to a less than ideal telephone line. It is recommended that you configure the same latency delay for both upstream and downstream.

35.1 VDSL Commands

The following table describes commonly used parameter notation for these commands.

Table 261 VDSL Command Parameters

NOTATION	DESCRIPTION
<i>name</i>	A name of up to 31 printable characters.
<i>max-rate</i>	The maximum transmission rate, 64-128000 in kbps.
<i>min-rate</i>	The minimum transmission rate, 32-128000 in kbps.
<i>min-inp</i>	The minimum number of Impulse Noise Protection (INP) Discrete Multi-Tone (DMT) symbols. 0-32 in 0.5 symbol steps, default: 4.
<i>upshift-nrm</i>	The upshift noise margin 0-310 in steps of 0.1 dB, default: 90
<i>downshift-nrm</i>	The downshift noise margin 0-310 in steps of 0.1 dB, default: 30
<i>upshift-time</i>	The rate adaption upshift time. 0-16383 in seconds, default: 30
<i>downshift-time</i>	The rate adaption downshift time. 0-16383 in seconds, default: 30
<i>target-snr</i>	The target Signal to Noise Ratio (SNR) margin. 0-310 in step of 0.1 dB, default: 60
<i>max-snr</i>	The maximum SNR margin. 0-310 in step of 0.1 dB, default: 310
<i>min-snr</i>	The minimum SNR margin. 0-310 in step of 0.1 dB, default: 0

The following section lists the commands for this feature.

Table 262 VDSL Commands Summary

COMMAND	DESCRIPTION	M	P
<code>no dsl channel-profile <name></code>	Removes the specified DSL channel profile.	C	13
<code>show dsl channel-profile [name]</code>	Displays the names of all the DSL channel profiles if a name is not specified or the contents of the specified DSL channel profile.	E	13
<code>dsl channel-profile <name></code>	Enters the sub-command mode for configuring the specified DSL channel profile.	C	13
<code>exit</code>	Leaves the DSL channel profile configuration sub-command mode.	C	13

Table 262 VDSL Commands Summary (continued)

COMMAND	DESCRIPTION	M	P
<code>rate-ds <max-rate> <min-rate></code>	Configures the maximum and minimum downstream rates.	C	13
<code>rate-us <max-rate> <min-rate></code>	Configures the maximum and minimum upstream rates.	C	13
<code>max-delay-ds <delay></code>	Configure the maximum downstream latency delay, 0-63 in ms.	C	13
<code>max-delay-us <delay></code>	Configure the minimum downstream latency delay, 0-63 in ms.	C	13
<code>min-inp-ds <min-inp></code>	Configures the downstream minimum Impulse Noise Protection (INP) for a 4.3125 KHz carrier space DSL link. 0-32	C	13
<code>min-inp-us <min-inp></code>	Configures the upstream minimum INP for a 4.3125 KHz carrier space DSL link. 0-32	C	13
<code>min-inp8-ds <min-inp></code>	Configures the downstream minimum INP for a 8.625 KHz carrier space DSL link. 0-32	C	13
<code>min-inp8-us <min-inp></code>	Configures the upstream minimum INP for a 8.625 KHz carrier space DSL link. 0-32	C	13
<code>phyr-ds enable disable auto</code>	Configures PhyR (physical layer protection) for downstream traffic. Turn it on or off or have the IES use it automatically. PhyR has the same function as INP (Impulse Noise Protection) but is more effective.	C	13
<code>phyr-us enable disable auto</code>	Configures PhyR (physical layer protection) for upstream traffic. Turn it on or off or have the IES use it automatically. PhyR has the same function as INP (Impulse Noise Protection) but is more effective.	C	13
<code>no dsl line-profile <name></code>	Removes the specified DSL line profile.	C	13
<code>show dsl line-profile [name]</code>	Displays the names of all the DSL line profiles if a name is not specified or the contents of the specified DSL line profile.	E	13
<code>dsl line-profile <name></code>	Enters the sub-command mode for configuring the specified DSL line profile.	C	13
<code>exit</code>	Leaves the DSL line profile configuration sub-command mode.		
<code>ra-mode-ds</code> <code>manual rainit dynamicra</code>	Configures the downstream rate adaption mode. manual: no rate adaption rainit: rate adaption during initialization process only dynamicra: rate adaption during initialization process and showtime default: init	C	13
<code>ra-mode-us</code> <code>manual rainit dynamicra</code>	Configures the upstream rate adaption mode. manual: no rate adaption rainit: rate adaption during initialization process only dynamicra: rate adaption during initialization process and showtime default: init	C	13
<code>ra-nrm-ds <upshift-nrm></code> <code><downshift-nrm></code>	Configures the downstream rate adaption upshift and downshift noise margins	C	13
<code>ra-nrm-us <upshift-nrm></code> <code><downshift-nrm></code>	Configures the upstream rate adaption upshift and downshift noise margins	C	13
<code>ra-time-ds <upshift-time></code> <code><downshift-time></code>	Configures the downstream rate adaption upshift and downshift times.	C	13
<code>ra-time-us <upshift-time></code> <code><downshift-time></code>	Configures the upstream rate adaption upshift and downshift times.	C	13
<code>snrm-ds <target-snrm> <max-snrm></code> <code><min-snrm></code>	Configures the downstream target, maximum, and minimum Signal to Noise Ratio (SNR) margins.	C	13

Table 262 VDSL Commands Summary (continued)

COMMAND	DESCRIPTION	M	P
<code>snrm-us <target-snr> <max-snr> <min-snr></code>	Configures the upstream target, maximum, and minimum SNR margins.	C	13
<code>min-msg-rate-ds <min-msg-rate></code>	Configures the downstream minimum overhead message rate. <i>min-msg-rate</i> : 4000-236000 in bits per second	C	13
<code>min-msg-rate-us <min-msg-rate></code>	Configures the upstream minimum overhead message rate <i>min-msg-rate</i> : 4000-236000 in bits per second	C	13
<code>psd-mask-ds <carrier-index> <psd> [<carrier-index> <psd> ...]</code>	Configures a customized downstream Power Spectrum Density (PSD) mask. <i>carrier-index</i> : The sub-carrier tone index 0-4095. <i>psd</i> : 0-200 or 255. 0 = -140dBm/Hz, -200 = -40 dBm/Hz in step of 0.5 dBm/Hz, 255 = 0 W/Hz	C	13
<code>psd-mask-us <carrier-index> <psd> [<carrier-index> <psd> ...]</code>	Configures a customized upstream PSD mask. <i>carrier-index</i> : The sub-carrier tone index 0-4095. <i>psd</i> : 0- 200 or 255. 0 = -140dBm/Hz, -200 = -40 dBm/Hz in step of 0.5 dBm/Hz, 255 = 0 W/Hz	C	13
<code>max-nor-atp-ds <tx-power></code>	Configures the downstream maximum nominal aggregation transmit power. <i>tx-power</i> : 0-255 in step of 0.1 dB, default: 200	C	13
<code>max-nor-atp-us <tx-power></code>	Configures the upstream maximum nominal aggregation transmit power. <i>tx-power</i> : 0-255 in step of 0.1 dB, default: 130	C	13
<code>max-arp-us <rx-power></code>	Configures the upstream maximum aggregation receive power. <i>rx-power</i> : -255-255 in step of 0.1dB, default: 130	C	13
<code>pm-mode allow-l3 allow-l2 allow-both</code>	Configures the power management operating mode (used for ADSL2 and ADSL2+ protocol). <i>allow-l3</i> : Allows the DSL line to autonomously change to idle (L3) state. <i>allow-l2</i> : Allows the DSL line to autonomously change to low power (L2) state. <i>allow-both</i> : Allows the DSL line to autonomously change to idle (L3) state and low power (L2) state.	C	13
<code>no pm-mode</code>	Disables power management (used for ADSL2 and ADSL2+ protocol).	C	13
<code>pm-parameters <l0-time> <l2-time> <l2-power-down-step> <l2-power-down-max></code>	Sets the L0 (full power) and L2 (low power) power mode transition settings (used for ADSL2 and ADSL2+ protocol). <i>l0-time</i> : Time (0-255 seconds) to stay in L0 mode. <i>l2-time</i> : Time (0-255 seconds) to wait before performing another power trim in L2 mode. <i>l2-power-down-step</i> : Maximum total aggregate power reduction in dB (0-15) per power trim in L2 mode, default: 1 <i>l2-power-down-max</i> : Maximum total aggregate power reduction in dB (0-15) in L2 mode, default: 6	C	13

Table 262 VDSL Commands Summary (continued)

COMMAND	DESCRIPTION	M	P
<code>rfiband <start-carrier> <end-carrier> [<start-carrier> <end-carrier> ...]</code>	Configures and enables Notch Frequency Interference (RFI) bands. <i>start-carrier</i> : 0-4096 <i>end-carrier</i> : 0-4096	C	13
<code>no rfiband</code>	Disables Notch Frequency Interference (RFI) bands.	C	13
<code>bitswap-ds inactive</code>	Disables downstream bit swap.	C	13
<code>bitswap-us inactive</code>	Disables upstream bit swap.	C	13
<code>no bitswap-ds inactive</code>	Enables downstream bit swap.	C	13
<code>no bitswap-us inactive</code>	Enables upstream bit swap.	C	13
<code>snr-mode-ds</code>	Enables downstream virtual noise (used for VDSL2 protocol).	C	13
<code>snr-mode-us</code>	Enables upstream virtual noise (used for VDSL2 protocol).	C	13
<code>no snr-mode-ds</code>	Disables downstream virtual noise (used for VDSL2 protocol).	C	13
<code>no snr-mode-us</code>	Disables upstream virtual noise (used for VDSL2 protocol).	C	13
<code>refvn-ds <carrier-index> <vn-psd> [<carrier-index> <vn-psd> ...]</code>	Configures the downstream virtual noise PSD level by defining the break points (used for VDSL2 protocol). <i>carrier-index</i> : 0-4095 <i>vn-psd</i> : 0-200 or 255. 0 = -140dBm/Hz, -200 = -40 dBm/Hz in steps of 0.5 dBm/Hz, 255 = 0 W/Hz	C	13
<code>refvn-us <carrier-index> <vn-psd> [<carrier-index> <vn-psd>...]</code>	Configures the upstream virtual noise PSD level by defining the break points (used for VDSL2 protocol). <i>carrier-index</i> : 0-4095 <i>vn-psd</i> : 0-200 or 255. 0 = -140dBm/Hz, -200 = -40 dBm/Hz in steps of 0.5 dBm/Hz, 255 = 0 W/Hz	C	13
<code>no refvn-ds</code>	Disables the downstream PSD mask.	C	13
<code>no refvn-us</code>	Disables the upstream PSD mask.	C	13
<code>dpbo-escm-a <escm-a></code>	Configures Downstream Power Back Off (DPBO) E-side Cable Model (ESCM) parameter A (used for VDSL2 protocol). <i>escm-a</i> : 0-640. 0: -1, 640: 1.5 in steps of 2 ⁻⁸ default: 256	C	13
<code>dpbo-escm-b <escm-b></code>	Configures DPBO E-side Cable Model (ESCM) parameter B (used for VDSL2 protocol). <i>escm-b</i> : 0-640. 0: -1, 640: 1.5 in steps of 2 ⁻⁸ default: 512	C	13
<code>dpbo-escm-c <escm-c></code>	Configures DPBO E-side Cable Model (ESCM) parameter C (used for VDSL2 protocol). <i>escm-c</i> : 0-640. 0: -1, 640: 1.5 in steps of 2 ⁻⁸ default: 256	C	13
<code>dpbo-esel <esel></code>	Configures DPBO E-side cable Electrical Length (used for VDSL2 protocol). <i>esel</i> : 0-511. 0: 0dB, 511: 255.5dB in steps of 0.5 dB default: 0	C	13

Table 262 VDSL Commands Summary (continued)

COMMAND	DESCRIPTION	M	P
<code>dpbo-mus <mus></code>	Configures the DPBO Minimum Usable received PSD mask (used for VDSL2 protocol). <i>mus</i> : 0-255. 0: 0dBm/Hz, 255: -127.5dBm/Hz in steps of -0.5 dBm/Hz default: 180	C	13
<code>dpbo-fmax <fmax></code>	Configures the DPBO maximum frequency (used for VDSL2 protocol). <i>fmax</i> : 32-6959. 32: 138 KHz, 6959: 30010 KHz in steps of 4.3125 KHz default: 512	C	13
<code>dpbo-fmin <fmin></code>	Configures the DPBO minimum frequency (used for VDSL2 protocol). <i>fmin</i> : 0-2048. 0: 0KHz, 2048: 8832 KHz in steps of 4.3125 KHz default: 32	C	13
<code>dbpo-epsd <carrier-index> <epsd> [<carrier-index> <epsd> ...]</code>	Configures the DPBO PSD mask used at exchange (used for VDSL2 protocol). <i>carrier-index</i> : 0-4095 <i>epsd</i> : 0-190. scalar value 0--95dBm in steps of -0.5dBm	C	13
<code>dbpo-epsd <psdid></code>	Configures the DBPO standard PSB mask (used for VDSL2 protocol). <i>psdid</i> : 1-6. 1: psd_co, 2: psd-flat, 3: psd_cab_ansi, 4: psd_cab_etsi, 5: psd_exch_etsi, 6:psd_exch_ansi	C	13
<code>upbo-kl <kl></code>	Configures the Upstream Power Back Off (UPBO) electrical length (used for VDSL2 protocol). <i>kl</i> : 0-1280 in 0.1 dB default: 0	C	13
<code>upbo-klf auto override</code>	Configures the UPBO force mode (used for VDSL2 protocol). <i>auto</i> : DSL autonomously determines the electrical length <i>override</i> : force to utilize configured UPBO kl as electrical length default: disable	C	13
<code>no upbo-klf</code>	Disables UPBO (used for VDSL2 protocol).	C	13
<code>upbo-psd-a <psd-a></code>	Configures UPBO referenced PSD parameter A (used for VDSL2 protocol). <i>psd-a</i> : 4000-8095 in 0.01 dBm/Hz	C	13
<code>upbo-psd-b <psd-b></code>	Configures UPBO referenced PSD parameter B. <i>psd-b</i> : 0-4095 in 0.01 dBm/Hz	C	13
<code>vdsl2-profile <vdsl2_profile_list></code>	Configures the list of allowed VDSL2 profiles (used for VDSL2 protocol). <i>vdsl2_profile_list</i> : list of (8a, 8b, 8c, 8d, 12a, 12b, 17a) default: 8a,8b,8c,8d,12a,12b,17a	C	13
<code>limit-mask <limit-mask></code>	Configures the standard PSD mask. <i>limit-mask</i> : d32, d48, d64, d128, b7-1 to b7-10, b8-1 to b8-16 default: d32	C	13
<code>us0-band</code>	Enables the upstream band 0 (used for VDSL2 protocol).	C	13
<code>no us0-band</code>	Disables the upstream band 0 (used for VDSL2 protocol).	C	13

Table 262 VDSL Commands Summary (continued)

COMMAND	DESCRIPTION	M	P
<code>us0-mask <us0-mask></code>	Configures standard upstream band 0 PSD mask. <i>us0-mask</i> : eu32, eu36, eu40, eu44, eu48, eu52, eu56, eu60, eu64, or eu128 default: eu32	C	13
<code>transmission-type <type-list></code>	Configures the allowed DSL modes. <i>type-list</i> : list of vdsl2, adsl2+, adsl2, gdmr, t1413, glite, annex-m, annex-l, annex-j, and annex-i	C	13
<code>no dsl alarm-line-profile <name></code>	Removes the specified DSL alarm line profile.	C	13
<code>show dsl alarm-line-profile <name></code>	Displays the contents of the specified DSL alarm line profile.	E	13
<code>dsl alarm-line-profile <name></code>	Enters the sub-command mode for configuring the specified DSL alarm line profile.	C	13
<code>exit</code>	Leaves the DSL alarm line profile configuration sub-command mode.	C	13
<code>xtuc-15min-fecs-threshold <threshold></code>	Configures the number of Forward Error Correction Seconds (FECS) allowed on the system within 15 minutes. 0-900, default: 0.	C	13
<code>xtuc-15min-es-threshold <threshold></code>	Configures the number of Errored Seconds (ES) allowed on the system within 15 minutes. 0-900, default: 0.	C	13
<code>xtuc-15min-lofs-threshold <threshold></code>	Configures the number of Loss of Frame Seconds (LOFS) allowed on the system within 15 minutes. 0-900, default: 0.	C	13
<code>xtuc-15min-lprs-threshold <threshold></code>	Configures the number of Loss of Power Seconds (LPRS) allowed on the system within 15 minutes. 0-900, default: 0.	C	13
<code>xtuc-15min-ses-threshold <threshold></code>	Configures the number of Severely Errored Seconds (SES) allowed on the system within 15 minutes. 0-900, default: 0.	C	13
<code>xtuc-15min-loss-threshold <threshold></code>	Configures the number of Loss of Signal Seconds (LoSS) allowed on the system within 15 minutes. 0-900, default: 0.	C	13
<code>xtuc-15min-uas-threshold <threshold></code>	Configures the number of UnAvailable Seconds (UAS) errors allowed on the system within 15 minutes. 0-900, default: 0.	C	13
<code>xtur-15min-fecs-threshold <threshold></code>	Configures the number of Forward Error Correction Seconds (FECS) allowed on subscriber devices within 15 minutes. 0-900, default: 0.	C	13
<code>xtur-15min-es-threshold <threshold></code>	Configures the number of Errored Seconds (ES) allowed on subscriber devices within 15 minutes. 0-900, default: 0.	C	13
<code>xtur-15min-lofs-threshold <threshold></code>	Configures the number of Loss of Frame Seconds (LOFS) allowed on subscriber devices within 15 minutes. 0-900, default: 0.	C	13
<code>xtur-15min-lprs-threshold <threshold></code>	Configures the number of Loss of Power Seconds (LPRS) allowed on subscriber devices within 15 minutes. 0-900, default: 0.	C	13
<code>xtur-15min-ses-threshold <threshold></code>	Configures the number of Severely Errored Seconds (SES) allowed on subscriber devices within 15 minutes. 0-900, default: 0.	C	13
<code>xtur-15min-loss-threshold <threshold></code>	Configures the number of Loss of Signal Seconds (LoSS) allowed on subscriber devices within 15 minutes. 0-900, default: 0.	C	13
<code>xtur-15min-uas-threshold <threshold></code>	Configures the number of UnAvailable Seconds (UAS) errors allowed on subscriber devices within 15 minutes. 0-900, default: 0.	C	13
<code>15min-failed-full-init-threshold <threshold></code>	Configures the number of times a full initialization is allowed to fail on subscriber devices within 15 minutes. 0-2147483647, default: 0.	C	13
<code>no dsl alarm-channel-profile <name></code>	Removes the specified DSL alarm channel profile.	C	13

Table 262 VDSL Commands Summary (continued)

COMMAND	DESCRIPTION	M	P
show dsl alarm-channel-profile [name]	Displays the names of all the DSL alarm channel profiles if a name is not specified or the contents of the specified DSL alarm channel profile.	E	13
dsl alarm-channel-profile <name>	Enters the sub-command mode for configuring the specified DSL alarm channel profile.	C	13
exit	Leaves the DSL alarm channel profile configuration sub-command mode.	C	13
xtuc-15min-errcoding-threshold <threshold>	Configures the number of Code Violations (incorrect cyclic redundancy check) allowed on the system within 15 minutes. 0- 2147483647, default: 0.	C	13
xtuc-15min-corrected-threshold <threshold>	Configures the number of corrected error blocks allowed on the system within 15 minutes. 0- 2147483647, default: 0.	C	13
xtur-15min-errcoding-threshold <threshold>	Configures the number of Code Violations (incorrect cyclic redundancy check) allowed on the subscriber devices within 15 minutes. 0- 2147483647, default: 0.	C	13
xtur-15min-corrected-threshold <threshold>	Configures the number of corrected error blocks allowed on the subscriber devices within 15 minutes. 0- 2147483647, default: 0.	C	13
no dsl line-template <name>	Removes the specified DSL line template.	C	13
show dsl line-template [name]	Displays the names of all the DSL line templates if a name is not specified or the contents of the specified DSL line template.	E	13
dsl line-template <name>	Enters the sub-command mode for configuring the specified DSL line template.	C	13
exit	Leaves the DSL line template configuration sub-command mode.	C	13
channel-profile <name>	Configures the referenced DSL channel profile. Default: DEFVAL	C	13
line-profile <name>	Configures the referenced DSL line profile. Default: DEFVAL	C	13
no dsl alarm-template <name>	Removes the specified DSL alarm template.	C	13
show dsl alarm-template <name>	Displays the names of all the DSL alarm templates if a name is not specified or the contents of the specified DSL alarm template.	E	13
dsl alarm-template <name>	Enters the sub-command mode for configuring the specified DSL alarm template.	C	13
exit	Leaves the DSL alarm template configuration sub-command mode.	C	13
alarm-channel-profile <name>	Configures the referenced DSL alarm channel profile. Default: DEFVAL	C	13
alarm-line-profile <name>	Configures the referenced DSL alarm line profile. Default: DEFVAL	C	13
interface dsl <slot/portlist>	Enters the sub-command mode for configuring the specified DSL ports.	C	13
exit	Leaves the DSL port configuration.	C	13
active	Enables the specified DSL ports on the IES.	C	13
no active	Disables the specified DSL ports on the IES.	C	13
name <port-name-string>	Sets a name of up to 31 printable characters for the ports. Spaces are allowed.	C	13
line-template <line-template>	Configures the referenced DSL line template to the specified DSL ports. <i>line-template</i> : up to 31 printable characters	C	13

Table 262 VDSL Commands Summary (continued)

COMMAND	DESCRIPTION	M	P
<code>fallback-template <line-template></code>	Configures the specified DSL ports to use the specified DSL line template for fallback purposes. <i>line-template</i> : up to 31 printable characters	C	13
<code>alarm-template <alarm-template></code>	Configures the referenced DSL alarm template to the specified DSL ports. <i>line-template</i> : up to 31 printable characters, default is DEFVAL	C	13
<code>transmission-type auto vds12 adsl2+ adsl2 gdm glite t1413</code>	Configures the allowed transmission type. If the setting is undefined the system takes settings from the profile for transmission type, Annex M/L/I/J, power management, and TX power mode. If it is set, the system takes settings from port settings. <i>auto</i> : auto select transmission type. <i>vds12 adsl2+ adsl2 gdm glite t1413</i> : allow the specified protocol only.	C	13
<code>no transmission-type</code>	Removes the transmission type setting. The system takes the transmission type, Annex M/L/I/J, power management, TX power mode, and minimum INP settings from the line profile. This is the default setting.	C	13
<code>annexm active</code>	Enables Annex M. This is an ADSL setting.	C	13
<code>no annexm active</code>	Disables Annex M. This is an ADSL setting.	C	13
<code>annexl active</code>	Enables Annex L. This is an ADSL setting.	C	13
<code>no annexl active</code>	Disables Annex L. This is an ADSL setting.	C	13
<code>annexi active</code>	Enables Annex I. This is an ADSL setting.	C	13
<code>no annexi active</code>	Disables Annex I. This is an ADSL setting.	C	13
<code>annexj active</code>	Enables Annex J. This is an ADSL setting.	C	13
<code>no annexj active</code>	Disables Annex J. This is an ADSL setting.	C	13
<code>pm-mode allow-l3 allow-l2 allow-both</code>	Configures the power management operating mode (used for ADSL2 and ADSL2+ protocols only). <i>allow-l3</i> : DSL can automatically change to idle (L3) state. <i>allow-l2</i> : DSL can automatically change to low power (L2) state. <i>allow-both</i> : DSL can automatically change to idle (L3) and low power (L2) state.	C	13
<code>no pm-mode</code>	Disables power management operating mode.	C	13
<code>pm-parameters <l0-time> <l2-time> <l2-power-down-step> <l2-power-down-max></code>	Configures power management parameters (used for ADSL2 and ADSL2+ protocols). <i>l0-time</i> : 0-255 in seconds, default: 255 <i>l2-time</i> : 0-255 in seconds, default: 255 <i>l2-power-down-step</i> : 0-15 in dB, default: 1 <i>l2-power-down-max</i> : 0-15 in dB, default: 6	C	13

Table 262 VDSL Commands Summary (continued)

COMMAND	DESCRIPTION	M	P
power-mode fix rate power <max-us-txpower> <max-ds-txpower> <max-us-rxpower>	Configures TX power mode, maximum upstream/downstream transmit power, and maximum receive power at the ATU-C. fix rate power: TX power mode fix: fix to the maximum rate rate: priority to rate power: priority to power max-us-txpower: maximum upstream allowed transmit power, -130-200, the unit is 0.1 dBm max-ds-txpower: maximum downstream allowed transmit power, -50-200, the unit is 0.1 dBm max-us-rxpower: maximum aggregate receive power at the ATU-C, -255-255, the unit is 0.1 dBm	C	13
min-inp-ds <min-inp>	Configures downstream minimum INP for 4.3125 KHz carrier space DSL link. min-inp: 0-32	C	13
min-inp-us <min-inp>	Configures upstream minimum INP for 4.3125 KHz carrier space DSL link. min-inp: 0-32	C	13
dsl gbond group <name>	Creates a DSL bonding group with the specified name and enters the sub-command mode for configuring it.	C	13
portlist <portlist>	Sets the bonding group port list, for example: 2/1,2/2. The two ports in a bonding group must be sequential. Members of a bonding group must also be in the same DSL physical layer. This means that on the VLC ports 12 and 13 cannot be in a group together.	C	13
protocol <0 1 2>	Configures the protocol the bonding group uses, 0:atm 1:ptm 2:auto.	C	13
active	Turns on port bonding for this group.	C	13
linetemplate <line-template>	Specifies the DSL line template the group uses.	C	13
fallbacktemplate <fallback-template>	Select the DSL line template the group uses for fallback.	C	13
no active	Turns off port bonding for this group.	C	13
no dsl gbond group <name>	Deletes the specified bonding group.	C	13
show dsl gbond	Displays the bonding group list.	E	13
show dsl gbond status	Displays the status of all of the bonding groups.	E	13
show dsl gbond status <name>	Displays the status of the specified bonding group.	E	13
show dsl gbond config	Displays the configuration of all the bonding groups.	E	13
show dsl gbond config <name>	Displays the configuration of the specified bonding group.	E	13
show dsl gbond counters <name>	Displays the bonding group counters.	E	13
show interface dsl <slot/portlist> config	Displays the DSL configuration of the specified DSL ports.	E	13
show interface dsl <slot/portlist> lineinfo	Displays the current 15 minutes DSL line information for the specified DSL ports.	E	13

Table 262 VDSL Commands Summary (continued)

COMMAND	DESCRIPTION	M	P
<code>show interface dsl <slot/ portlist> linerate</code>	Displays the current 15 minutes DSL line rate for the specified DSL ports.	E	13
<code>show interface dsl <slot/ portlist> status</code>	Displays the current 15 minutes DSL line status for the specified DSL ports.	E	13
<code>clear interface dsl <slot/ portlist> performance</code>	Clears the current or historical 15-minutes and 1-day DSL line status for the specified DSL ports.	E	13
<code>show interface dsl <slot/ portlist> performance current 15- min 1-day</code>	Displays the current or historical 15-minutes and 1-day DSL line status for the specified DSL ports.	E	13
<code>show interface dsl <slot/ portlist> line</code>	Displays the detailed DSL line information for the specified DSL ports.	E	13
<code>show interface dsl <slot/ portlist> channel</code>	Displays the detailed DSL channel information for the specified DSL ports.	E	13
<code>show interface dsl <slot/ portlist> band</code>	Displays the DSL band information for the specified DSL ports.	E	13
<code>show interface dsl <slot/ portlist> medleypsd</code>	Displays the DSL medley psd information for the specified DSL ports.	E	13
<code>show interface dsl <slot/ portlist> qln</code>	Displays the DSL Quiet Line Noise (QNL) level information for the specified DSL ports.	E	13
<code>show interface dsl <slot/ portlist> snr</code>	Displays the DSL SNR information for the specified DSL ports.	E	13
<code>show interface dsl <slot/ portlist> hlog</code>	Displays the DSL HLOG information for the specified DSL ports. These channel characteristics can be used in analyzing the physical condition of the ADSL or VDSL line. The format provides magnitude values in a logarithmic scale.	E	13
<code>show interface dsl <slot/ portlist> bitalloc</code>	Displays the number of bits transmitted for each DMT tone for the specified DSL ports. The better (or shorter) the line, the higher the number of bits transmitted for a DMT tone. The maximum is 15.	E	13
<code>dsl diagnostic delt <slot/ portlist></code>	Performs the DSL Dual End Loop Test (DELT) test on the specified DSL ports. ADSL ports must use ADSL, ADSL2, or ADSL2+ operational mode and have a connection. VDSL port must use VDSL2, ADSL2 or ADSL2+ operational mode and have a connection. The subscriber device must also support DELT. It takes about one minute for the loop diagnostics to finish.	E	13
<code>show interface dsl <slot/ portlist> diagnostic delt result hlin hlog qln snr</code>	Displays the DSL DELT test results for the specified DSL ports. Use the loop diagnostics results to analyze problems with the physical ADSL or VDSL line.	E	13
<code>dsl diagnostic selt <slot/ portlist></code>	Performs the Single End Loop Test (SELT) on the specified DSL ports to check the distance to the subscriber. Note: The port must have an open loop. There cannot be a DSL device, phone, fax machine, or other device connected to the subscriber's end of the telephone line.	E	13
<code>show interface dsl <slot/ portlist> diagnostic selt</code>	Displays the SELT results (such as line type and loop length) for the specified DSL ports.	E	13
<code>dsl diagnostic oamf5 <slot/port> <vpi/vci></code>	Performs an OAM F5 loopback test on the specified ATM PVC of the specified DSL port.	C	13

Table 262 VDSL Commands Summary (continued)

COMMAND	DESCRIPTION	M	P
<code>show interface dsl <slot/ portlist> diagnostic oamf5</code>	Displays the OAM F5 loopback test results for the specified DSL port.	E	13
<code>clear interface dsl <slot/ portlist> statistics</code>	Clears the packet statistics for the specified DSL ports.	E	13
<code>show interface dsl <slot/ portlist> statistics</code>	Displays the packet statistics for the specified DSL ports.	E	13

CHAPTER 36

FE

Use these commands to configure the Fast Ethernet subscriber ports.

Table 263 fe Commands Summary

COMMAND	DESCRIPTION	M	P
<code>interface fe <portlist></code>	Configures the specified FE UNI ports. You can specify a single port <1>, all ports <*> or a list of ports <1,2>. You can also include a range of ports <1-2>.	C	13
<code>exit</code>	Leaves the FE UNI port configuration.	C	13
<code>active</code>	Enables the FE UNI ports.	C	13
<code>no active</code>	Disables the FE UNI ports.	C	13
<code>speed <rate> <duplex></code>	Configures the FE UNI port's speed and duplex mode. <i>rate</i> : 100 or 10 (MB/s) <i>duplex</i> : full or half	C	13
<code>no speed</code>	Restores the FE UNI port's speed and duplex mode to auto-negotiation	C	13
<code>flow-control active</code>	Turns on flow control functions on the FE UNI ports.	C	13
<code>no flow-control</code>	Turns off flow control functions on the FE UNI ports.	C	13
<code>name <port-name-string></code>	Sets a name of up to 31 printable characters for the FE UNI ports.	C	13
<code>no name</code>	Resets the name of the ports to the default.	C	13
<code>show interface fe <slot/portlist> config</code>	Displays the FE configuration for the specified UNI ports. You can specify a single port <1>, all ports <*> or a list of ports <1,2>. You can also include a range of ports <1-2>.	E	13
<code>show interface fe <slot/portlist> status</code>	Displays the current FE line status for the specified UNI ports. You can specify a single port <1>, all ports <*> or a list of ports <1,2>. You can also include a range of ports <1-2>.	E	13
<code>clear interface fe <slot/ portlist> statistics</code>	Clears packet statistics for the specified FE UNI ports. You can specify a single port <1>, all ports <*> or a list of ports <1,2>. You can also include a range of ports <1-2>.	E	13
<code>show interface fe <slot/portlist> statistics</code>	Displays packet statistics for the specified FE UNI ports. You can specify a single port <1>, all ports <*> or a list of ports <1,2>. You can also include a range of ports <1-2>.	E	13

CHAPTER 37

VLAN

Use these commands to configure general VLAN settings, transparent VLAN, VLAN TLS, VLAN translation and aggregation, and VLAN trunking.

37.1 VLAN Overview

These sections introduce VLAN and the VLAN modes on the IES. See the later sections in this chapter for details on the VLAN commands.

Static VLANs are created manually. Use a static VLAN to decide whether an incoming frame on a port should be

- sent to a VLAN group as normal depending on its VLAN tag.
- sent to a group whether it has a VLAN tag or not.
- blocked from a VLAN group regardless of its VLAN tag.

You can also tag all (previously untagged) frames going out through a port with a specified VLAN ID.

Packets on the NNI (Network Node Interface) side (uplink ports) can be any of the following:

- untagged
- tagged with a service provider VLAN ID (SVID)
- tagged with a SVID and a customer VID (CVID)

Packets on the UNI (User Network Interface) side (DSL ports) can be any of the following:

- untagged
- tagged with a CVID

Other important VLAN information:

- For PTM mode, a DSL port is a logical Ethernet port.
- For ATM mode, an ATM PVC is a logical Ethernet port.
- VLAN modes can be applied to any logical port (PTM or ATM).
- A logical port can join more than one VLAN mode, but the UNI VLAN used in each joined VLAN mode must be unique.
- The uplink port joins the NNI VLAN specified in VLAN modes, multicast VLAN, the management VLAN, and the VoIP VLAN.
- The IES drops double-tagged packets received on a UNI port regardless of the VLAN mode.

37.1.1 Transparent VLAN Mode

- Transparent VLAN does not change the type of the VLAN tag in uplink and DSL ports.
- In the uplink port, the VLAN Tag Protocol Identifier (TPID) is a Service provider Tag Protocol Identifier (S TPID). You can configure the S-tag TPID to be the same as the Customer TPID (C TPID) (0x8100), and the users will think it is fully transparent.
- Transparent VLAN can co-exist with other VLAN modes. The only limitation is VLAN transparent cannot co-work with VLAN TLS in the same logical port.

Note: Use the `interface ge-nni <portlist>` and `vlan all` commands to add Gigabit Ethernet uplink ports to all VLANs (1 ~ 4093) to make sure VLAN transparent traffic can go through the uplink.

Table 264 Transparent VLAN CLI Examples

VLAN MODE	NNI VLAN	UNI VLAN	CLI EXAMPLES
Transparent (PTM)	untag S(VID a)	untag C(VID a)	<code>interface dsl 2/1</code> <code>vlan transparent</code>
Transparent (ATM)	untag S(VID a)	untag C(VID a)	<code>interface dsl 2/1</code> <code>vlan transparent atm-vc 0/33</code>

37.1.2 VLAN Tagging and Trunk Mode

- An S tag with PVID is added in the NNI side for untagged packets from the UNI side.
- The VLAN ID for single-tagged packets is not changed on either side, but the Tag Protocol Identifier (TPID) is different. The Service provider Tag Protocol Identifier (S TPID) is on the NNI side and a Customer TPID (C TPID) is on the UNI side.
- The IES only forwards traffic for VLANs configured on the UNI side. If you configure the UNI side as untagged only, the IES only forwards untagged packets.
- VLAN tagging and trunk can co-exist with other VLAN modes.

Table 265 VLAN Tagging and Trunk CLI Examples

VLAN MODE	NNI VLAN	UNI VLAN	CLI EXAMPLES
VLAN Tagging and Trunk (PTM-untagged)	S(PVID)	untag	<code>interface dsl 2/1</code> <code>vlan trunk uni-untag svlan 100 spbit 0</code>
VLAN Tagging and Trunk (ATM-untagged)	S(PVID)	untag	<code>interface dsl 2/1</code> <code>vlan trunk atm-vc 0/33 uni-untag svlan 100 spbit 0</code>
VLAN Tagging and Trunk (PTM-tagged)	S(VID a)	C(VID a)	<code>interface dsl 2/1</code> <code>vlan trunk uni-vlan 100</code>
VLAN Tagging and Trunk (ATM-tagged)	S(VID a)	C(VID a)	<code>interface dsl 2/1</code> <code>vlan trunk atm-vc 0/33 uni-vlan 100</code>

37.1.3 Stacking VLAN Tagging and Trunk Mode

- Compared to VLAN tagging and trunk mode this mode adds an outer tag.
- An S tag with SVID and a C tag with PVID are added on the NNI side for untagged packets from the UNI side.

- The C tag for UNI side, single-tagged case is not changed in both sides, and a S tag with SVID is added.
- The IES only forwards traffic for VLANs configured on the UNI side.
- VLAN stacking tagging and trunk can co-exist with other VLAN modes.

Table 266 Stacking VLAN Tagging and Trunk CLI Examples

VLAN MODE	NNI VLAN	UNI VLAN	CLI EXAMPLES
Stacking VLAN Tagging and Trunk (PTM-untagged)	S(SVID) + C(PVID)	untag	interface dsl 2/1 vlan trunk uni-untag svlan 200 spbit 0 cvlan 100 cpbit 0
Stacking VLAN Tagging and Trunk (ATM-untagged)	S(SVID) + C(PVID)	untag	interface dsl 2/1 vlan trunk atm-vc 0/33 uni-untag svlan 200 spbit 0 cvlan 100 cpbit 0
Stacking VLAN Tagging and Trunk (PTM-tagged)	S(SVID) + C(VID a)	C(VID a)	interface dsl 2/1 vlan trunk uni-vlan 100 svlan 200
Stacking VLAN Tagging and Trunk (ATM-tagged)	S(SVID) + C(VID a)	C(VID a)	interface dsl 2/1 vlan trunk atm-vc 0/33 uni-vlan 100 svlan 200

37.1.4 VLAN Translation and Aggregation Mode

VLAN translation changes the VLAN tag on traffic received from a DSL port to another VLAN ID for the service provider's network. This makes it easier to deploy customer-specific VLANs because all the CPE devices can use the same VLAN configuration. You only need to configure VLAN translation on the IES to use unique VLAN IDs for each CPE device's traffic.

- This mode performs VLAN translation between the NNI and UNI sides.
- The NNI side is tagged with an S tag and UNI side is tagged with a C tag.
- Two or more different UNI VLAN IDs translated to a NNI VLAN ID is VLAN aggregation.
- 1:1 VLAN translation mapping is VLAN translation.
- Only VLANs joined on the UNI side will be forwarded.
- VLAN translation and aggregation can co-exist with other VLAN modes.

Table 267 VLAN Translation and Aggregation CLI Examples

VLAN MODE	NNI VLAN	UNI VLAN	CLI EXAMPLES
VLAN Translation (PTM)	S(VID x)	C(VID a)	interface dsl 2/1 vlan translation uni-vlan 100 svlan 1100
VLAN Translation (ATM)	S(VID x)	C(VID a)	interface dsl 2/1 vlan translation atm-vc 0/33 uni-vlan 100 svlan 1100
VLAN Aggregation (PTM)	S(VID y) S(VID y)	C(VID b) C(VID c)	interface dsl 2/1 vlan translation uni-vlan 101 svlan 1100 vlan translation uni-vlan 102 svlan 1100
VLAN Aggregation (ATM)	S(VID y) S(VID y)	C(VID b) C(VID c)	interface dsl 2/1 vlan translation atm-vc 0/33 uni-vlan 101 svlan 1100 vlan translation atm-vc 0/33 uni-vlan 102 svlan 1100

37.1.5 Stacking VLAN Translation and Aggregation Mode

- Compared to VLAN translation and aggregation mode, this mode adds an outer tag.
- This mode performs VLAN translation between the NNI and UNI sides.
- The NNI side is tagged with double tags, S(SVID) + C(CVID), and the UNI side is tagged with a C tag.
- Two or more different UNI VLAN IDs translated to a NNI VLAN ID is VLAN aggregation.
- 1:1 VLAN translation mapping is VLAN translation.
- The IES only forwards traffic for VLANs configured on the UNI side.
- Stacking VLAN translation and aggregation can co-exist with other VLAN modes.

Table 268 Stacking VLAN Translation and Aggregation CLI Examples

VLAN MODE	NNI VLAN	UNI VLAN	CLI EXAMPLES
Stacking VLAN Translation (PTM)	S(SVID) + C(VID x)	C(VID a)	interface dsl 2/1 vlan translation uni-vlan 100 svlan 2100 cvlan 1100
Stacking VLAN Translation (ATM)	S(SVID) + C(VID x)	C(VID a)	interface dsl 2/1 vlan translation atm-vc 0/33 uni-vlan 100 svlan 2100 cvlan 1100
Stacking VLAN Aggregation (PTM)	S(SVID) + C(VID y) S(SVID) + C(VID y)	C(VID b) C(VID c)	interface dsl 2/1 vlan translation uni-vlan 101 svlan 2100 cvlan 1100 vlan translation uni-vlan 102 svlan 2100 cvlan 1100
Stacking VLAN Aggregation (ATM)	S(SVID) + C(VID y) S(SVID) + C(VID y)	C(VID b) C(VID c)	interface dsl 2/1 vlan translation atm-vc 0/33 uni-vlan 101 svlan 2100 cvlan 1100 vlan translation atm-vc 0/33 uni-vlan 102 svlan 2100 cvlan 1100

37.1.6 VLAN TLS Mode

- VLAN Transparent LAN Service (TLS) adds an outer tag regardless of whether the UNI side is untagged or single tagged.
- VLAN TLS packets are not handled by any control protocol (DHCP, IGMP, ...), so the UNI traffic is tunneled into the TLS VLAN.
- VLAN TLS mode forwards all traffic of VLANs not configured as part of other modes.
- VLAN TLS can co-exist with other VLAN modes in the IES, however you cannot use the same individual VLAN for TLS and other VLAN models concurrently. VLAN TLS also cannot co-work with VLAN transparent on the same logical port.

Table 269 VLAN TLS CLI examples

VLAN MODE	NNI VLAN	UNI VLAN	CLI EXAMPLES
VLAN TLS (PTM)	S(TLSVID) S(TLSVID) + C(VID a)	untag C(VID a)	interface dsl 2/1 vlan tls svlan 1000 spbit 3
VLAN TLS (ATM)	S(TLSVID) S(TLSVID) + C(VID a)	untag C(VID a)	interface dsl 2/1 vlan tls atm-vc 0/33 svlan 1000 spbit 3

37.1.7 Multicast VLAN

IGMP (Internet Group Management Protocol) is a network-layer protocol used to establish membership in a multicast group - it is not used to carry user data. Multicast VLAN is designed for applications (such as Media-on-Demand (MoD)) using multicast traffic across an Ethernet ring-based service provider network. Multicast VLAN allows one single multicast VLAN to be shared among different subscriber VLANs on the network. This improves bandwidth utilization by reducing multicast traffic in the subscriber VLANs and simplifies multicast group management.

- Multicast VLAN (MVLAN) applies only to downstream multicast stream and IGMP or Multicast Listener Discovery (MLD) packets. The IES forwards upstream IGMP packets according to the unicast VLAN modes the UNI port has joined.
- MVLAN must co-work with one of the 4 VLAN modes - VLAN tagging and trunk, stacking VLAN tagging and trunk, VLAN translation and aggregation, or stacking VLAN translation and aggregation.
- A UNI port must join one of the 4 VLAN modes before it can join a MVLAN. The UNI VLAN in the joined VLAN modes and MVLAN must be the same.
- Add the ATM VC to MVLAN (see [Section 25.1 on page 365](#)).

Table 270 Multicast VLAN CLI examples

VLAN MODE	NNI VLAN	UNI VLAN	CLI EXAMPLES
Multicast VLAN (PTM-untagged)	S(VID a)	untag	<pre>interface dsl 2/1 vlan trunk uni-untag svlan 100 spbit 0 igmp-mld mvlan 200 untag</pre>
Multicast VLAN (ATM-untagged)	S(VID a)	untag	<pre>interface dsl 2/1 vlan trunk atm-vc 0/33 uni-untag svlan 100 spbit 0 igmp-mld mvlan 200 untag atm-vc 0/33 vc priority 0 mvlan</pre>
Multicast VLAN (PTM-tagged)	S(VID a)	C(VID a)	<pre>interface dsl 2/1 vlan trunk uni-vlan 200 igmp-mld mvlan 200</pre>
Multicast VLAN (ATM-tagged)	S(VID a)	C(VID a)	<pre>interface dsl 2/1 vlan trunk atm-vc 0/33 uni-vlan 200 igmp-mld mvlan 200</pre>
Multicast VLAN (PTM-tagged)	S(VID x)	C(VID a)	<pre>interface dsl 2/1 vlan trunk uni-vlan 100 igmp-mld mvlan 200 uni-vlan 100</pre>
Multicast VLAN (ATM-tagged)	S(VID x)	C(VID a)	<pre>interface dsl 2/1 vlan trunk atm-vc 0/33 uni-vlan 100 igmp-mld mvlan 200 uni-vlan 100 atm-vc 0/33 vc priority 0 mvlan</pre>

37.1.8 Management and VoIP VLAN

- The management VLAN and VoIP VLAN both accept only single tagged packets on both the NNI and CPU ports.
- UNI ports can communicate with the CPU port if the UNI port joins the management VLAN.

Table 271 Management and VoIP VLAN CLI examples

VLAN MODE	NNI VLAN	UNI VLAN	CLI EXAMPLES
Management VLAN	S(VID a)	S(VID a)	ip inband mgmt-vlan 100
VoIP VLAN	S(VID a)	S(VID a)	voip ip address 192.168.2.20/24 vlan 100

37.2 General VLAN Commands

Use these commands to configure global VLAN settings or show VLAN member ports for all VLAN modes. The following table describes the commands.

Table 272 VLAN Commands Summary

COMMAND	DESCRIPTION	M	P
vlan stpid <tpid>	Configures the S (subscriber) tag TPID in hexadecimal format. <i>tpid</i> : 0x8000-0xffff	C	13
no vlan stpid	Resets the S tag TPID to the default value of 0x8100 in hexadecimal format.	C	13
vlan single-tag-mode stag ctag	stag: single-tag packets sent from NNI tagged with S tag ctag: single-tag packets sent from NNI tagged with C tag (0x8100)	C	13
show vlan [vid-list]	Displays S tag TPID, single-tag mode and the member ports of specified VLANs or all VLANs. <i>vid-list</i> : list of (1-4093), for example 1,3 or 1,3,5-21 or *	E	13
show interface dsl <slot/ portlist> vlan	Displays all the VLANs joined by the specified DSL ports.	E	13
show interface fe <slot/ portlist> vlan	Displays all the VLANs joined by the specified FE ports.	E	13
show interface ge-nni <slot/ portlist> vlan	Displays all the VLANs joined by the specified Gigabit Ethernet uplink ports.	E	13
interface ge-nni <portlist>	Configures the specified Gigabit Ethernet uplink ports. You can specify a single port <1>, all ports <*> or a list of ports <1,2>. You can also include a range of ports <1-2>.	C	13
exit	Leaves the Gigabit Ethernet Gigabit Ethernet uplink port configuration.	C	13
vlan <vid>	Adds the Gigabit Ethernet uplink ports to the specified VLAN.	C	13
vlan-untag <vid> pbit <pbit>	Joins specified NNI ports to a VLAN. The frame is transmitted/received as untagged. If an NNI port has joined all VLANs by the "vlan all" command, this command takes higher priority. <i>vid</i> : 1-4093 <i>pbit</i> : 0-7	C	13
no vlan <vid>	Removes the Gigabit Ethernet uplink ports from the specified VLAN.	C	13
vlan all	Adds the specified Gigabit Ethernet uplink ports to all VLANs (1 ~ 4093). Note: When using transparent VLAN, use this vlan all command to make sure VLAN transparent traffic can go through the uplink.	C	13
no vlan all	Removes the Gigabit Ethernet uplink ports from all VLANs joined by using the vlan all command.	C	13

37.2.1 Command Examples

See [Section 20.1.3 on page 302](#) for an example about how to change STPID.

This example shows the settings on VLAN 100. From the command output, The STPID is 88a8 and packets sent by the IES are with C tag. Port 1 of the line card in slot 2 and Gigabit Ethernet ports 1 and 2 are the members.

```

ras# show vlan 100
S tag TPID: 8100 (hex)
single tag mode: ctag

VLAN ID  0000000001111111112222222223333333334444444455555555566666
100      123456789012345678901234567890123456789012345678901234
=====
slot    2:V-----
slot    3:-----
slot    4:-----
slot    5:-----
enet    :VV
ras#

```

This example adds Gigabit Ethernet port 2's VLAN ID to 100 only. By default, the IES adds all Gigabit Ethernet ports to all VLANs. You have to remove port 2 from all VLANs before adding it to VLAN 100.

```

ras# show interface ge-nni * vlan
Port    vlan
enet1   all
enet2   all
ras# config
ras(config)# interface ge-nni 2
ras(config)# no vlan all
ras(config-interface-ge-nni-2)# vlan 100
ras(config-interface-ge-nni-2)# exit
ras(config)# exit
ras# show interface ge-nni * vlan
Port    vlan
enet1   all
enet2   100
ras#

```

37.3 Transparent VLAN Commands

Transparent VLAN does not change the type of the VLAN tag in uplink and user (DSL) ports. You can configure the S-tag TPID on the uplink port to be the same as the C-tag TPID on the DSL port (0x8100) so the behavior appears truly transparent.

See [Section 37.1.1 on page 421](#) for more on transparent VLAN and command examples.

Note: Use the `interface ge-nni <portlist>` and `vlan all` commands to add Gigabit Ethernet uplink ports to all VLANs (1 ~ 4093) to make sure VLAN transparent traffic can go through the uplink.

The following table describes commonly used parameter notation for these commands.

Table 273 Transparent VLAN Command Parameters

NOTATION	DESCRIPTION
<i>vpi</i>	The VPI (Virtual Path Indicator) 0-255.
<i>vci</i>	The VCI (Virtual Channel Indicator) 32-65535.

This table describes the commands.

Table 274 Transparent VLAN Commands Summary

COMMAND	DESCRIPTION	M	P
<code>interface dsl <slot/portlist></code>	Enters the sub-command mode for configuring the specified DSL ports.	C	13
<code>exit</code>	Leaves the DSL port configuration.	C	13
<code>vlan transparent</code>	Enables transparent VLAN on the specified DSL ports. In PTM mode, a DSL port is a logical Ethernet port.	C	13
<code>no vlan transparent</code>	Disables transparent VLAN on the specified DSL ports.	C	13
<code>vlan transparent atm-vc <vpi>/<vci></code>	Enables transparent VLAN on the specified DSL ATM virtual circuit. In ATM mode, an ATM PVC is a logical Ethernet port.	C	13
<code>no vlan transparent atm-vc <vpi>/<vci></code>	Disables transparent VLAN on the specified DSL ATM virtual circuit.	C	13
<code>interface fe <slot/portlist></code>	Enters the sub-command mode for configuring the specified FE ports.	C	13
<code>exit</code>	Leaves the FE port configuration.	C	13
<code>vlan transparent</code>	Enables transparent VLAN on the specified FE ports.	C	13
<code>no vlan transparent</code>	Disables transparent VLAN on the specified FE ports.	C	13

37.3.1 Command Examples

This example enables port 4 of the line card in slot 2 and also enables VLAN transparent and loop guard on it.

```

ras# config
ras(config)# interface dsl 2/4
ras(config-interface-dsl-2/4)# active
ras(config-interface-dsl-2/4)# vlan transparent
ras(config-interface-dsl-2/4)# loopguard
ras(config-interface-dsl-2/4)# exit
ras(config)# exit
ras#

```

37.4 VLAN TLS Commands

Use these commands to configure Transparent LAN Service (TLS) on the IES. Transparent LAN Service (also known as VLAN stacking or Q-in-Q) allows a service provider to distinguish multiple customers VLANs, even those with the same (customer-assigned) VLAN ID, within its network.

Use TLS to add an outer VLAN tag to the inner IEEE 802.1Q tagged frames that enter the network. By tagging the tagged frames ("double-tagged" frames), the service provider can manage up to 4,093

VLAN groups with each group containing up to 4,093 customer VLANs. This allows a service provider to provide different services, based on specific VLANs, for many different customers.

A service provider's customers may require a range of VLANs to handle multiple applications. A service provider's customers can assign their own inner VLAN tags to traffic. The service provider can assign an outer VLAN tag for each customer. Therefore, there is no VLAN tag overlap among customers, so traffic from different customers is kept separate.

Before the IES sends the frames from the customers, the VLAN ID is added to the frames. When packets intended for specific customers are received on the IES, the outer VLAN tag is removed before the traffic is sent.

See [Section 37.1.6 on page 423](#) for more on VLAN TLS and command examples.

The following table describes commonly used parameter notation for these commands.

Table 275 VLAN TLS Command Parameters

NOTATION	DESCRIPTION
<code>svid</code>	The SVID (Subscriber VLAN ID) 1-4093.
<code>vpi</code>	The VPI (Virtual Path Indicator) 0-255.
<code>vci</code>	The VCI (Virtual Channel Indicator) 32-65535.

This table describes the commands.

Table 276 VLAN TLS Commands Summary

COMMAND	DESCRIPTION	M	P
<code>interface dsl <slot/portlist></code>	Configures the specified DSL ports.	C	13
<code>exit</code>	Leaves the DSL port configuration.	C	13
<code>vlan tls svlan <svid> spbit <spbit> [force- spbit]</code>	Enables Transparent LAN service on the specified DSL ports. In PTM mode, a DSL port is a logical Ethernet port. The IES adds the S tag (SVID) to packets from the DSL ports before forwarding them through an uplink interface. <i>spbit</i> : 0-7, if a priority bit is not assigned, the S priority bit is copied from the customer priority bit. <i>force-spbit</i> : if not specified, only untagged frames will adopt the S priority bit in upstream traffic. If specified, untagged, priority tagged, and C tagged frames will adopt the S priority bit in upstream traffic.	C	13
<code>no vlan tls</code>	Disables Transparent LAN service on the specified DSL ports.	C	13
<code>vlan tls atm-vc <vpi>/ <vci> svlan <svid> spbit <spbit> [force-spbit]</code>	Enables Transparent LAN service on the specified DSL ATM virtual circuit. In ATM mode, an ATM PVC is a logical Ethernet port. The IES adds the S tag (SVID) to packets from the DSL ATM virtual circuits before forwarding them through an uplink interface. <i>spbit</i> : 0-7, if a priority bit is not assigned, the S priority bit is copied from the customer priority bit. <i>force-spbit</i> : if not specified, only untagged frames will adopt the S priority bit in upstream traffic. If specified, untagged, priority tagged, and C tagged frames will adopt the S priority bit in upstream traffic.	C	13
<code>no vlan tls atm-vc <vpi>/ <vci></code>	Disables Transparent LAN service on the specified DSL ATM virtual circuit.	C	13
<code>interface fe <slot/portlist></code>	Configures the specified FE ports.	C	13
<code>exit</code>	Leaves the FE port configuration.	C	13

Table 276 VLAN TLS Commands Summary (continued)

COMMAND	DESCRIPTION	M	P
<code>vlan tls svlan <svid> spbit <spbit> [force- spbit]</code>	Enables Transparent LAN service on the specified FE ports. The IES adds the S tag (SVID) to packets from the FE ports before forwarding them through an uplink interface. <i>spbit</i> : 0-7, if a priority bit is not assigned, the S priority bit is copied from the customer priority bit. <i>force-spbit</i> : if not specified, only untagged frames will adopt the S priority bit in upstream traffic. If specified, untagged, priority tagged, and C tagged frames will adopt the S priority bit in upstream traffic.	C	13
<code>no vlan tls</code>	Disables Transparent LAN service on the specified FE ports.	C	13

37.4.1 Command Examples

This example enables port 4 of the line card in slot 2 and also enables VLAN TLS with S tag VLAN 100 with S priority bit 0.

```

ras# config
ras(config)# interface dsl 2/4
ras(config-interface-dsl-2/4)# active
ras(config-interface-dsl-2/4)# vlan tls svlan 100 spbit 0
ras(config-interface-dsl-2/4)# exit
ras(config)# exit
ras# show vlan 100
S tag TPID: 8100 (hex)
single tag mode: ctag

VLAN ID  0000000001111111112222222222333333333344444444445555555555666666
100      1234567890123456789012345678901234567890123456789012345678901234
=====
slot    2:---V-----
slot    3:-----
slot    4:-----
slot    5:-----
enet     :--
ras#

```

37.5 VLAN Translation and Aggregation Commands

VLAN translation changes the VLAN tag on traffic received from a subscriber port to another VLAN ID for the service provider's network. This makes it easier to deploy customer-specific VLANs because all the CPE devices can use the same VLAN configuration. You only need to configure VLAN translation on the IES to use unique VLAN IDs for each subscriber's traffic. VLAN aggregation lets the IES translate two or more different UNI VLAN IDs on a DSL port to a NNI VLAN ID.

See [Section 37.1.4 on page 422](#) for more on VLAN translation and aggregation and command examples.

The following table describes commonly used parameter notation for these commands.

Table 277 VLAN Translation and Aggregation Command Parameters

NOTATION	DESCRIPTION
svid	The SVID (Service provider VLAN ID) 1-4093.
cvid	The CVID (Customer VLAN ID) 1-4093.
vpi	The VPI (Virtual Path Indicator) 0-255.
vci	The VCI (Virtual Channel Indicator) 32-65535.

This table describes the commands.

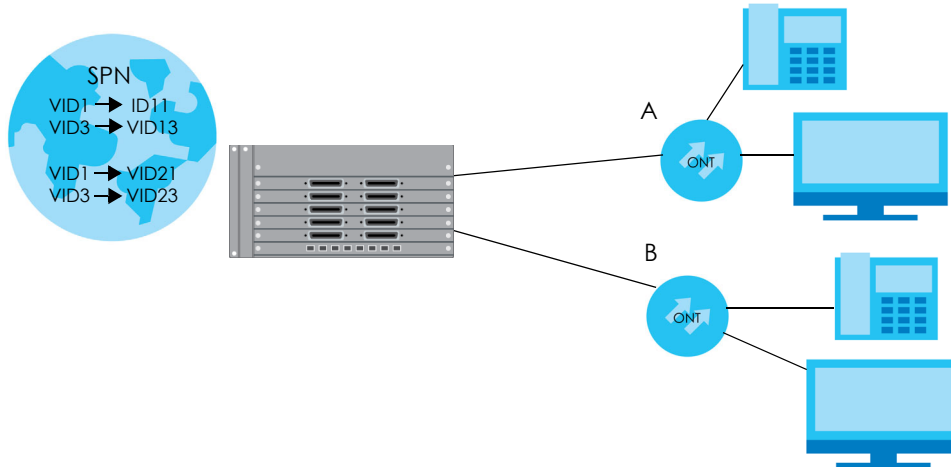
Table 278 VLAN Translation and Aggregation Commands Summary

COMMAND	DESCRIPTION	M	P
interface dsl <slot/portlist>	Enters the sub-command mode for configuring the specified DSL ports.	C	13
exit	Leaves the DSL port configuration.	C	13
vlan translation uni-vlan <uni-vid> svlan <svid> [cvlan <cvid>]	Cross-connects uni-vid tagged packets from the specified DSL ports to the S(svid) VLAN or S(svid) + C(cvid) on uplink ports. In PTM mode, a DSL port is a logical Ethernet port.	C	13
no vlan translation uni-vlan <uni-vid>	Removes the cross-connection of the uni-vid tagged packets from the specified DSL ports.	C	13
vlan translation atm-vc <vpi>/<vci> uni-vlan <uni-vid> svlan <svid> [cvlan <cvid>]	Cross-connects uni-vid tagged packets from the specified DSL ATM virtual circuit to the S(svid) VLAN or S(svid) + C(cvid) on uplink ports. In ATM mode, an ATM PVC is a logical Ethernet port.	C	13
no vlan translation atm-vc <vpi>/<vci> uni-vlan <uni-vid>	Removes the cross-connection of the uni-vid tagged packets from the specified DSL ATM virtual circuit.	C	13
interface fe <slot/portlist>	Enters the sub-command mode for configuring the specified FE ports.	C	13
exit	Leaves the FE port configuration.	C	13
vlan translation uni-vlan <uni-vid> svlan <svid> [cvlan <cvid>]	Cross-connects uni-vid tagged packets from the specified FE ports to the S(svid) VLAN or S(svid) + C(cvid) on uplink ports.	C	13
no vlan translation uni-vlan <uni-vid>	Removes the cross-connection of the uni-vid tagged packets from the specified FE ports.	C	13

37.5.1 Command Examples

In the following figure CPE devices A and B both add VLAN tag 1 to voice traffic and tag 3 to data traffic. xVLAN separates these VLANs within the Service Provider's Network (SPN) by translating A's VLAN tags to 11 and 13 and B's VLAN tags to 21 and 23.

The advantage is that both CPE devices have the same VLAN configuration, therefore reducing CPE device configuration complexity.

Figure 250 VLAN Translation Example

This example shows how to enable ports 5 and 6 of the line card in slot 2 and configures the VLAN translation settings on them.

```

ras# config
ras(config)# interface dsl 2/5
ras(config-interface-dsl-2/5)# active
ras(config-interface-dsl-2/5)# vlan translation uni-vlan 11 svlan 1
ras(config-interface-dsl-2/5)# vlan translation uni-vlan 13 svlan 3
ras(config-interface-dsl-2/5)# exit
ras(config)# interface dsl 2/6
ras(config-interface-dsl-2/6)# active
ras(config-interface-dsl-2/6)# vlan translation uni-vlan 21 svlan 1
ras(config-interface-dsl-2/6)# vlan translation uni-vlan 23 svlan 3
ras(config-interface-dsl-2/6)# exit
ras(config)#
ras#

```

37.6 VLAN Trunk Commands

VLAN Trunk configures "VLAN Tagging and Trunk mode", and "Stacking VLAN Tagging and Trunk mode" as described in [Section 37.1.2 on page 421](#) and [Section 37.1.3 on page 421](#).

The following table describes commonly used parameter notation for these commands.

Table 279 VLAN Trunking Command Parameters

NOTATION	DESCRIPTION
<i>svid</i>	The SVID (Service provider VLAN ID) 1-4093.
<i>cvid</i>	The CVID (Customer VLAN ID) 1-4093.
<i>spbit</i>	The service provider priority bit 0-7.
<i>cpbit</i>	The customer priority bit 0-7.
<i>etype</i>	The Ethernet type, 0000-ffff in hexadecimal.
<i>uni-vid</i>	The VLAN ID on the UNI (DSL) ports, 1-4093.

Table 279 VLAN Trunking Command Parameters (continued)

NOTATION	DESCRIPTION
<i>vpi</i>	The VPI (Virtual Path Indicator) 0-255.
<i>vci</i>	The VCI (Virtual Channel Indicator) 32-65535.

This table describes the commands.

Table 280 VLAN Trunking Commands Summary

COMMAND	DESCRIPTION	M	P
<code>interface dsl <slot/portlist></code>	Configures the specified DSL ports.	C	13
<code>exit</code>	Leaves the DSL port configuration.	C	13
<code>vlan trunk uni-untag svlan <svid> spbit <spbit> [cvlan <cvid> cpbit <cpbit>]</code>	Cross-connects untagged packets in the specified ports to the specified S VLAN or S + C VLAN on uplink ports.	C	13
<code>no vlan trunk uni-untag</code>	Removes the cross-connection of untagged packets on the specified DSL ports.	C	13
<code>vlan trunk uni-untag ether-type <etype> svlan <svid> spbit <spbit> [cvlan <cvid> cpbit <cpbit>]</code>	Cross-connects untagged packets in the specified ports to the specified S VLAN or S + C VLAN on uplink ports based on the ether-type field.	C	13
<code>no vlan trunk uni-untag ether-type <etype></code>	Removes the ether-type based cross-connection of untagged packets on the specified DSL ports.	C	13
<code>vlan trunk uni-vlan <uni-vid> [svlan <svid>]</code>	Cross-connects uni-vid tagged packets in the specified DSL ports to the S (uni-vid) VLAN if SVLAN is not specified or S (svid) + C (uni-vid) on uplink ports if svlan is specified.	C	13
<code>no vlan trunk uni-vlan <uni-vid></code>	Removes the cross-connection of the uni-vid tagged packets on the specified DSL ports.	C	13
<code>vlan trunk atm-vc <vpi>/<vci> uni-untag svlan <svid> spbit <spbit> [cvlan <cvid> cpbit <cpbit>]</code>	Cross-connects untagged packets in the specified DSL ATM virtual circuits to the specified S VLAN or S + C VLAN on uplink ports.	C	13
<code>no vlan trunk atm-vc <vpi>/<vci> uni-untag</code>	Removes the cross-connection of untagged packets in the specified DSL ATM virtual circuits.	C	13
<code>vlan trunk atm-vc <vpi>/<vci> uni-untag ether-type <etype> svlan <svid> spbit <spbit> [cvlan <cvid> cpbit <cpbit>]</code>	Cross-connects untagged packets in the specified DSL ATM virtual circuits to the specified S VLAN or S + C VLAN on uplink ports based on the ether-type field.	C	13
<code>no vlan trunk atm-vc <vpi>/<vci> uni-untag ether-type <etype></code>	Removes the ether-type based cross-connection of untagged packets on the specified DSL ATM virtual circuits.	C	13
<code>vlan trunk atm-vc <vpi>/<vci> uni-vlan <uni-vid> [svlan <svid>]</code>	Cross-connects uni-vid tagged packets in the specified DSL ATM virtual circuits to the S (uni-vid) VLAN if svlan is not specified or S (svid) + C (uni-vid) on NNI ports if svlan is specified.	C	13
<code>no vlan trunk atm-vc <vpi>/<vci> uni-vlan <uni-vid></code>	Removes the cross-connection of the uni-vid tagged packets in the specified UNI ATM virtual circuits.	C	13
<code>interface fe <slot/portlist></code>	Configures the specified FE ports.	C	13
<code>exit</code>	Leaves the FE port configuration.	C	13

Table 280 VLAN Trunking Commands Summary (continued)

COMMAND	DESCRIPTION	M	P
<code>vlan trunk uni-untag svlan <svid> spbit <spbit> [cvlan <cvid> cpbit <cpbit>]</code>	Cross-connects untagged packets in the specified FE ports to the specified S VLAN or S + C VLAN on uplink ports.	C	13
<code>no vlan trunk uni-untag</code>	Removes the cross-connection of untagged packets on the specified FE ports.	C	13
<code>vlan trunk uni-untag ether-type <etype> svlan <svid> spbit <spbit> [cvlan <cvid> cpbit <cpbit>]</code>	Cross-connects untagged packets in the specified FE ports to the specified S VLAN or S + C VLAN on uplink ports based on the ether-type field.	C	13
<code>no vlan trunk uni-untag ether-type <etype></code>	Removes the ether-type based cross-connection of untagged packets on the specified FE ports.	C	13
<code>vlan trunk uni-vlan <uni-vid> [svlan <svid>]</code>	Cross-connects uni-vid tagged packets in the specified FE ports to the S (uni-vid) VLAN if SVLAN is not specified or S (svid) + C (uni-vid) on uplink ports if svlan is specified.	C	13
<code>no vlan trunk uni-vlan <uni-vid></code>	Removes the cross-connection of the uni-vid tagged packets on the specified FE ports.	C	13

37.6.1 Command Examples

This example shows how to enable port 7 of the line card in slot 2 and configure the VLAN trunking settings with S VLAN 200 and C VLAN 100 on it. Both the S priority bits of S VLAN and C VLAN are set to 0.

```

ras# config
ras(config)# interface dsl 2/7
ras(config-interface-dsl-2/7)# active
ras(config-interface-dsl-2/7)# vlan trunk uni-untag svlan 200 spbit 0 cvlan 100
cpbit 0
ras(config-interface-dsl-2/7)# exit
ras(config)# exit
ras#

```

CHAPTER 38

VoIP

38.1 VoIP Overview

Use the Voice over IP (VoIP) commands to configure and manage the IES's POTS (Plain Old Telephone System) service.

VoIP (Voice over IP) is the sending of voice signals over the Internet Protocol. This allows you to make phone calls and send faxes over the Internet at a fraction of the cost of using the traditional circuit-switched telephone network. You can also use servers to run telephone service applications like PBX services and voice mail. Internet Telephony Service Provider (ITSP) companies provide VoIP service.

Circuit-switched telephone networks require 64 kilobits per second (kbps) in each direction to handle a telephone call. VoIP can use advanced voice coding techniques with compression to reduce the required bandwidth.

The VOP connects POTS end-user telephone subscribers to the IP network by converting the analog voice signal into data packets and transmitting them over the network.

38.2 H.248 and SIP

The IES uses a VOP line card for VoIP communications.

Note: The firmware version determines whether the IES uses H.248 or SIP for VoIP (see [Section 2.5 on page 36](#) for details).

38.3 H.248

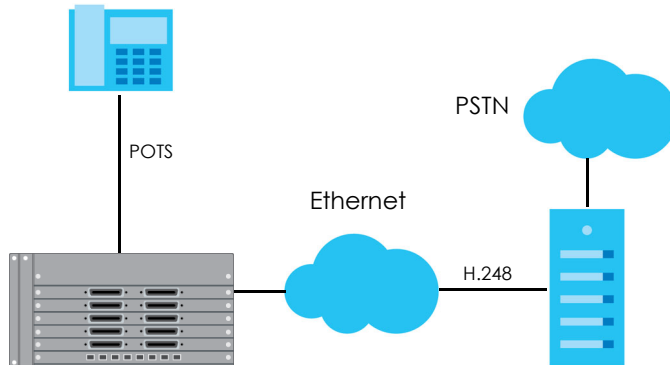
The H.248 protocol, also known as MEGACO (MEdia GAteway COntrol) or the Gateway Control Protocol, defines a VoIP network in which basic functions (such as voice coding and decoding) are performed by one device, and higher functions (such as setting up and managing calls) are performed by another. An H.248 VoIP network consists of one or more media gateways and a media gateway controller.

- Media gateways (MGs) encode and decode voice data, transmitting it from one network to another (for example, from the PSTN to an IP network, and vice versa). The POTS cards are MGs.
- Media gateway controllers (MGCs) are intelligent devices that manage the media gateways. They set up, manage and tear down calls by providing instructions to the MGs.

Voice services are delivered over the IES POTS card telephone port to a standard telephone. An internal analog telephone adapter (ATA) on the VOP converts the voice traffic to POTS from real-time transport protocol (RTP) over IP.

The voice traffic and H.248 signaling from the IES are sent to the active Gigabit Ethernet backbone network. An external MGC or H.248 voice gateway converts the voice traffic to other formats as required.

Figure 251 Delivering H.248 Services Example



38.4 SIP

The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet.

SIP signaling is separate from the media for which it handles sessions. The media that is exchanged during the session can use a different path from that of the signaling. SIP handles telephone calls and can interface with traditional circuit-switched telephone networks.

38.5 VoIP Commands

The following table describes commonly used parameter notation for these commands.

Table 281 VoIP Command Parameters

NOTATION	DESCRIPTION
profile-name	The name of a profile, up to 31 printable characters.
name	The name of a profile, up to 31 printable characters.

This table describes the commands.

Table 282 VoIP Commands Summary

COMMAND	DESCRIPTION	M	P
<code>voip countrycode <country-code></code>	Configures country code for predefined VOIP parameters <i>country-code</i>: 0: USA 23: Germany 1: Japan 24: Greece 2: Taiwan 25: Australia 3: Austria 26: New Zealand 4: Belgium 27: Hong Kong 5: Bulgaria 28: Singapore 6: Czech 29: Morocco 7: Denmark 30: Ireland 8: Finland 31: Malaysia 9: France 32: Russia 10: Hungary 33: Thailand 11: Iceland 34: Israel 12: Italy 35: UAE 13: Luxembourg 36: China 14: Netherlands 37: Ukraine 15: Norway 38: South Africa 16: Poland 39: South Korea 17: Portugal 40: Philippines 18: Slovakia 41: India 19: Spain 42: Turkey 20: Sweden 43: Vietnam 21: Switzerland 44: Brazil 22: UK 45: Iran default: 42 Turkey	C	13
<code>show voip countrycode</code>	Displays country code information.	E	13

Table 282 VoIP Commands Summary (continued)

COMMAND	DESCRIPTION	M	P
voip diagnostic mlt test <slot>/<port> <option> [force]	Performs metallic line test on the specified VoIP ports. <i>option:</i> all vac vdc rload riso cap ren ring metering dialtone digit roh loop rrev all: Perform all tests on the line connected to the specified VoIP line card port. vac: Test the line's AC voltage only. vdc: Test the line's DC voltage only. rload: Test the line's load resistance only riso: Test the line's isolation resistance only. cap: Test the line's capacitance only. ren: Test the line's ringer equivalent number only. ring: Test the line's ring voltage only. metering: Test the line's metering voltage only. dialtone: Test the line's dialtone only. digit: Test if the line circuit accepts dialed digits and switches the call to its destination. roh: Test if the receiver is off hook only. loop: Test loop condition including feeding voltage battery high and low, loop resistance, loop current, and voltage between TIP/ RING. rrev: Test loop condition in battery reversal condition. force: Perform the tests immediately, even if the port is in use.	E	13

Table 282 VoIP Commands Summary (continued)

COMMAND	DESCRIPTION	M	P
<pre>voip diagnostic mlt test tel <tel-number> <option> [force]</pre>	Performs the metallic line test by the specified VoIP telephone number. <i>tel-number</i>: Existing telephone number. <i>option</i>: all vac vdc rload riso cap ren ring metering dialtone digit roh loop rev all: Perform all tests on the line connected to the specified VoIP line card port. vac: Test the line's AC voltage only. vdc: Test the line's DC voltage only. rload: Test the line's load resistance only riso: Test the line's isolation resistance only. cap: Test the line's capacitance only. ren: Test the line's ringer equivalent number only. ring: Test the line's ring voltage only. metering: Test the line's metering voltage only. dialtone: Test the line's dialtone only. digit: Test if the line circuit accepts dialed digits and switches the call to its destination. roh: Test if the receiver is off hook only. loop: Test loop condition including feeding voltage battery high and low, loop resistance, loop current, and voltage between TIP/ RING. rrev: Test loop condition in battery reversal condition. force: Perform the tests immediately, even if the port is in use.	E	13

Table 282 VoIP Commands Summary (continued)

COMMAND	DESCRIPTION	M	P
<pre>voip diagnostic mlt test termination-id <termination-id> <option> [force]</pre>	Performs the metallic line test by the specified VoIP H.248 termination ID. This command applies when using H.248 firmware. <i>termination-id</i>: Existing termination ID. <i>option</i>: all vac vdc rload riso cap ren ring metering dialtone digit roh loop rev all: Perform all tests on the line connected to the specified VoIP line card port. vac: Test the line's AC voltage only. vdc: Test the line's DC voltage only. rload: Test the line's load resistance only riso: Test the line's isolation resistance only. cap: Test the line's capacitance only. ren: Test the line's ringer equivalent number only. ring: Test the line's ring voltage only. metering: Test the line's metering voltage only. dialtone: Test the line's dialtone only. digit: Test if the line circuit accepts dialed digits and switches the call to its destination. roh: Test if the receiver is off hook only. loop: Test loop condition including feeding voltage battery high and low, loop resistance, loop current, and voltage between TIP/ RING. rrev: Test loop condition in battery reversal condition. force: Perform the tests immediately, even if the port is in use.	E	13

Table 282 VoIP Commands Summary (continued)

COMMAND	DESCRIPTION	M	P
<code>voip diagnostic mlt test</code> <code><account> <option></code> <code>[force]</code>	Performs the metallic line test by the specified VoIP SIP account. This command applies when using SIP firmware. <i>account</i>: Existing account. <i>option</i>: all vac vdc rload riso cap ren ring metering dialtone digit roh <i>all</i>: Perform all tests on the line connected to the specified VoIP line card port. <i>vac</i>: Test the line's AC voltage only. <i>vdc</i>: Test the line's DC voltage only. <i>rload</i>: Test the line's load resistance only <i>riso</i>: Test the line's isolation resistance only. <i>cap</i>: Test the line's capacitance only. <i>ren</i>: Test the line's ringer equivalent number only. <i>ring</i>: Test the line's ring voltage only. <i>metering</i>: Test the line's metering voltage only. <i>dialtone</i>: Test the line's dialtone only. <i>digit</i>: Test if the line circuit accepts dialed digits and switches the call to its destination. <i>roh</i>: Test if the receiver is off hook only. <i>force</i>: Perform the tests immediately, even if the port is in use.	E	13
<code>show voip h248</code>	Displays H.248 configuration. This command applies when using H.248 firmware.	E	13
<code>voip h248</code>	Enters the sub-command mode for configuring the global H.248 settings. This command applies when using H.248 firmware.	C	13
<code>exit</code>	Leaves VoIP H.248 editing. This command applies when using H.248 firmware.		
<code>clear statistics</code>	Clears control packet statistics. This command applies when using H.248 firmware.	C	13
<code>digit-map-timeout</code> <code><start-timeout></code> <code><short-timeout></code> <code><long-timeout></code>	Configures digit collection timeout. This command applies when using H.248 firmware. <i>start-timeout</i>: Set the timeout period if the user doesn't send any DTMF signal after off-hook, in seconds (0-99). 0 disables the timeout. <i>short-timeout</i>: Set the H.248 short time-out, in seconds (1-99). You define the short and long timeout values and the IES selects which to use. <i>long-timeout</i>: Set the H.248 long time-out, in seconds (1-99). You define the short and long timeout values and the MGC selects which to use. <i>start-timeout</i>: 16 <i>short-timeout</i>: 4 <i>long-timeout</i>: 4	C	13

Table 282 VoIP Commands Summary (continued)

COMMAND	DESCRIPTION	M	P
dscp <dscp>	Configures the value of the DSCP bit (0-63) carried on H.248 packets. This command applies when using H.248 firmware. Default:48.	C	13
encode long short	Configures the text encoding type of the H.248 messages the IES sends out. This command applies when using H.248 firmware. long: Long text encoding. short: Short text encoding. default: Long text.	C	13
force-version	Forces the IES to use only H.248 version 1 for VoIP. This command applies when using H.248 firmware.	C	13
no force-version	Allows the IES to use H.248 version 1 or 2 for VoIP. This command applies when using H.248 firmware.	C	13
inactivity-timer <timeout>	Configures the inactivity timeout. The MG sends a notify packet if there is no communication between the Media Gateway (MG) and the Media Gateway Controller (MGC) in the configured timeout period. This command applies when using H.248 firmware. timeout: 0-65535 in units of 10 milliseconds. 0 disables this feature. Default: 0.	C	13
mg	Has the IES start MG operation and attempt to register with the MGC. This command applies when using H.248 firmware.	C	13
no mg	Has the IES stop MG operation and de-register from the MGC. This command applies when using H.248 firmware.	C	13
mg <mg-name>	Configures the H.248 MG name. This command applies when using H.248 firmware. mg-name: up to 31 characters.	C	13
mg port <mg-port>	Configures the TCP/UDP port number the H.248 MG uses. This command applies when using H.248 firmware. mg-port: 1025-65535, default: 2944.	C	13
mgc ip <mgc-ip-dn>	Configures the H.248 primary MGC IP address or domain name. This command applies when using H.248 firmware. mgc-ip-dn: 0.0.0.0-223.255.255.255 or domain name, default: 0.0.0.0	C	13
mgc port <mgc-port>	Configures the H.248 primary MGC TCP/UDP port. This command applies when using H.248 firmware. mgc-port: 1025-65535, default: 2944.	C	13
mgc2	Enables the secondary MGC. This command applies when using H.248 firmware.	C	13
no mgc2	Disables the secondary MGC. This command applies when using H.248 firmware.	C	13
mgc2 ip <mgc-ip-dn>	Configures the H.248 secondary MGC IP address or domain name. This command applies when using H.248 firmware. mgc-ip-dn: 0.0.0.0-223.255.255.255 or domain name. This is not available when the secondary MGC is disabled.	C	13

Table 282 VoIP Commands Summary (continued)

COMMAND	DESCRIPTION	M	P
<code>mgc2 port <mgc-port></code>	Configures the H.248 secondary MGC TCP/UDP port. This command applies when using H.248 firmware. <i>mgc-port</i> : 1025-65535 Note: This is not available when the secondary MGC is disabled.	C	13
<code>retransmit-time <init-retransmit-time> <min-retransmit-time> <max-retransmit-time> <retransmit-window></code>	Configures the retransmission timers. This command applies when using H.248 firmware. <i>init-retransmit-time</i> : 100-20000 milliseconds (in increments of 100). The initial retransmit timer is used when the MG didn't establish a control link between the MG and MGC during this enable time. <i>min-retransmit-time</i> : 100-1000 milliseconds (in increments of 100). The minimum duration between any two packets after registration. <i>max-retransmit-time</i> : 1000-20000 milliseconds (in increments of 100). The maximum duration between any two packets after registration. <i>retransmit-window</i> : 1000-60000 milliseconds (in increments of 100). The total retransmit timer.	C	13
<code>rfc2833</code>	Enables RFC2833 DTMF relay when the MGC allows. The system transmits DTMF signals as voice (in-band) or as separate RFC 2833 packets (out-of-band) according to the MGC's configuration. This command applies when using H.248 firmware.	C	13
<code>no rfc2833</code>	Disables RFC2833 DTMF relay when the MGC allows. The system transmits DTMF signals as voice (in-band). This command applies when using H.248 firmware.	C	13
<code>rfc2833 ptype <rfc2833-ptype></code>	Configures the RFC2833 RTP payload type used for DTMF relay. This command applies when using H.248 firmware. <i>rfc2833-ptype</i> : 96-127, default: 101. This is only available when RFC2833 is enabled.	C	13
<code>rtp-port <start-port> <end-port></code>	Configures the UDP port range used by RTP packets. This command applies when using H.248 firmware. <i>start-port</i> : An even number from 4000-64000. <i>end-port</i> : An even number from 5000-65000, at least 1000 larger than <i>start-port</i> .	C	13

Table 282 VoIP Commands Summary (continued)

COMMAND	DESCRIPTION	M	P
<code>soft-switch</code> <code>DEFVAL zxss10-ss huawei-soft3000 alu-5020 nsn iskratel</code>	Configures special call flows for interoperability with special MGCs. This command applies when using H.248 firmware. DEFVAL: The default call flow. zxss10-ss: Special call flow for interoperability with the ZTE zxss10 soft switch. huawei-soft3000: Special call flow for interoperability with the HUAWEI-soft3000 soft switch. alu-5020: Special call flow for interoperability with the ALU-5020 soft switch. nsn: Special call flow for interoperability with the NSN soft switch. iskratel: Special call flow for interoperability with the ISKRATEL soft switch.	C	13
<code>t38</code>	Enables support for the T.38 fax relay standard. This command applies when using H.248 firmware. When you enable T.38 the system uses T.30 to transmit faxes as voice (in-band) or T.38 to transmit faxes as separate packets (out-of-band) according to the MGC's configuration.	C	13
<code>no t38</code>	Disables support for the T.38 fax relay standard. The system uses T.30 to transmit faxes as voice (in-band). This command applies when using H.248 firmware.	C	13
<code>transport udp tcp</code>	Sets whether to use UDP or TCP as the H.248 transport protocol. This command applies when using H.248 firmware. Default: tcp	C	13
<code>vbd</code>	Enables the Voice Band Data service. Voice band data uses V.152 to define settings for transmitting data in order to improve voice quality. Whether or not V.152 is actually used depends on the MGC's configuration. This command applies when using H.248 firmware.	C	13
<code>no vbd</code>	Disables the Voice Band Data service. This command applies when using H.248 firmware.	C	13
<code>rtp-termination-id prefix <prefix></code>	Sets the RTP ephemeral termination ID's prefix. It can be up to 31 characters. This command applies when using H.248 firmware. Default: RTP/	C	13
<code>rtp-termination-id suffix-start-number <start-number></code>	Configures the RTP ephemeral termination ID's suffix start number. This command applies when using H.248 firmware. start-number: Up to 15 digits, default: 1	C	13
<code>rtp-termination-id suffix-length <suffix-length></code>	Configures how many digits to use for the RTP ephemeral termination ID. This command applies when using H.248 firmware. suffix-length: 0-15, default: 0	C	13
<code>voip ip address <ip-address>/<mask> vlan <vid> [pbit <pbit>]</code>	Configures the VoIP interface IP address, mask, VLAN ID, and priority bit. Disables the DHCP client function on the interface if it is enabled. ip-address: 1.0.0.0 ~ 223.255.255.255	C	13
<code>voip ip address dhcp vlan <vid> [pbit <pbit>]</code>	Configures the VoIP interface as a DHCP client.	C	13
<code>voip ip address dhcp release renew</code>	Performs the DHCP operations on the VoIP interface. release: Release the dynamic IP address renew: Renew the dynamic IP address	C	13

Table 282 VoIP Commands Summary (continued)

COMMAND	DESCRIPTION	M	P
voip ip dns <dns-ip>	Configures the DNS server address that the VoIP interface uses. <i>dns-ip</i> : 0.0.0.0 ~ 223.255.255.255	C	13
voip ip default-gateway <gateway-ip>	Configures the default gateway of the VoIP interface. <i>gateway-ip</i> : 0.0.0.0-223.255.255.255	C	13
show voip ip address	Displays the VoIP interface IP address.	E	13
show voip ip default-gateway	Displays the VoIP interface default gateway.	E	13
show voip ip dns-ip	Displays the VoIP interface DNS IP address.	E	13
show voip ip mode	Displays the VoIP interface DHCP settings.	E	13
voip rtp ip address <ip-address>/<mask> vlan <vid>	Configures the VoIP RTP interface IP address, subnet mask, and VLAN ID. Disables the DHCP client function on the interface if it is enabled. <i>ip-address</i> : 0.0.0.1 ~ 223.255.255.255 <i>mask</i> : 1 ~ 30	C	13
voip rtp ip address dhcp vlan <vid>	Configures the VoIP RTP interface to act as a DHCP client.	C	13
voip rtp ip address dhcp release renew	Performs the specified DHCP operation on the VoIP RTP interface. <i>release</i> : Release dynamic IP address. <i>renew</i> : Renew dynamic IP address.	C	13
voip rtp ip default-gateway <gateway-ip>	Configures the default gateway of the VoIP RTP interface. <i>gateway-ip</i> : 0.0.0.1 ~ 223.255.255.255	C	13
no voip rtp	Removes all the VoIP RTP configurations.	C	13
show voip rtp ip address	Displays the VoIP RTP interface's IP address settings.	E	13
show voip rtp ip default-gateway	Displays the default gateway of the VoIP RTP interface.	E	13
show voip rtp ip dhcp	Displays the DHCP setting on the VoIP RTP interface.	E	13
show interface voip <slot/portlist>	Displays the configuration on the specified VoIP ports	E	13
interface voip <slot/portlist>	Enters the sub-command mode for configuring the specified VoIP ports.	C	13
exit	Leaves the VoIP port configuration sub-command mode.	C	13
dsp-profile <profile-name>	Configures the VoIP DSP profile. Default: DEFVAL	C	13
vbd-dsp-profile <profile-name>	Configures the VoIP DSP profile for voice band data service.	C	13
no vbd-dsp-profile	Removes reference to a VoIP DSP profile for voice band data service. The voice band data service will refer to the VoIP DSP profile used for voice service.	C	13
clear call-statistics	Clears the VoIP SIP call statistics. This command applies when using SIP firmware.	C	13
active	Enables the VoIP port.	C	13
no active	Disables the VoIP port.	C	13

Table 282 VoIP Commands Summary (continued)

COMMAND	DESCRIPTION	M	P
<code>pots data-gain <tx-gain> <rx-gain></code>	Sets the amount of gain (increase in volume) to apply to the voice band data service the subscriber transmits (tx) or receives (rx). A negative value decreases the volume. <i>tx-gain</i> : -20-20 in units of 1dB, default: 0 <i>rx-gain</i> : -20-20 in units of 1 dB, default: -3	C	13
<code>pots voice-gain <tx-gain> <rx-gain></code>	Sets the amount of gain (increase in volume) to apply to the voice signal the subscriber transmits (tx) or receives (rx). A negative value decreases the volume. <i>tx-gain</i> : -20-20 in units of 1 dB, default: 0 <i>rx-gain</i> : -20-20 in units of 1 dB, default: -3	C	13
<code>pots battery low high boost</code>	Controls the battery supply of a port. <i>low</i> : is for short loop. <i>high</i> : is for long loop. <i>boost</i> : is for even more power for an even longer loop.	C	13
<code>pots vmwi <FSK voltage></code>	Configures the Visual Message Waiting Indicator (VMWI) format for the port. This command applies when using SIP firmware. <i>FSK</i> : Frequency shift keying <i>voltage</i> : send a higher voltage to the user port periodically	C	13
<code>no pots vmwi</code>	Restores the VMWI format to the default value. This command applies when using SIP firmware.	C	13
<code>impedance <impedance></code>	Sets the POTS impedance level on the specified subscriber port. <i>impedance</i> : Desired impedance, 0-10 0: 600ohm 1: 600ohm_1000nf 2: 220ohm_820ohm_120nf 3: 270ohm_750ohm_150nf 4: 300ohm_1000ohm_220nf 5: 370ohm_620ohm_310nf 6: 220ohm_680ohm_100nf 7: 220ohm_820ohm_115nf 8: 900ohm 9: 200ohm_680ohm_100nf 10: 900ohm_2160nf Default: Not specified (use the impedance value defined in the currently selected country code)	C	13
<code>no impedance</code>	Has the specified subscriber port use the impedance value defined in the currently selected country code.	C	13
<code>h248 termination-id <termination-id></code>	Configures the H.248 physical termination ID. This command applies when using H.248 firmware. <i>termination-id</i> : Up to 31 printable characters	C	13

Table 282 VoIP Commands Summary (continued)

COMMAND	DESCRIPTION	M	P
<code>sip account <account></code>	This command applies when using SIP firmware. Configures an account for SIP registration. Use up to 63 characters.	C	13
<code>sip name <name></code>	This command applies when using SIP firmware. Configures a name for SIP registration. Use up to 47 characters.	C	13
<code>sip password <password></code>	This command applies when using SIP firmware. Sets the password for SIP registration. Use up to 31 printable characters.	C	13
<code>sip tel-number <tel-number></code>	This command applies when using SIP firmware. Sets the telephone number. The telephone number must be unique. Use up to 15 alphanumeric characters or use two quotation marks ("") to clear the field for SIP registration.	C	13
<code>sip hotline <on <hotline-no> <timeout> off></code>	This command applies when using SIP firmware. Configures the hotline feature to have the IES automatically dial a number when someone picks up the phone connected to the selected port. <i>hotline-no</i>: Specify the telephone number to call. Use up to 31 characters. Only alphanumeric characters and '+' are allowed. Note: '+' is only allowed as the first character. <i>timeout</i>: the number of seconds the IES waits before dialing the hotline number. 0-255 seconds. 0 means dial immediately.	C	13
<code>sip svc-profile <profile name></code>	This command applies when using SIP firmware. Configures the VoIP SIP Service profile of SIP Call service settings for the port.	C	13
<code>sip polarity-reverse <on off></code>	This command applies when using SIP firmware. Turns polarity reversal on or off. Turn on polarity reversal to reverse the tip and ring after a call is established and again after it terminates. This is used for example, as a charging signal for some types of payphone.	C	13
<code>show voip pots</code>	Displays the POTS parameters.	E	13
<code>show voip pots ring</code>	This command applies when using SIP firmware. Displays the POTS ring pattern setting for SIP.	E	13
<code>voip pots</code>	Enters the sub-command mode for configuring the system-wide POTS parameters.	C	13
<code>exit</code>	Leaves the POTS editing sub-command mode.	C	13
<code>hook-flash-time <max-time> <min-time></code>	Sets how long (in milliseconds) a user has to press the flash key to register its use. <i>max-time</i>: 20-1500 in units of milliseconds <i>min-time</i>: 20-1500 in units of milliseconds <i>min-time</i> < <i>max-time</i> <= 1500 milliseconds. If <i>min-time</i> is less than max-break time, the pulse digit detection will be disabled. Max-break time can be found in the country code setting. default: Not specified (the IES uses the value defined in the currently selected country code).	C	13
<code>no hook-flash-time</code>	Uses the value defined in the current selected country code.		
<code>off-hook-time <min-time></code>	Configures the off-hook detection time threshold. <i>min-time</i>: 0-30 in units of milliseconds default: 30.	C	13
<code>no off-hook-time</code>	Uses the value defined in the current selected country code.	C	13

Table 282 VoIP Commands Summary (continued)

COMMAND	DESCRIPTION	M	P
ring index <index>	Enters sub-commands for configuring the specified ring pattern index. This command applies when using SIP firmware. <i>index</i> : 1-16	C	13
exit	Leaves the ring index editing sub-command mode. This command applies when using SIP firmware.	C	13
name <name>	This ring index sub-command configures the name for the ring pattern index. This command applies when using SIP firmware. <i>name</i> : 1-31 printable characters	C	13
no name	This ring index sub-command restores the name for the ring pattern index. This command applies when using SIP firmware.	C	13
pattern on1 <on-period> off1 <off-period> [on2 <on-period> off2 <off-period> on3 <on-period> off3 <off-period>]	This ring index sub-command configures the ring pattern. This command applies when using SIP firmware. <i>on-period</i> : the duration of the ring. 100-10000 in milliseconds. Or use 65535 to set a continuous time and have the IES ignore the following parameters. <i>off-period</i> : the length of time between rings. 100-10000 in milliseconds. Or use 65535 to set a continuous time and have the IES ignore the following parameters.	C	13
no pattern	This ring index sub-command restores the ring pattern to the default value. This command applies when using SIP firmware.	C	13
show voip countrycode	Displays the country code information.	E	13
show voip diagnostic mlt <slot>/<port>	Displays the Metal Line Test results on the specified VoIP port.	E	13
show voip diagnostic mlt tel <tel-number>	Displays Metal Line Test results on the specified phone number.	E	13
show voip diagnostic mlt termination-id <termination-id>	Displays Metal Line Test results on the specified H.248 termination ID.	E	13
show voip diagnostic mlt <account>	This command applies when using SIP firmware. Displays Metal Line Test results on the specified SIP account.	E	13
show interface voip <slot>/<portlist>	Displays the configuration of the specified VoIP ports.	E	13
show interface voip <slot>/<portlist> lineinfo	Displays the line info for the specified VoIP ports.	E	13
show interface voip <slot>/<portlist> statistics	Displays the statistics on the specified VoIP ports.	E	13
show interface voip <slot>/<port-list> service-stat	Displays the service state for the specified VoIP ports.	E	13
no voip dsp-profile <name>	Removes the specified VoIP DSP profile.	C	13
show voip dsp-profile <name>	Displays the content of the specified VoIP DSP profile.	E	13
voip dsp-profile <name>	Enters the sub-command mode for configuring the specified VoIP DSP profile.	C	13

Table 282 VoIP Commands Summary (continued)

COMMAND	DESCRIPTION	M	P
<code>codec <codec></code> [<codec> ...]	Configures the preferred voice codec. <i>codec</i> : g711a, g711mu, g723, g726-16, g726-24, g726-32, g726-40, and g729ab default: g711a g711mu	C	13
<code>dscp <dscp></code>	Configures the DSCP value carried on the RTP packets for normal voice service. <i>dscp</i> : 0-63 default: 48	C	13
<code>echo-tail <echo-tail></code>	Configures the echo cancellation echo tail length in milliseconds. <i>echo-tail</i> : 8, 16, 32, 64, 128 default: 32	C	13
<code>echo-cancel</code>	Enables the echo cancellation for normal voice service.	C	13
<code>no echo-cancel</code>	Disables the echo cancellation for normal voice service.	C	13
<code>g711vpi <vpi></code>	Configures the voice packet interval for the G.711 codec for normal voice service. <i>vpi</i> : 10, 20, 30 or 40 milliseconds. default: 20	C	13
<code>g723vpi <vpi></code>	Configures the voice packet interval for the G.723 codec for normal voice service. <i>vpi</i> : 30 or 60 milliseconds. default: 30	C	13
<code>g726vpi <vpi></code>	Configures the voice packet interval for the G.726 codec for normal voice service. <i>vpi</i> : 10, 20, 30, or 40 milliseconds default: 20	C	13
<code>g729vpi <vpi></code>	Configures the voice packet interval for the G.729 codec for normal voice service <i>vpi</i> : 10, 20, 30, 40, 50 or 60 milliseconds default: 20	C	13
<code>pbit <pbit></code>	Configures the PBIT value (0-7) carried on the RTP packets for normal voice service. Default: 7	C	13
<code>play-buffer <min-delay> <max-delay></code>	Configures the voice play out buffer depth for normal voice service. <i>min-delay</i> : 10-500 in milliseconds <i>max-delay</i> : 10-500 in milliseconds default: <i>min-delay</i> : 10 ms <i>max-delay</i> : 80 ms	C	13
<code>vad-inactive</code>	Disables Voice Activity Detection for normal voice service.	C	13
<code>no vad-inactive</code>	Enables Voice Activity Detection for normal voice service.	C	13
<code>exit</code>	Leaves DSP profile editing.	C	13

38.6 H.248 Command Examples

These commands apply when using H.248 firmware. This example shows how to let two ports make VoIP-H248 calls to each other. You have to first configure the following settings depending on your MGC's settings:

- Enable VLAN on all Gigabit Ethernet ports
- The IP address, VLAN and priority for VoIP interface: 192.168.2.10/24, VLAN 200, priority 7
- MGC IP address: 192.168.2.100
- MG name: MG1_2U
- Termination IDs of ports 1 and 2 of the VoIP line card on slot 3: term1_1 and term1_2
- DSP profile: DEFVAL

Finally, activate VoIP on the ports and then the ports can make a VoIP-H248 call to each other.

```

ras# config
ras(config)# interface ge-nni *
ras(config-interface-ge-nni-*)# vlan all
ras(config-interface-ge-nni-*)# exit
ras(config)# voip ip address 192.168.2.10/24 vlan 200 pbit 7
ras(config)# voip h248
ras(config-voip-h248)# mgc ip 192.168.2.100
ras(config-voip-h248)# mg MG1_2U
ras(config-voip-h248)# mg
ras(config-voip-h248)# exit
ras(config)# interface voip 3/1
ras(config-interface-voip-3/1)# dsp-profile DEFVAL
ras(config-interface-voip-3/1)# h248 termination-id term1_1
ras(config-interface-voip-3/1)# active
ras(config-interface-voip-3/1)# exit
ras(config)# interface voip 3/2
ras(config-interface-voip-3/2)# dsp-profile DEFVAL
ras(config-interface-voip-3/2)# h248 termination-id term1_2
ras(config-interface-voip-3/2)# active
ras(config-interface-voip-3/2)# exit

```

Here is an example of configuring H.248 VoIP. The following commands configure the IES to:

- Use VoIP IP address 172.16.19.200, netmask 24, and VID2 for VoIP.
- Have VoIP port 1 on the POTS card in slot 4 use A301 as its termination ID.
- Enable VoIP port 1 on the POTS card in slot 4.
- Set the country code to 0 to use the USA VoIP parameters.
- Use a MGC at IP address 172.16.19.24 using port 2988.
- Use the long encoding format.

- Start the MG to have it register with the MGC.

```

ras# configure
ras(config)# voip ip address 172.16.19.200/24 vlan 2
ras(config)# interface voip 4/1
ras(config-interface-voip-4/1)# h248 termination-id A301
ras(config-interface-voip-4/1)# active
ras(config-interface-voip-4/1)# exit
ras(config)# countrycode 0
ras(config)# voip h248
ras(config-voip-h248)# voip ip address 192.168.3.174/24 vlan 2
ras(config-voip-h248)# mgc ip 172.16.19.24
ras(config-voip-h248)# mgc port 2988
ras(config-voip-h248)# encode long
ras(config-voip-h248)# mg
ras(config-voip-h248)# exit
ras(config)# exit

```

Test your configuration by making a call from a phone connected to the port you configured. Alternatively, use the `show interface voip <slot>/<portlist> linestat` command to check whether the relevant port is successfully registered with the MGC (the state should be "idle").

38.7 VoIP SIP Commands (SIP Firmware Only)

These commands apply when using SIP firmware. Use the `voip sip` command in configuration mode to access the SIP configuration subcommands in the following table. Use enable mode to enter the enable mode (E) commands.

Table 283 VoIP SIP Commands (SIP Firmware Only)

COMMAND	DESCRIPTION	M	P
<code>exit</code>	Leaves VoIP SIP editing.	C	13
<code>key-pattern <name></code>	Configures a SIP key pattern and enters the sub-command mode for editing it. A key pattern profile is a set of telephone keys that users press to access a variety of features such as call hold, call transfer, and so on. <i>name</i> : 1-31 printable characters.	C	13
<code>exit</code>	Leaves SIP key pattern editing.	C	13
<code>call-transfer <pattern></code>	Sets the key pattern for transferring a call. <i>pattern</i> : up to 7 characters, allowed characters are 0-9, *, and #. Example: 43#	C	13
<code>call-wait-off <pattern></code>	Sets the key pattern for turning the call waiting service off. <i>pattern</i> : up to 7 characters, allowed characters are 0-9, *, and #. Example: #43#	C	13
<code>call-wait-on <pattern></code>	Sets the key pattern for turning the call waiting service on. <i>pattern</i> : up to 7 characters, allowed characters are 0-9, *, and #. Example: *43#	C	13
<code>call-wait-disconn <pattern></code>	Sets the key pattern the user presses to disconnect a current call and accept a waiting call (one character only). <i>pattern</i> : 1 character, allowed characters are 0-9, *, and #. Example: 1	C	13

Table 283 VoIP SIP Commands (SIP Firmware Only) (continued)

COMMAND	DESCRIPTION	M	P
<code>call-wait-onhold <pattern></code>	Sets the key pattern the user presses to place a current call on hold and accept a waiting call (one character only). <i>pattern</i> : 1 character, allowed characters are 0-9, *, and #. Example: 2	C	13
<code>call-wait-reject <pattern></code>	Sets the key pattern the user presses to reject a waiting call. <i>pattern</i> : 1 character, allowed characters are 0-9, *, and #. Example: 0	C	13
<code>clir <pattern></code>	Sets the key pattern the user presses to restrict his/her phone number by not sending caller ID information. <i>pattern</i> : up to 7 characters, allowed characters are 0-9, *, and #.	C	13
<code>dnd-off <pattern></code>	Sets the key pattern the user presses to turn off Do Not Disturb (1~7 characters). <i>pattern</i> : up to 7 characters, allowed characters are 0-9, *, and #.	C	13
<code>dnd-on <pattern></code>	Sets the key pattern the user presses to turn on Do Not Disturb (1~7 characters). <i>pattern</i> : up to 7 characters, allowed characters are 0-9, *, and #.	C	13
<code>no keypattern <name></code>	Removes the specified SIP key pattern. <i>name</i> : specify the name of an existing key pattern, 1-31 printable characters.	C	13
<code>show keypattern [name]</code>	Displays the settings of all the key patterns or the specified one. <i>name</i> : specify the name of an existing key pattern, 1-31 printable characters.	E	3
<code>dialplan <name> index <index></code>	This <code>voip sip</code> subcommand configures a dial plan entry of the specified index in the specified dial plan table and enters the subcommand mode for editing it. Use the dial plan entries to configure the IES to identify specific types of phone numbers dialed by a user, and to process the number before transmission by deleting, replacing, or adding digits according to the relevant rule. The dial plan can also forward the call to a specific SIP server. <i>name</i> : the name of the dial plan, 1-31 printable characters. <i>index</i> : the index of the dial plan table, 1-32.	C	13
<code>exit</code>	Leaves the dial plan profile editing subcommands.	C	13

Table 283 VoIP SIP Commands (SIP Firmware Only) (continued)

COMMAND	DESCRIPTION	M	P
<code>pattern <pattern></code>	This subcommand within the <code>dialplan</code> subcommands sets the pattern of dialed digits to which this dial plan index refers. The IES applies the dial plan index's rule if the user dials a number that matches the pattern. <i>pattern</i>: up to 47 characters. Allowed characters are: - Numerals "0" ~ "9" "x" representing a digit 0 ~ 9, a "*", or a "#". - Asterisk "*" (meaning just an "*") - Period "." (representing zero or more repetitions of the character or range preceding it). For example "5." means no fives (nothing) or any number of fives; but not any other character. "[1~3]." means no ones, twos, or threes (nothing) or any number of ones, twos, or threes; but not any other character. - Tilde "~" (representing a range of digits, for example "[3~9]"). The tilde must be used in brackets, and characters to either side of the tilde must both be digits. - Comma ",", (representing a choice of digits. for example "[4,9]"). The comma must be used in brackets, and characters to either side of the comma must both be digits. - Pipe " ", separating number plan patterns. - Brackets "[" and "]" (representing an allowed range, for example "[1,3~5]"). - A maximum of one pair of parentheses "(" and ")" "T" if a user dials some numbers and then presses "#", the rule will be applied and the numbers will be dialed out at once. For example: take the pattern "002(1.)T" and rule "\1". The "002(1.)" pattern represents "002" followed by zero or more ones. The "\1" rule replaces the "002" with the zero or more ones. So, if a user presses 00211111#, the VOP will dial out 11111 immediately. Note: If only pattern is set, the indexed pattern and rule pair will be cleared.	C	13

Table 283 VoIP SIP Commands (SIP Firmware Only) (continued)

COMMAND	DESCRIPTION	M	P
<code>rule <rule></code>	This subcommand within the <code>dialplan</code> subcommands sets the action the IES applies if the user dials a number that matches the dial plan index's pattern. <i>rule</i>: Up to 15 characters, allowed characters are 0~9, and: “\c” = the Pattern String is replaced by the countrycode (specified in the relevant call service profile). “\d” = the Pattern String is replaced by the national destination (region) code (specified in the relevant call service profile). “\1” = the Pattern String is replaced by the characters represented inside the parentheses “(” and “)” in the Pattern String. This means the characters represented inside the Pattern String's parentheses are used in dialing the call and the rest of the Pattern String's represented characters are discarded. “deny” = the Pattern String is not allowed. For example: - If the Pattern String is “00244(x.)”, the Rule String is “\c\1” and the country code in the relevant call service profile is “28”, the dialed number “00244123456” becomes “28123456”. - If the Pattern String is “010(x.)”, the Rule String is “\d\1” and the national destination code in the relevant call service profile is “01473”, the dialed number “010456789” becomes “01473456789”. - If the Pattern String is “0440(1x.)” and the Rule String is “\1”, the dialed number “04401473987654” becomes “1473987654”.	C	13
<code>no dialplan <name> [index <index>]</code>	Removes the specified dial plan or the specified index in the specified dial plan table. <i>name</i>: the name of the dial plan, 1-31 printable characters. <i>index</i>: the index of the dial plan table, 1-32.	C	13
<code>show dialplan [name]</code>	Displays the settings of all dial plans or the specified dial plan. <i>name</i>: the name of the dial plan, 1-31 printable characters.	E	3
<code>localcall enter-time <enter-time> exit-time <exit-time></code>	When the IES cannot connect to the SIP server, it can still allow subscribers to call other connected subscribers. Configure the enter time and exit time for enabling the local call service. <i>enter-time</i>: the interval between disconnecting from the SIP server and then entering the local call state. 1-60 in minutes. Default 1 minute. <i>exit-time</i>: the interval between establishing a stable connection to the SIP server and returning from local call service to normal call services. 1-60 in minutes. Default 1 minute.	C	13
<code>no localcall</code>	Restores the local call parameters to the default values.	C	13
<code>localhelp <name> index <index></code>	Local help lets you configure which local subscribers are called instead of public emergency (or other) numbers in the event that the link to the VoIP provider is not available. This command configures an index of emergency call setting and enters the subcommands for editing it. <i>name</i>: 1-31 printable characters	C	13
<code>exit</code>	Leaves the local help editing subcommands.	C	13

Table 283 VoIP SIP Commands (SIP Firmware Only) (continued)

COMMAND	DESCRIPTION	M	P
<code>tel <tel number></code>	This command configures the telephone number of the specified index in the specified local help table. <i>tel number</i> : up to 15 characters, only alphanumeric characters and '+' are allowed or use two quotation marks () to clear the field. Note: '+' only is allowed as the first character.	C	13
<code>no localhelp <name></code>	Removes the specified local help setting. <i>name</i> : 1-31 printable characters.	C	13
<code>show localhelp [name]</code>	Displays the settings of all the local help tables or the specified local help table. <i>name</i> : the name of the local help table, 1-31 printable characters.	E	3
<code>sip-profile <name></code>	Configures the specified SIP protocol configuration settings profile and enters the sub-command mode for editing it. <i>name</i> : the name of the profile, 1-31 printable characters.	C	13
<code>exit</code>	Leaves the SIP profile editing subcommands.	C	13
<code>sip-server <address-domain></code>	Specifies the IP address or domain name of the SIP server. <i>address-domain</i> : IP-address or domain name, maximum size of the domain name is 63.	C	13
<code>reg-server <address-domain></code>	Specifies the IP address or domain name of the SIP registration server. <i>address-domain</i> : IP-address or domain name, maximum size of the domain name is 63.	C	13
<code>proxy-server <address-domain></code>	Specifies the IP address or domain name of the SIP proxy server. <i>address-domain</i> : IP-address or domain name, maximum size of the domain name is 63.	C	13
<code>sip-server2 <address-domain></code>	Specifies the IP address or domain name of the secondary SIP server. <i>address-domain</i> : IP-address or domain name, maximum size of the domain name is 63.	C	13
<code>reg-server2 <address-domain></code>	Specifies the IP address or domain name of the secondary SIP registration server. <i>address-domain</i> : IP-address or domain name, maximum size of the domain name is 63.	C	13
<code>proxy-server2 <address-domain></code>	Specifies the IP address or domain name of the secondary SIP proxy server. <i>address-domain</i> : IP-address or domain name, maximum size of the domain name is 63.	C	13
<code>sip-port <port></code>	Specifies the port number of the primary SIP User Agent. <i>port</i> : 1025-65535, 0 for not specifying a port.	C	13
<code>reg-port <port></code>	Specifies the port number of the primary SIP registration server. <i>port</i> : 1025-65535, 0 for not specifying a port.	C	13
<code>proxy-port <port></code>	Specifies the port number of the primary SIP proxy server. <i>port</i> : 1025-65535, 0 for not specifying a port.	C	13

Table 283 VoIP SIP Commands (SIP Firmware Only) (continued)

COMMAND	DESCRIPTION	M	P
<code>sip2-port <port></code>	Specifies the port number of the secondary SIP User Agent. <i>port</i> : 1025-65535, 0 for not specifying a port.	C	13
<code>reg2-port <port></code>	Specifies the port number of the secondary SIP registration server. <i>port</i> : 1025-65535, 0 for not specifying a port.	C	13
<code>proxy2-port <port></code>	Specifies the port number of the secondary SIP proxy server. <i>port</i> : 1025-65535, 0 for not specifying a port.	C	13
<code>uri-type <sip tel></code>	Specifies the type of URI to use during the exchange of SIP message (SIP or telephone number).	C	13
<code>dual-server <on off></code>	Enables or disables the dual server feature.	C	13
<code>dns-srv <on off></code>	Enables or disables the dual server locating feature.	C	13
<code>dscp <dscp></code>	Specifies the DiffServ Code Point value for SIP and RTP packets. <i>dscp</i> : 0-63.	C	13
<code>switch-type <ZTE NSN ALU HUA ISK></code>	Specifies the type of VoIP switch. ZTE: ZTE Soft Switch NSN: NSN Soft Switch ALU: Alcatel-Lucent-HPSS/3.0.3 Soft Switch HUA: HUAWEI Soft3000 SoftSwitch ISK: ISKRATEL soft switch	C	13
<code>keep-alive <on <timeout> off></code>	Enables or disables the SIP session keep alive feature. When this is on, the SIP UA periodically sends SIP session refresh requests based on the configured session expiration time. <i>timeout</i> : session expiration time in seconds, 90-65535.	C	13
<code>prack <on off></code>	The PROvisional ACKnowledgement response is sent in reply to a SIP INVITE request. Enables or disables the SIP Provisional ACK feature.	C	13
<code>noncecountkeep</code>	Helps protect against replay attacks.	C	13
<code>rtp-port start-port <port> end-port <port></code>	Configures the start and end Real time Transport Protocol (RTP) ports to use for voice data transfer. Starting port should be even, 4000~64000. Ending port should be even, 5000~65000. There should be at least 1000 between the starting port and the ending port.	C	13
<code>failretry <time></code>	Configures the register fail retry interval time. <i>time</i> : register fail retry interval time in seconds, 120-900.	C	13
<code>registration <on <time> off></code>	Configures the registration period. <i>time</i> : registration expiration time, 120-65535 in seconds.	C	13
<code>no sip-profile <name></code>	Removes the specified SIP profile.	C	13
<code>show sip-profile [name]</code>	Displays the settings of all the SIP profiles or the specified SIP profile. <i>name</i> : the name of the SIP profile, 1-31 printable characters.	E	3

Table 283 VoIP SIP Commands (SIP Firmware Only) (continued)

COMMAND	DESCRIPTION	M	P
<code>svc-profile <name></code>	Configures a SIP call service settings profile with the specified name and enters the sub-command mode for editing it. <i>name</i> : the name of the profile, 1-31 printable characters.	C	13
<code>exit</code>	Leaves the SIP call service settings profile editing subcommands.	C	13
<code>callhold <on off></code>	Enables or disables the call hold service.	C	13
<code>calltransfer <on off></code>	Enables or disables the call transfer service.	C	13
<code>callwait <on off></code>	Enables or disables the call waiting service.	C	13
<code>centrex <on off></code>	Enables or disables centrex operation.	C	13
<code>cidcw <on off></code>	Enables or disables the display of caller ID during call waiting.	C	13
<code>clip <on off></code>	Enables or disables the Caller Line Identifier Presentation service.	C	13
<code>clir <on off></code>	Enables or disables caller ID restriction.	C	13
<code>dnd <on off></code>	Enables or disables Do not Disturb.	C	13
<code>dtmf <bypass rfc2833 <payload-type> sipinfo rfc2833like plaintext></code>	Sets how to handle DTMF signals. <i>bypass</i> : Do not relay DTMF signals. <i>rfc2833</i> : Relay DTMF tones according to RFC2833. The IES transmits DTMF tones by RTP packet whose payload type is specific and adjusted by negotiated SDP. <i>payload-type</i> : When you enable RFC 2833, set the RTP payload type (96-127) for identifying RFC 2833 packets. <i>sipinfo</i> : Relay DTMF signals via SIP INFO message. <i>rfc2833like</i> : Relay DTMF signals via SIP INFO but carrying RFC 2833 payload. <i>plaintext</i> : Relay DTMF signals as plain text.	C	13
<code>fax <t38 g711></code>	Sets whether to send fax signals by ITU-T T38 using UDP format or through RTP packets according to ITU-T G.711.	C	13
<code>firstdigit <fdt></code>	Sets the first digit timeout. This is the number of seconds a person has to dial the first digit after taking the phone off-hook. <i>fdt</i> : First digit timeout, 1-255 seconds.	C	13

Table 283 VoIP SIP Commands (SIP Firmware Only) (continued)

COMMAND	DESCRIPTION	M	P
flash <invite rfc2833 rfc2833like sipinfo1 sipinfo2 sipinfo3 sipinfo4 sipinfo5 [<rc>] sipinfo6 [<info>]>	Configures how the system processes the signal when a user presses the flash button on the phone. invite: Relay flash by SIP INVITE signal. rfc2833: Relay flash by RTP packet whose payload type is specific and adjusted according to the negotiated SDP. rfc2833like: Relay flash in SIP INFO packets, but carried as RFC 2833 payload sipinfo1: Relay flash by SIP INFO signal = 16 message. sipinfo2: Relay flash by SIP INFO signal = hf message. sipinfo3: Relay flash by SIP INFO signal = hook-flash message. sipinfo4: Relay flash by SIP INFO plain text "FLASH" message. sipinfo5: Relay flash by multiple SIP INFO signal messages and the content of the signal messages is determined by the replace characters <rc> you specify, example *#, <rc>: replace characters, up to 7 characters. A separate SIP INFO message is sent for each character you enter. sipinfo6: Relay flash by SIP INFO packets where the content of the message is determined by the text you enter. For example "event flashhook", <info>: specified information, 1-31 printable characters.	C	13
key-pattern <pattern table>	Specifies the VoIP key-pattern table the call service profile uses. pattern table: Name of the VoIP key-pattern table, up to 31 characters.	C	13
localcall <on off>	Sets whether or not to allow subscribers to call other subscribers if the system's connection to the SIP server is not available.	C	13
localhelp <on off>	Enables or disables the emergency call feature.	C	13
localhelpindex <index> tel <tel number> name <name>	Configures an index of emergency call settings. index: The entry index 1-8. tel number: The local help telephone number, up to 15 characters, only digit characters are allowed name: The local help table name, 1-31 printable characters.	C	13
mwi <on off>	Enables or disables MWI (Message Waiting Indication).	C	13
dialplan <on <cc> <ndc> <dialplan- table> off>	Configures the dialplan feature. cc: E.164 Country Code, up to 7 characters. ndc: E.164 National Destination Code, up to 7 characters. dialplan-table: Dial plan table name.	C	13
password < none <password>>	Sets the password for authorization of SIP messages.	C	13
reanswer <time>	When the system is using v5sip mode, this field sets the reanswer time period. The reanswer time controls the length of time between the user hanging up the phone, and the call being disconnected (the BYE request being sent). time: 0-30 seconds.	C	13
conference <on off>	Enables or disables the conference call feature.	C	13

Table 283 VoIP SIP Commands (SIP Firmware Only) (continued)

COMMAND	DESCRIPTION	M	P
<code>callsvcmode <europe usa></code>	Sets supplementary phone services to European (europe) or North American (usa) mode.	C	13
<code>onhooktransfer <on off></code>	Enables or disables call transfer when on-hook. This setting controls what happens when the initiator of a conference call hangs up. Turn this on to have the conference call continue without the initiator. Turn this off to have the conference call end when the initiator hangs up.	C	13
<code>conftransfer <on off></code>	Enables or disables call transfer while in a conference call. Turn this on to allow a subscriber to make a conference call and then transfer the call.	C	13
<code>firstdigit <fdt></code>	Sets the number of seconds (1-255) a person has to dial the first digit after taking the phone off-hook.	C	13
<code>interdigit <idt></code>	Sets the number of seconds (1-255) a person has between dialing digits.	C	13
<code>no localhelp index <index></code>	Removes the specified index of emergency call settings.	C	13
<code>no svc-profile <name></code>	Removes the specified SIP call service profile.	C	13
<code>cpt reorder <reorder time></code>	Configures the duration of the call progress re-order tone, also known as the congestion tone or fast busy tone. <i>reorder time</i> : 5-300 seconds.	C	13
<code>cpt howler <howler time></code>	Configures the duration of the call progress howler tone. This informs a customer that they left their receiver off-hook. <i>howler time</i> : 5-300 seconds.	C	13
<code>cpt reorder alerting <alerting time></code>	Configures the call progress alerting tone timeout. This is the ring signal to inform caller and callee that a phone call has been sent or has arrived. <i>alerting time</i> : 60-1200 seconds.	C	13
<code>no cpt reorder</code>	Restores the re-order tone duration to the system default value.	C	13
<code>no cpt howler</code>	Restores the howler tone duration to the system default value.	C	13
<code>no cpt alerting</code>	Restores the alerting tone duration to the system default value.	C	13

38.8 SIP Command Examples

These commands apply when using SIP firmware. This example shows how to let two ports make VoIP-SIP calls to each other.

- Provision slot 2 for VoIP.
- Inband IP address/subnet mask: 192.168.10.5/24
- The IP address/subnet mask, VLAN and priority for VoIP interface: 192.168.2.55/24, VLAN 2, priority 5
- Inband IP address/subnet mask: 192.168.1.5/24
- Enable VLAN 2 on all Gigabit Ethernet ports
- SIP server, registration server, and proxy server IP address: 192.168.2.241
- SIP, registration, and proxy port: 5060
- URI type: SIP

- Keep-alive: on, 3600 second timeout
- DSCP value for SIP and RTP packets: 23
- RTP start and end ports for RTP packets: 50000, 60000
- DSP profile: ims-dsp
- SIP call service profile: ims-svc
- VoIP port 1 SIP password 1234, account 11101, name 11101, and telephone number 11101
- VoIP port 2 SIP password 1234, account 11102, name 11102, and telephone number 11102

Finally, activate VoIP on the ports and then the ports can make SIP calls to each other.

```
ras# config
ras(config)# lc slot 2 provision vop
ras(config)# ip inband address 192.168.10.5/24
ras(config)# voip ip address 192.168.2.55/24 vlan 2 pbit 5
ras(config)# ip inband address 192.168.1.5/24
ras(config)# interface ge-nni *
ras(config-interface-ge-nni-*)# vlan 2
ras(config-interface-ge-nni-*)# exit
ras(config)# voip sip
ras(config-voip-sip)# sip-profile ims-sip
ras(config-voip-sip-sip-profile-ims-sip)# sip-server 192.168.2.241
ras(config-voip-sip-sip-profile-ims-sip)# sip-port 5060
ras(config-voip-sip-sip-profile-ims-sip)# reg-server 192.168.2.241
ras(config-voip-sip-sip-profile-ims-sip)# reg-port 5060
ras(config-voip-sip-sip-profile-ims-sip)# proxy-server 192.168.2.241
ras(config-voip-sip-sip-profile-ims-sip)# proxy-port 5060
ras(config-voip-sip-sip-profile-ims-sip)# uri-type sip
ras(config-voip-sip-sip-profile-ims-sip)# keep-alive on 3600
ras(config-voip-sip-sip-profile-ims-sip)# dscp 23
ras(config-voip-sip-sip-profile-ims-sip)# rtp-port start-port 50000 end-port 60000
ras(config-voip-sip-sip-profile-ims-sip)# exit
ras(config-voip-sip)# exit
ras(config)# voip dsp-profile ims-dsp
ras(config-voip-dsp-profile-ims-dsp)# exit
ras(config)# voip sip
ras(config-voip-sip)# svc-profile ims-svc
ras(config-voip-sip-svc-profile-ims-svc)# exit
ras(config-voip-sip)# exit
ras(config)# interface voip 2/1
ras(config-interface-voip-2/1)# no active
ras(config-interface-voip-2/1)# dsp-profile ims-dsp
ras(config-interface-voip-2/1)# sip sip-profile ims-sip
ras(config-interface-voip-2/1)# sip svc-profile ims-svc
ras(config-interface-voip-2/1)# active
ras(config-interface-voip-2/1)# sip password 1234
ras(config-interface-voip-2/1)# sip account 11101
ras(config-interface-voip-2/1)# sip name 11101
ras(config-interface-voip-2/1)# sip tel-number 11101
ras(config-interface-voip-2/1)# exit
ras(config)# interface voip 2/2
ras(config-interface-voip-2/2)# no active
ras(config-interface-voip-2/2)# dsp-profile ims-dsp
ras(config-interface-voip-2/2)# sip sip-profile ims-sip
ras(config-interface-voip-2/2)# sip svc-profile ims-svc
ras(config-interface-voip-2/2)# active
ras(config-interface-voip-2/2)# sip password 1234
ras(config-interface-voip-2/2)# sip account 11102
ras(config-interface-voip-2/2)# sip name 11102
ras(config-interface-voip-2/2)# sip tel-number 11102
ras(config-interface-voip-2/2)# exit
ras(config)# exit
```


CHAPTER 39

IEEE 802.1x Authentication

Use these commands to configure IEEE 802.1x authentication for authenticating subscribers.

IEEE 802.1x is an extended authentication protocol that allows support of RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile management on a network RADIUS server.

39.1 802.1x Command Summary

The following table describes commonly used parameter notation for these commands.

Table 284 dot1x Command Parameters

NOTATION	DESCRIPTION
<i>info</i>	The option 82 circuit ID format. It can use the following components: special characters except % => ~`!@#\$%^&*()-=_+{}<>?,./ %%: equals character % %0x00-%0xFF: represents byte value %pname: configured port name %pid: port index %chvpi: channel VPI %chvci: channel VCI %chid: channel ID, UNI VLAN for Ethernet, VPI.VCI for ATM %slotid: slot index of the logic port %svlan: SVLAN ID which a DHCP client runs on %cvlan: CVLAN ID which a DHCP client runs on %hname: host device name %cmac1: MAC address of a DHCP client in XX:XX:XX:XX:XX:XX format where X=0-F %cmac2: MAC address of a DHCP client in XXXXXXXXXXXX format where X=0-F %cmac3: MAC address of a DHCP client in Bytes %dmac1: MAC address of the host device in XX:XX:XX:XX:XX:XX format where X=0-F %dmac2: MAC address of the host device in XXXXXXXXXXXX format where X=0-F %dmac3: MAC address of the host device in Bytes %phtype: ATM: atm, Ethernet: eth %hmodel: model name of the host device %fwid: host device firmware ID %blank: blank character

The following section lists the commands for this feature.

Table 285 dot1x command summary

COMMAND	DESCRIPTION	M	P
<code>dot1x active</code>	Enables IEEE 802.1x authentication.	C	13
<code>show dot1x</code>	Displays IEEE 802.1x authentication settings.	E	3
<code>no dot1x active</code>	Disables IEEE 802.1x authentication.	C	13
<code>dot1x server radius index <1-16></code>	Configures an entry for RADIUS authentication server settings.	C	13
<code>address <ip-address></code>	Configures the authentication server's IP address.	C	13
<code>port <1-65535></code>	Configures the authentication server's port for 802.1x authentication.	C	13

Table 285 dot1x command summary (continued)

COMMAND	DESCRIPTION	M	P
<code>secret <string></code>	Configures a secret password shared with the RADIUS server. <i>string</i> : 1~31 printable characters	C	13
<code>no dot1x server radius index <1-16></code>	Clears the specified entry from the RADIUS authentication server settings.	C	13
<code>show dot1x server radius</code>	Displays all RADIUS authentication server settings.	E	3
<code>interface dsl <slot/portlist></code>	Enters the sub-command mode for configuring the specified DSL ports.	C	13
<code>dot1x active</code>	Enables IEEE 802.1x port authentication.	C	13
<code>dot1x control <auto auth unauth></code>	Configures the IEEE 802.1x port authentication option. auto: authenticate all subscribers before they can access the network through the ports. auth: allow all connected users to access the network through the ports without authentication. unauth: deny all subscribers access to the network through the ports.	C	13
<code>dot1x server radius index <index></code>	Specifies a RADIUS server used for the port authentication. You have to configure the RADIUS server using the <code>dot1x server radius index</code> command before using this command.	C	13
<code>dot1x auth-once</code>	Stops user re-authentication for the ports. The subscribers will not need to periodically re-enter their usernames and passwords to stay connected to the port.	C	13
<code>dot1x period <60-65535></code>	Configures how often in seconds a client has to re-enter his or her username and password to stay connected to the ports.	C	13
<code>dot1x circuit-id option-info <info></code>	Sets the DHCP option 82 Circuit ID format. Note: Make sure your RADIUS authentication server is option-82 capable before using this command.	C	13
<code>no dot1x active</code>	Disables IEEE 802.1x port authentication.	C	13
<code>no dot1x control</code>	Resets the IEEE 802.1x port authentication option setting to the default.	C	13
<code>no dot1x auth-once</code>	Enables user re-authentication for the ports. The subscribers have to periodically re-enter their usernames and passwords to stay connected to the ports.	C	13
<code>no dot1x period</code>	Resets the IEEE 802.1x re-authentication period to the default.	C	13
<code>no dot1x circuit-id</code>	Disables the DHCP option 82 on the ports.	C	13
<code>interface fe <slot/portlist></code>	Enters the sub-command mode for configuring the specified FE ports.	C	13
<code>dot1x active</code>	Enables IEEE 802.1x port authentication.	C	13
<code>dot1x control <auto auth unauth></code>	Configures the IEEE 802.1x port authentication option. auto: authenticate all subscribers before they can access the network through the ports. auth: allow all connected users to access the network through the ports without authentication. unauth: deny all subscribers access to the network through the ports.	C	13
<code>dot1x server radius index <index></code>	Specifies a RADIUS server used for the port authentication. You have to configure the RADIUS server using the <code>dot1x server radius index</code> command before using this command.	C	13

Table 285 dot1x command summary (continued)

COMMAND	DESCRIPTION	M	P
<code>dot1x auth-once</code>	Stops user re-authentication for the ports. The subscribers will not need to periodically re-enter their usernames and passwords to stay connected to the port.	C	13
<code>dot1x period <60-65535></code>	Configures how often in seconds a client has to re-enter his or her username and password to stay connected to the ports.	C	13
<code>dot1x circuit-id option-info <info></code>	Sets the DHCP option 82 Circuit ID format. Note: Make sure your RADIUS authentication server is option-82 capable before using this command.	C	13
<code>no dot1x active</code>	Disables IEEE 802.1x port authentication.	C	13
<code>no dot1x control</code>	Resets the IEEE 802.1x port authentication option setting to the default.	C	13
<code>no dot1x auth-once</code>	Enables user re-authentication for the ports. The subscribers have to periodically re-enter their usernames and passwords to stay connected to the ports.	C	13
<code>no dot1x period</code>	Resets the IEEE 802.1x re-authentication period to the default.	C	13
<code>no dot1x circuit-id</code>	Disables the DHCP option 82 on the ports.	C	13
<code>dot1x userprofile name <name> password <password></code>	Configures an IEEE 802.1x user account for local authentication. <i>name</i> : up to 31 printable characters. <i>password</i> : up to 31 printable characters.	C	13
<code>no dot1x userprofile name <name></code>	Deletes the specified IEEE 802.1x user account. <i>name</i> : up to 31 printable characters.	C	13
<code>show dot1x userprofile</code>	Displays all IEEE 802.1x user accounts.	E	3
<code>dot1x authentication <userprofile radius></code>	Configures the IEEE 802.1x port authentication method. <i>userprofile</i> : use the local database to authenticate users <i>radius</i> : use the remote RADIUS server to authenticate users	C	13
<code>show interface dsl <slot/portlist> dot1x status</code>	Displays the IEEE 802.1x port authentication settings for the specified ports.	E	3
<code>show interface dsl <slot/portlist> dot1x statistic</code>	Displays the IEEE 802.1x port authentication statistics for the specified ports.	E	3
<code>show interface fe <slot/portlist> dot1x status</code>	Displays the IEEE 802.1x port authentication settings for the specified ports.	E	3
<code>show interface fe <slot/portlist> dot1x statistic</code>	Displays the IEEE 802.1x port authentication statistics for the specified ports.	E	3

39.1.1 Command Examples

This example shows how to enable IEEE 802.1x authentication on subscriber ports 1 to 10 and use the RADIUS server set in entry 2 for port authentication. Then it sets the 802.1x authentication option to `auto` and re-authentication time interval to 28800 seconds (=8 hours). Finally, it displays the 802.1x authentication settings and statistics.

```

sysname# config
sysname(config)# interface dsl 2/1-2/10
sysname(config-interface-dsl-2/1-2/10)# dot1x active
sysname(config-interface-dsl-2/1-2/10)# dot1x server radius index 2
sysname(config-interface-dsl-2/1-2/10)# dot1x control auto
sysname(config-interface-dsl-2/1-2/10)# dot1x period 28800
sysname(config-interface-dsl-2/1-2/10)# exit
sysname(config)# exit
sysname# show interface dsl 2/1-2/10 dot1x status
port status control          radius index auth once reauth period
circuit-id option-info
-----
  1  V    auto                2    -                28800
  2  V    auto                2    -                28800
  3  V    auto                2    -                28800
  4  V    auto                2    -                28800
  5  V    auto                2    -                28800
  6  V    to                  2    -                28800
  7  V    auto                2    -                28800
  8  V    auto                2    -                28800
  9  V    auto                2    -                28800
 10  V    auto                2    -                28800

sysname# show interface dsl 2/1-2/10 dot1x statistic
port status control          reauth reauth period authorized reauth count
-----
  1  V    auto                V          28800      X                2
  2  V    auto                V          28800      X                2
  3  V    auto                V          28800      X                2
  4  V    auto                V          28800      X                2
  5  V    auto                V          28800      X                2
  6  V    auto                V          28800      X                2
  7  V    auto                V          28800      X                2
  8  V    auto                V          28800      X                2
  9  V    auto                V          28800      X                2
 10  V    auto                V          28800      X                2
sysname#

```

This example shows how to create two IEEE 802.1x user accounts and set the IES to use the local database for subscriber user authentication.

```
sysname# config
sysname(config)# dot1x userprofile name user password 0000
sysname(config)# dot1x userprofile name manager password 0000
sysname(config)# dot1x authentication userprofile
sysname(config)# exit
sysname# show dot1x userprofile
User profile list:
```

No.	Name	Password
1	manager	0000
2	user	0000

PART IV

Troubleshooting, Appendices, and Index

CHAPTER 40

Troubleshooting

This chapter explains how to troubleshoot the system hardware.

40.1 LEDs

See [Chapter 1 on page 20](#) for LED descriptions.

40.2 Power, Hardware Connection, and LED Problems

The management card's **ALM** LED is on.

The IES has detected a critical alarm. This could be an alarm on the IES itself or an alarm triggered by an external sensor connected to the **COM** terminals. Examples of a critical alarm are when the voltage or temperature is outside of the normal range.

Check the logs to see the cause of the alarm. Take appropriate measures to remove the cause of the alarm. For example, you may need to change the fan module if the fans are not operating normally (see [Section 4.1 on page 58](#) for directions).

One of the management card's Gigabit Ethernet interface's LEDs is not on.

- 1 Make sure the interface is enabled.
- 2 Make sure that the interface's speed and duplex settings match those on the port on the peer Ethernet device.
- 3 Check the fiber optic Ethernet cable and connections between the SFP module and the peer Ethernet device.
- 4 If the interface is an SFP slot, check the transceiver.
- 5 Make sure that the peer Ethernet device is functioning properly.
- 6 If the Ethernet cable and peer Ethernet device are both OK and the LEDs stay off, there may be a problem with the interface. Contact the distributor.

A SFP slot's **LNK** LED turns on and off intermittently.

- 1 Check the fiber optic Ethernet cable and connections between the SFP module and the peer Ethernet device.
- 2 Make sure that the peer Ethernet device is functioning properly.
- 3 If the Ethernet cable and peer Ethernet device are both OK and the **LNK** LED keeps turning off and on, there may be a problem with the port. Contact the distributor.

40.3 Voice Problems

40.3.1 No Voice on an ADSL Connection

The ADSL line cards allow the telephone wiring used for DSL connections to also simultaneously carry normal voice conversations.

Table 286 Voice troubleshooting

STEP	CORRECTIVE ACTION
1	Make sure the subscriber has a POTS splitter properly installed.
2	Check the telephone wire connections between the subscriber and the MDF(s).
3	Check the telephone wire and connections between the MDF(s) and USER port(s). Refer to the pin assignments in the line card User's Guide.
4	Check the telephone wire and connections between the MDF(s) and the CO port(s). Check the telephone wire mapping on the MDF(s).
5	Check the connection from the MDF(s) to the PBX or the telephone company PSTN or ISDN switch.
6	Make sure the in-house wiring works and is connected properly.
7	Repeat the steps above using a different DSL port.

40.3.2 No Voice on a VoIP Connection

Check the POTS and line card connections between the subscriber, the MDF(s) and the POTS line card.

40.3.3 Testing Wiring

Systematically test wiring using a functioning telephone to determine if there is a wiring problem. If the connection is good, the telephone will return a dial tone.

APPENDIX A

Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a Zyxel office for the region in which you bought the device.

See <http://www.zyxel.com/homepage.shtml> and also http://www.zyxel.com/about_zyxel/zyxel_worldwide.shtml for the latest information.

Please have the following information ready when you contact an office.

Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

Corporate Headquarters (Worldwide)

Taiwan

- Zyxel Communications Corporation
- <http://www.zyxel.com>

Asia

China

- Zyxel Communications (Shanghai) Corp.
- Zyxel Communications (Beijing) Corp.
- Zyxel Communications (Tianjin) Corp.
- <http://www.zyxel.cn>

India

- Zyxel Technology India Pvt Ltd
- <http://www.zyxel.in>

Kazakhstan

- Zyxel Kazakhstan
- <http://www.zyxel.kz>

Korea

- Zyxel Korea Corp.
- <http://www.zyxel.kr>

Malaysia

- Zyxel Malaysia Sdn Bhd.
- <http://www.zyxel.com.my>

Pakistan

- Zyxel Pakistan (Pvt.) Ltd.
- <http://www.zyxel.com.pk>

Philippines

- Zyxel Philippines
- <http://www.zyxel.com.ph>

Singapore

- Zyxel Singapore Pte Ltd.
- <http://www.zyxel.com.sg>

Taiwan

- Zyxel Communications Corporation
- <http://www.zyxel.com/tw/zh/>

Thailand

- Zyxel Thailand Co., Ltd
- <http://www.zyxel.co.th>

Vietnam

- Zyxel Communications Corporation-Vietnam Office
- <http://www.zyxel.com/vn/vi>

Europe

Austria

- Zyxel Deutschland GmbH
- <http://www.zyxel.de>

Belarus

- Zyxel BY
- <http://www.zyxel.by>

Belgium

- Zyxel Communications B.V.
- <http://www.zyxel.com/be/nl/>
- <http://www.zyxel.com/be/fr/>

Bulgaria

- Zyxel България
- <http://www.zyxel.com/bg/bg/>

Czech Republic

- Zyxel Communications Czech s.r.o
- <http://www.zyxel.cz>

Denmark

- Zyxel Communications A/S
- <http://www.zyxel.dk>

Estonia

- Zyxel Estonia
- <http://www.zyxel.com/ee/et/>

Finland

- Zyxel Communications
- <http://www.zyxel.fi>

France

- Zyxel France
- <http://www.zyxel.fr>

Germany

- Zyxel Deutschland GmbH
- <http://www.zyxel.de>

Hungary

- Zyxel Hungary & SEE
- <http://www.zyxel.hu>

Italy

- Zyxel Communications Italy
- <http://www.zyxel.it/>

Latvia

- Zyxel Latvia
- <http://www.zyxel.com/lv/lv/homepage.shtml>

Lithuania

- Zyxel Lithuania
- <http://www.zyxel.com/lt/lt/homepage.shtml>

Netherlands

- Zyxel Benelux
- <http://www.zyxel.nl>

Norway

- Zyxel Communications
- <http://www.zyxel.no>

Poland

- Zyxel Communications Poland
- <http://www.zyxel.pl>

Romania

- Zyxel Romania
- <http://www.zyxel.com/ro/ro>

Russia

- Zyxel Russia
- <http://www.zyxel.ru>

Slovakia

- Zyxel Communications Czech s.r.o. organizacna zlozka
- <http://www.zyxel.sk>

Spain

- Zyxel Communications ES Ltd
- <http://www.zyxel.es>

Sweden

- Zyxel Communications
- <http://www.zyxel.se>

Switzerland

- Studerus AG

- <http://www.zyxel.ch/>

Turkey

- Zyxel Turkey A.S.
- <http://www.zyxel.com.tr>

UK

- Zyxel Communications UK Ltd.
- <http://www.zyxel.co.uk>

Ukraine

- Zyxel Ukraine
- <http://www.ua.zyxel.com>

Latin America

Argentina

- Zyxel Communication Corporation
- <http://www.zyxel.com/ec/es/>

Brazil

- Zyxel Communications Brasil Ltda.
- <https://www.zyxel.com/br/pt/>

Ecuador

- Zyxel Communication Corporation
- <http://www.zyxel.com/ec/es/>

Middle East

Israel

- Zyxel Communication Corporation
- <http://il.zyxel.com/homepage.shtml>

Middle East

- Zyxel Communication Corporation
- <http://www.zyxel.com/me/en/>

North America

USA

- Zyxel Communications, Inc. - North America Headquarters
- <http://www.zyxel.com/us/en/>

Oceania

Australia

- Zyxel Communications Corporation
- <http://www.zyxel.com/au/en/>

Africa

South Africa

- Nology (Pty) Ltd.
- <http://www.zyxel.co.za>

APPENDIX B

Legal Information

Copyright

Copyright © 2020 by Zyxel Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of Zyxel Communications Corporation.

Published by Zyxel Communications Corporation. All rights reserved.

Disclaimer

Zyxel does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. Zyxel further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Regulatory Notice and Statement

UNITED STATES of AMERICA



The following information applies if you use the product within USA area

FCC EMC Statement

- This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:
 - (1) This device may not cause harmful interference, and
 - (2) This device must accept any interference received, including interference that may cause undesired operation.
- Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
- This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense

CANADA

The following information applies if you use the product within Canada area

Industry Canada ICES statement

CAN ICES-3 (A)/NMB-3(A)

EUROPEAN UNION



The following information applies if you use the product within the European Union.

CE EMC statement

WARNING: This equipment is compliant with Class A of EN55032. In a residential environment this equipment may cause radio interference.

List of National Codes

COUNTRY	ISO 3166 2 LETTER CODE	COUNTRY	ISO 3166 2 LETTER CODE
Austria	AT	Liechtenstein	LI
Belgium	BE	Lithuania	LT
Bulgaria	BG	Luxembourg	LU
Croatia	HR	Malta	MT
Cyprus	CY	Netherlands	NL
Czech Republic	CR	Norway	NO
Denmark	DK	Poland	PL
Estonia	EE	Portugal	PT
Finland	FI	Romania	RO
France	FR	Serbia	RS
Germany	DE	Slovakia	SK
Greece	GR	Slovenia	SI
Hungary	HU	Spain	ES
Iceland	IS	Sweden	SE
Ireland	IE	Switzerland	CH
Italy	IT	Turkey	TR
Latvia	LV	United Kingdom	GB

Safety Warnings

For your safety, be sure to read and follow all warning notices and instructions.

For your safety, be sure to read and follow all warning notices and instructions.

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT stack other devices or equipment on the device.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- ONLY qualified service personnel should service or disassemble this device.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY a power wire of the appropriate wire gauge (see [Table 18 on page 33](#) for details) for your device. Connect it to a power supply of the correct voltage (see [Table 18 on page 33](#) for details).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.

- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Keep the air filters clean, in order to ensure sufficient airflow.
- Fuse Warning! Replace a fuse only with a fuse of the same type and rating.
- This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.
- Connect the frame ground before you connect any other cables or wiring and disconnect all cables or wiring before disconnecting the frame ground.
- Earthing connection has to be installed by service personnel.
- The length of exposed (bare) power wire should not exceed 12 mm.

IMPORTANT SAFETY INSTRUCTIONS

- 1 Warning! Energy Hazard. Remove all metal jewelry, watches, and so on from your hands and wrists before serving this device.
 - 2 Warning! To avoid risk of electric shock, remove only one card at a time and do not place fingers or objects inside the chassis. Cover empty slots with slot covers.
 - 3 Warning! Use the fan module handles when pulling out or pushing in the fan module. Be careful not to put fingers or objects inside the fan module.
 - 4 Caution! The RJ-45 jacks are not used for telephone line connection.
 - 5 Caution! To reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cord.
 - 6 Caution: Use a UL listed or CSA Certified DC power source to connect to DC PSU.
 - 7  Hazardous Moving Parts. Keep body parts away from fan blades.
 - 8  Hot Surface. Do not touch.
-
- 1 Avertissement : Risque de choc électrique. Retirer tout bijoux en métal et votre montre de vos mains et poignets avant de manipuler cet appareil
 - 2 Avertissement : Pour éviter tout risque de choc électrique ne retirer qu'une carte à la fois et ne pas insérer vos doigts ou tout objet sous le châssis. Recouvrir les ouvertures avec les caches adaptés.
 - 3 Avertissement : Utiliser les poignées du châssis pour retirer ou insérer le module de ventilation Faites attention à vos doigts et à tout objet quand vous manipulez le ventilateur
 - 4 Attention : Les câbles RJ-45 ne doivent pas être utilisés pour les connexions téléphoniques.
 - 5 ATTENTION – Pour réduire les risques d'incendie, utiliser uniquement des conducteurs de télécommunications 26 AWG au de section supérieure.
 - 6 Attention: Utilisez une source d'alimentation CC répertoriée UL ou certifiée CSA pour la connexion au bloc d'alimentation CC.

- 7  Mobilité des pièces détachées. S'assurer que les pièces détachées ne sont pas en contact avec les pales du ventilateur.
- 8  Surface brûlante. Ne pas toucher.

Environment Statment

European Union - Disposal and Recycling Information

The symbol below means that according to local regulations your product and/or its battery shall be disposed of separately from domestic waste. If this product is end of life, take it to a recycling station designated by local authorities. At the time of disposal, the separate collection of your product and/or its battery will help save natural resources and ensure that the environment is sustainable development.

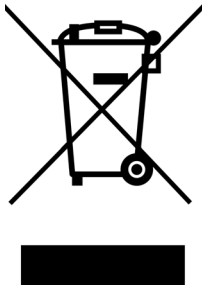
Die folgende Symbol bedeutet, dass Ihr Produkt und/oder seine Batterie gemäß den örtlichen Bestimmungen getrennt vom Hausmüll entsorgt werden muss. Wenden Sie sich an eine Recyclingstation, wenn dieses Produkt das Ende seiner Lebensdauer erreicht hat. Zum Zeitpunkt der Entsorgung wird die getrennte Sammlung von Produkt und/oder seiner Batterie dazu beitragen, natürliche Ressourcen zu sparen und die Umwelt und die menschliche Gesundheit zu schützen.

El símbolo de abajo indica que según las regulaciones locales, su producto y/o su batería deberán depositarse como basura separada de la doméstica. Cuando este producto alcance el final de su vida útil, llévelo a un punto limpio. Cuando llegue el momento de desechar el producto, la recogida por separado éste y/o su batería ayudará a salvar los recursos naturales y a proteger la salud humana y medioambiental.

Le symbole ci-dessous signifie que selon les réglementations locales votre produit et/ou sa batterie doivent être éliminés séparément des ordures ménagères. Lorsque ce produit atteint sa fin de vie, amenez-le à un centre de recyclage. Au moment de la mise au rebut, la collecte séparée de votre produit et/ou de sa batterie aidera à économiser les ressources naturelles et protéger l'environnement et la santé humaine.

Il simbolo sotto significa che secondo i regolamenti locali il vostro prodotto e/o batteria deve essere smaltito separatamente dai rifiuti domestici. Quando questo prodotto raggiunge la fine della vita di servizio portarlo a una stazione di riciclaggio. Al momento dello smaltimento, la raccolta separata del vostro prodotto e/o della sua batteria aiuta a risparmiare risorse naturali e a proteggere l'ambiente e la salute umana.

Symbolen innebär att enligt lokal lagstiftning ska produkten och/eller dess batteri kastas separat från hushållsavfallet. När den här produkten når slutet av sin livslängd ska du ta den till en återvinningsstation. Vid tiden för kasseringen bidrar du till en bättre miljö och mänsklig hälsa genom att göra dig av med den på ett återvinningsställe.



台灣

以下訊息僅適用於產品銷售至台灣地區

第十二條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。

前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

警告使用者

- 這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

安全警告

為了您的安全，請先閱讀以下警告及指示：

- 請勿將此產品接近水、火焰或放置在高溫的環境。

- 避免設備接觸
任何液體 - 切勿讓設備接觸水、雨水、高濕度、污水腐蝕性的液體或其他水份。
灰塵及污物 - 切勿接觸灰塵、污物、沙土、食物或其他不合適的材料。
- 雷雨天氣時，不要安裝，使用或維修此設備。有遭受電擊的風險。
- 切勿重摔或撞擊設備，並勿使用不正確的電源變壓器。
- 若接上不正確的電源變壓器會有爆炸的風險。。
- 請勿隨意更換產品內的電池。
- 如果更換不正確之電池型式，會有爆炸的風險，請依製造商說明書處理使用過之電池。
- 請將廢電池丟棄在適當的電器或電子設備回收處。
- 請勿將設備解體。
- 請勿阻礙設備的散熱孔，空氣對流不足將會造成設備損害。
- 請插在正確的電壓供給插座（如：北美 / 台灣電壓 110V AC，歐洲是 230V AC）。
- 假若電源變壓器或電源變壓器的纜線損壞，請從插座拔除，若您還繼續插電使用，會有觸電死亡的風險。
- 請勿試圖修理電源變壓器或電源變壓器的纜線，若有毀損，請直接聯絡您購買的店家，購買一個新的電源變壓器。
- 請勿將此設備安裝於室外，此設備僅適合放置於室內。
- 請勿隨一般垃圾丟棄。
- 請參閱產品背貼上的設備額定功率。
- 請參考產品型錄或是彩盒上的作業溫度。
- 設備必須接地，接地導線不允許被破壞或沒有適當安裝接地導線，如果不確定接地方式是否符合要求可聯繫相應的電氣檢驗機構檢驗。
- 如果您提供的系統中有提供熱插拔電源，連接或斷開電源請遵循以下指導原則
 - 先連接電源線至設備連，再連接電源。
 - 先斷開電源再拔除連接至設備的電源線。
 - 如果系統有多個電源，需拔除所有連接至電源的電源線再關閉設備電源。
- 產品沒有斷電裝置或者採用電源線的插頭視為斷電裝置的一部分，以下警語將適用：
 - 對永久連接之設備，在設備外部須安裝可觸及之斷電裝置；
 - 對插接式之設備，插座必須接近安裝之地點而且是易於觸及的。

FCC 聲明與警告

FCC 干擾聲明

本交換器符合 FCC 法規第 15 部分的規定，操作時必須符合下列兩項條件：

- 1 本交換器不得造成有害的干擾。
- 2 本交換器必須接受所接收到的干擾，包括可能導致作業異常的干擾。

FCC 警告

本裝置已經測試證明符合 FCC 法規第 15 部分有關甲類數位交換器的限制；這些限制是為合理防止本裝置在商業環境中使用時產生有害干擾。本設備會產生、運用及發射射頻能量，若不根據本使用手冊指示進行安裝及使用，將可能造成干擾，影響無線電通訊的正常作業。在住宅區操作本設備可能造成前述干擾，改善此種狀況所需的費用必須由使用者自行負擔。

CE 標誌警告：

此為甲類產品。在居住環境中使用，本產品可能產生無線電干擾，使用者必須採取適當措施因應。

台灣 BSMI (經濟部標準檢驗局) 甲類產品警告：

警告使用者

這是甲類的資訊產品，在居住的環境使用時，
可能造成射頻干擾，在這種情況下，
使用者會被要求採取某些適當的對策。

注意

除非本手冊另有規定，否則不得擅自變更或修改本裝置。若擅自進行此類變更或修改，您可能無法繼續對本設備進行任何操作。

廢棄及回收資訊

產品上廢棄回收標記，代表請勿將本產品及包裝配件或其內所附的電池視為一般家庭廢棄物處理，應交由當地合格回收處理廠進行回收或報廢處理。廢棄回收處理的行動亦能對自然資源與環境永續發展有所貢獻。



認證

前往 www.zyxel.com 觀看本產品相關的文件和認證

安全警告

為了您的安全，請務必詳讀並遵守以下警告告示和說明

- 請勿讓本裝置靠近有水的地方，例如潮濕的地下室或靠近游泳池的地方。
- 請勿將本裝置暴露在潮濕、灰塵、或腐蝕性液體中。
- 請勿在本裝置上放置其他物品。
- 請勿在雷雨期間安裝、使用、或維修本裝置。閃電可能會帶來電擊的危險。
- 只連接適當的配件到本裝置。
- 僅合格維修人員可維修或拆解本裝置。更多詳細資訊請連絡經銷商。
- 確認將纜線連接至正確的埠上。
- 小心置放連接的纜線，以防不經意踩踏或絆倒。
- 在維修或拆解本裝置之前，請記得拔下本裝置的所有連接纜線。
- 本裝置應只能使用符合電線標準尺寸的電源線 (請參閱第 79 頁的第 5 章)，並且只能連接到正確的電壓電源 (請參閱第 79 頁的第 5 章)。
- 請勿放置任何物品在電源轉接器或電源線上，亦請勿將產品放置在變壓器或電線可能被踩到的地方。
- 如果電源變壓器或電源線已損壞，請勿使用本產品，否則可能造成觸電。
- 如果電源變壓器或電源線已損壞，請自電源上移除並從產品上拔掉。
- 請勿自行嘗試修復電源變壓器或電源線，連絡您當地的供應商並購買新的變壓器或電源線。
- 請勿在室外使用本裝置，並確定所有的連接都在室內，以避免遭到閃電雷擊的危險。
- 請勿阻擋裝置的通風槽，氣流不足可能損壞裝置。
- 請保持空氣濾網清潔，以確保足夠的氣流。
- 保險絲警告！只能用相同類型與等級的保險絲做更換。
- 警告：此設備必須連接保護接地，絕對不要斷開接地導線或在沒有安裝適當的接地導線的情況下操作設備。如果您無法確定是否已適當接地，請與相關電力檢查機關或電工聯絡。
- 在連接其他電纜或電線之前，先連接保護接地；如需移除連接，請先移除電纜或電線，最後再移除保護接地。
- 保護接地的連接必須由服務人員親自安裝。
- 電源線的外露 (裸線) 長度不得超過 12 mm。

安全性指南

- 能量危險警告！操作本設備之前，請移除您身上的所有金屬首飾，手錶等。
- 警告！避免觸電，請一次只移除一張卡板，請勿將手指伸入或將其他物品置入機框內。沒有使用的插槽請將其插槽蓋蓋上。
- 風扇模組警告！當您在拉出或推入風扇模組時，請勿將手指或其他異物放入風扇模組內。
- 警告！請勿將乙太網路插口連接電話線。
- 警告！為了降低火災的風險，只能使用 26 號 AWG 或更大的電信線路
-  危險運轉零件，請遠離風扇葉片。
-  主機表面因運轉可能產生高溫，請勿觸碰。

Viewing Certifications

Go to <http://www.zyxel.com> to view this product's documentation and certifications.

Zyxel Limited Warranty

Zyxel warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized Zyxel local distributor for details about the Warranty Period of this product. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, Zyxel will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of Zyxel. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. Zyxel shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Trademarks

ZyNOS (Zyxel Network Operating System) and ZON (Zyxel One Network) are registered trademarks of Zyxel Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Open Source Licenses

This product contains in part some free software distributed under GPL license terms and/or GPL like licenses. Open source licenses are provided with the firmware package. You can download the latest firmware at www.zyxel.com. To obtain the source code covered under those Licenses, please contact support@zyxel.com.tw to get it.