

User's Guide

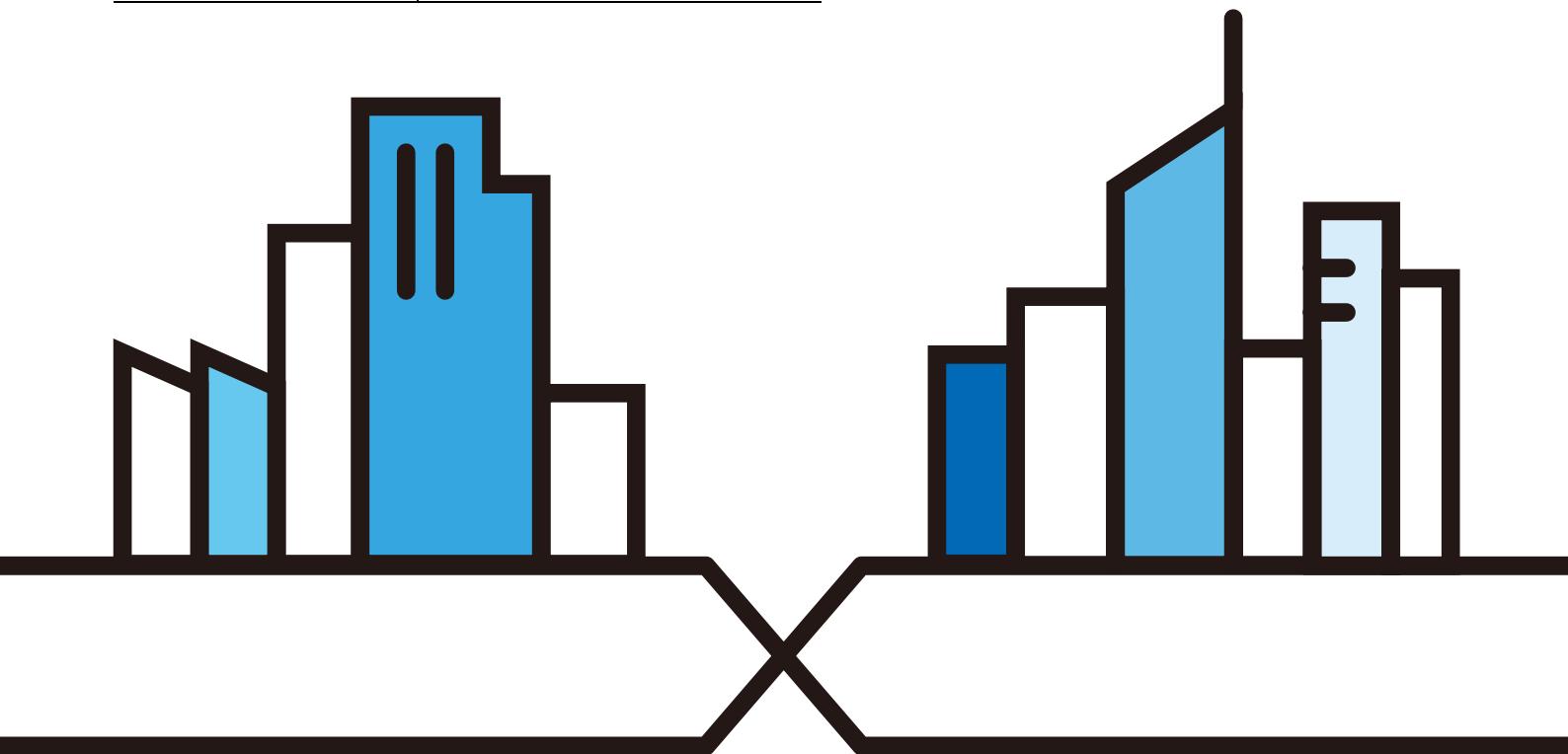
OLT1404/1408A

1U pizza box GPON OLT with 4/8 GPON ports

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 4.02 Ed. 1, 09/2018



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 OLT.



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 OLT1404A and OLT1408A may be referred to as the “OLT” in this guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Advanced Application** > **Spanning Tree Protocol** > **RSTP** means you first click **Advanced Application** in the navigation panel, then the **Spanning Tree Protocol** sub menu and finally the **RSTP** tab to get to that screen.

Icons Used in Figures

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

OLT 	Generic Switch 	Generic Router
Fiber Link 	Multi-Dwelling Unit (MDU) 	ONT
Smart TV 	Desktop 	Laptop

Document Conventions

Server	Headquarters	Branch Office
		
Home	Street Cabinet	
		

Contents Overview

Introduction and Hardware Installation	29
System Introduction	30
Hardware Installation	32
Hardware Panels	42
Web Configurator	50
The Web Configurator	51
Initial Setup Example	59
Tutorials	63
Status	79
Basic Setting	84
VLAN	95
Static MAC Forward Setup	109
Static Multicast Forwarding	111
Filtering	114
Spanning Tree Protocol	116
Bandwidth Control	131
Broadcast Storm Control	134
Mirroring	136
Link Aggregation	138
Port Security	146
Classifier	148
Policy Rule	155
Queuing Method	162
VLAN Stacking	165
Multicast	171
AAA	182
IP Source Guard	192
.....	213
Loop Guard	214
PPPoE	218
Error Disable	228
ONT VoIP	233
PON DDMI	243
File Transfer	249
ONT PM Counter	250
QoS Profile	251
OLT Registration	255

ONT Template	265
ONT Quick Setup	277
Static Route	285
DHCP	288
Maintenance	301
Access Control	308
Diagnostic	332
Syslog Setup	334
MAC Table	339
IP Table	342
ARP Table	344
Routing Table	346
Battery	347
CLI Commands	350
How to Access and Use the CLI	354
Privilege Level and Command Mode	357
Provisioning User Interfaces	364
Basic Settings	370
IPv6	381
VLAN	400
Static MAC Forwarding	411
Static Multicast Forwarding	413
AAA	417
TACACS+	421
Display Commands	423
Filtering	424
Spanning Tree Protocol	426
Bandwidth Control	438
MTU	440
Broadcast Storm Control	441
Port Mirroring	444
Link Aggregation	446
RADIUS	451
Port Security	453
Classifier	456
RMON	462
Policy Rule	466
Queuing Method	472
VLAN Stacking and Translation	475
Multicast	485
IP Source Guard	494
VoIP	505

Loop Guard	526
Static Route	531
DHCP	533
File Management	543
Access Control	546
Diagnostics	559
Syslog	563
MAC Address	565
ARP Table	568
Routing Table	570
Running Configuration	572
OLT Configuration	575
PON Port Status	579
Remote ONT	580
Port Protection Switching	606
WRED	608
PPPoE IA	609
Port Bridge	615
IP and MAC Anti-Spoofing	616
CPU Protection and DDoS	620
Error-Disable Recovery	623
Battery	625
Additional Commands	626
.....	627
Product Specifications	628

Table of Contents

Document Conventions	3
Contents Overview	5
Table of Contents	8
 Part I: Introduction and Hardware Installation 29	
Chapter 1	
System Introduction	30
1.1 System Description	30
Chapter 2	
Hardware Installation	32
2.1 General Installation Instructions	32
2.2 Rack Mounting	32
2.2.1 Installation Requirements	32
2.2.2 Precautions	32
2.2.3 Attaching the Mounting Brackets to the OLT	33
2.2.4 Mounting the OLT on a Rack	33
2.3 Connecting the OLT Frame Grounds	34
2.4 Connect the DC Power	34
2.5 Battery	37
2.5.1 Battery Charge	38
2.5.2 Battery Sensor Connection	39
2.6 Fan Module	40
2.6.1 Remove and Install the Fan Module	40
Chapter 3	
Hardware Panels	42
3.1 Front Panel	42
3.1.1 Gigabit Ethernet Ports	43
3.1.2 SFP/SFP+ Slots	43
3.1.3 GPON SFP Slots	46
3.1.4 Console Port	47
3.1.5 Management Port	47
3.1.6 ALARM Port	47
3.1.7 OLT Power Connections	48

3.2 LEDs	48
----------------	----

Part II: Web Configurator.....50

Chapter 4

The Web Configurator.....	51
---------------------------	----

4.1 Overview	51
4.2 System Login	51
4.3 The Status Screen	52
4.3.1 Change Your Password	55
4.4 Saving Your Configuration	56
4.5 Lockout	56
4.6 Resetting the OLT	57
4.6.1 Reload the Configuration File	57
4.7 Logging Out of the Web Configurator	57
4.8 Help	58

Chapter 5

Initial Setup Example	59
-----------------------------	----

5.1 Overview	59
5.1.1 Creating a VLAN	59
5.1.2 Setting Port VID	60
5.2 Configuring OLT Management IP Address	61

Chapter 6

Tutorials	63
-----------------	----

6.1 Overview	63
6.2 How to Use DHCPv4 Snooping on the OLT	63
6.3 How to Use DHCPv4 Relay on the OLT	67
6.3.1 DHCP Relay Tutorial Introduction	67
6.3.2 Creating a VLAN	68
6.3.3 Configuring DHCPv4 Relay	70
6.3.4 Troubleshooting	71
6.4 How to Use VLAN Stacking on PON Ports	71
6.4.1 Apply VLAN Stacking to All VLANs	71
6.4.2 Apply VLAN Stacking to Specific VLANs	72
6.5 How to Use VLAN Stacking on ONTs	73
6.5.1 Apply VLAN Stacking to All VLANs	73
6.5.2 Apply VLAN Stacking to Specific VLANs	74
6.6 How to Upgrade ONTs to the Latest Firmware via the OLT	75

Chapter 7	
Status	79
7.1 Overview	79
7.1.1 What You Can Do	79
7.2 Status	79
7.2.1 Port Details	80
Chapter 8	
Basic Setting	84
8.1 Overview	84
8.1.1 What You Can Do	84
8.2 System Information	84
8.3 General Setup	86
8.4 Introduction to VLANs	88
8.5 Switch Setup	88
8.6 IP Setup	90
8.7 Port Setup	92
Chapter 9	
VLAN.....	95
9.1 Overview	95
9.1.1 What You Can Do	95
9.1.2 What You Need to Know	95
9.2 VLAN Status	98
9.2.1 VLAN Details	98
9.3 Configure VLAN Port Settings	99
9.3.1 Subnet Based VLANs	102
9.3.2 Protocol Based VLANs	104
9.4 Configure a Static VLAN	106
Chapter 10	
Static MAC Forward Setup	109
10.1 Overview	109
10.1.1 What You Can Do	109
10.2 Configuring Static MAC Forwarding	109
Chapter 11	
Static Multicast Forwarding.....	111
11.1 Static Multicast Forward Setup Overview	111
11.1.1 What You Can Do	111
11.1.2 What You Need To Know	111
11.2 Configuring Static Multicast Forwarding	112

Chapter 12	
Filtering.....	114
12.1 Filtering Overview	114
12.1.1 What You Can Do	114
12.2 Configure a Filtering Rule	114
Chapter 13	
Spanning Tree Protocol	116
13.1 Spanning Tree Protocol Overview	116
13.1.1 What You Can Do	116
13.1.2 What You Need to Know	116
13.2 Spanning Tree Protocol Status Screen	118
13.3 Spanning Tree Configuration	119
13.4 Configure Rapid Spanning Tree Protocol	119
13.5 Rapid Spanning Tree Protocol Status	121
13.6 Configure Multiple Spanning Tree Protocol	122
13.6.1 Multiple Spanning Tree Protocol Port Configuration	125
13.7 Multiple Spanning Tree Protocol Status	127
13.8 Technical Reference	128
13.8.1 MSTP Network Example	128
13.8.2 MST Region	129
13.8.3 MST Instance	129
13.8.4 Common and Internal Spanning Tree (CIST)	130
Chapter 14	
Bandwidth Control	131
14.1 Bandwidth Control Overview	131
14.1.1 What You Can Do	131
14.2 Bandwidth Control Setup	131
Chapter 15	
Broadcast Storm Control	134
15.1 Broadcast Storm Control Overview	134
15.1.1 What You Can Do	134
15.2 Broadcast Storm Control Setup	134
Chapter 16	
Mirroring.....	136
16.1 Mirroring Overview	136
16.1.1 What You Can Do	136
16.2 Port Mirroring Setup	136

Chapter 17	
Link Aggregation	138
17.1 Link Aggregation Overview	138
17.1.1 What You Can Do	138
17.1.2 What You Need to Know	138
17.2 Link Aggregation Status	139
17.3 Link Aggregation Setting	140
17.3.1 Link Aggregation Control Protocol	142
17.4 Technical Reference	144
17.4.1 Static Trunking Example	144
Port Security.....	146
17.5 Port Security Overview	146
17.5.1 What You Can Do	146
17.6 Port Security Setup	146
Classifier.....	148
17.7 Classifier Overview	148
17.7.1 What You Can Do	148
17.7.2 What You Need to Know	148
17.8 Classifier	149
17.8.1 Viewing and Editing Classifier Configuration Summary	152
17.9 Classifier Example	153
Chapter 18	
Policy Rule	155
18.1 Policy Rules Overview	155
18.1.1 What You Need to Know	155
18.1.2 What You Can Do	156
18.2 Configuring Policy Rules	156
18.3 Policy Example	160
Chapter 19	
Queuing Method.....	162
19.1 Queuing Method Overview	162
19.1.1 What You Can Do	162
19.1.2 What You Need to Know	162
19.2 Configuring Queuing	163
Chapter 20	
VLAN Stacking.....	165
20.1 VLAN Stacking Overview	165
20.1.1 VLAN Stacking Example	165

Table of Contents

20.2 VLAN Stacking Port Roles	166
20.3 VLAN Tag Format	166
20.3.1 Frame Format	167
20.4 Configuring VLAN Stacking	167
20.4.1 Port-based Q-in-Q	169
Chapter 21	
Multicast.....	171
21.1 Multicast Overview	171
21.1.1 What You Can Do	171
21.1.2 What You Need to Know	171
21.2 Multicast Status	173
21.3 Multicast Setting	176
21.3.1 IGMP Snooping VLAN	178
21.3.2 Mcast Channel	180
Chapter 22	
AAA.....	182
22.1 AAA Overview	182
22.1.1 What You Can Do	182
22.1.2 What You Need to Know	182
22.2 AAA Screens	183
22.3 RADIUS Server Setup	183
22.4 TACACS+ Server Setup	185
22.5 AAA Setup	186
22.6 Technical Reference	189
22.6.1 Vendor Specific Attribute	189
22.6.2 Supported RADIUS Attributes	190
22.6.3 Attributes Used for Authentication	190
Chapter 23	
IP Source Guard.....	192
23.1 IP Source Guard Overview	192
23.1.1 What You Can Do	192
23.1.2 What You Need to Know	193
23.2 IP Source Guard Setup	193
23.3 IP Source Guard Static Binding	194
23.4 DHCP Snooping	195
23.5 DHCP Snooping Configure	198
23.5.1 DHCP Snooping Port Configure	200
23.5.2 DHCP Snooping VLAN Configure	201
23.6 ARP Inspection Status	202
23.7 ARP Inspection VLAN Status	203

Table of Contents

23.8 ARP Inspection Log Status	204
23.9 ARP Inspection Configure	205
23.9.1 ARP Inspection Port Configure	207
23.9.2 ARP Inspection VLAN Configure	208
23.10 Technical Reference	209
23.10.1 DHCP Snooping Overview	209
23.10.2 ARP Inspection Overview	211
	213

Chapter 24 Loop Guard	214
---------------------------------------	------------

24.1 Loop Guard Overview	214
24.1.1 What You Can Do	214
24.1.2 What You Need to Know	214
24.2 Loop Guard Setup	215

Chapter 25 PPPoE	218
----------------------------------	------------

25.1 PPPoE Intermediate Agent Overview	218
25.1.1 What You Can Do	218
25.1.2 What You Need to Know	218
25.2 PPPoE Screen	220
25.3 PPPoE Intermediate Agent	220
25.3.1 PPPoE IA Per-Port	222
25.3.2 PPPoE IA for VLAN	224
25.3.3 PPPoE IA for ONT PPPoE Option	225
25.3.4 PPPoE IA Statistic	226

Chapter 26 Error Disable	228
--	------------

26.1 Static Routing Overview	228
26.1.1 CPU Protection Overview	228
26.1.2 Error-Disable Recovery Overview	228
26.1.3 What You Can Do	228
26.2 Error Disable Screen	229
26.3 CPU Protection Configuration	229
26.4 Error-Disable Detect Configuration	231
26.5 Error-Disable Recovery Configuration	231

Chapter 27 ONT VoIP	233
-------------------------------------	------------

27.0.1 ONT VoIP Profile	233
27.0.2 What You Can Do	233

27.0.3 What You Need to Know	233
27.1 ONT VoIP Common Profile	234
27.2 ONT VoIP SIP Profile	237
27.3 ONT VoIP Dial Plan Profile	240
Chapter 28	
PON DDMI	243
28.1 Overview	243
28.1.1 What You Can Do	243
28.2 The PON DDMI Screen	243
28.2.1 ONT DDMI	245
28.3 ONT Alarm Profile	245
28.4 PON DDMI Setup	247
Chapter 29	
File Transfer	249
29.1 Overview	249
29.2 The File Transfer Screen	249
Chapter 30	
ONT PM Counter	250
30.1 Overview	250
30.2 The ONT PM Counter Screen	250
Chapter 31	
QoS Profile	251
31.1 ONT QoS	251
31.1.1 What You Can Do	251
31.2 ONT QoS Ingress Profile	251
31.3 ONT QoS Bandwidth Profile	252
31.4 ONT QoS Pbit Profile	253
Chapter 32	
OLT Registration	255
32.1 OLT Registration Overview	255
32.1.1 What You Can Do	255
32.1.2 What You Need to Know	255
32.2 The OLT Registration Screen	256
32.3 The Tca Configuration Screen	258
32.4 The ONT Summary Screen	260
32.5 The OLT Status Screen	261
32.6 The OLT Counter Screen	262
32.7 The Tca Status Screen	263

Chapter 33	
ONT Template.....	265
33.1 ONT Template Overview	265
33.1.1 What You Can Do	265
33.2 The ONT Template Screen	265
33.2.1 ONT Bandwidth Group	268
33.2.2 Uniport Queue	269
33.2.3 Uniport VLAN	271
33.2.4 Uniport Multicast	273
33.2.5 Uniport VoIP	275
Chapter 34	
ONT Quick Setup.....	277
34.1 Overview	277
34.1.1 What You Can Do	277
34.2 The ONT Quick Setup Screen	277
34.3 The ONT Status Screen	279
34.4 The ONT Alarm Screen	279
34.5 The ONT Bandwidth Group Screen	281
34.6 The Unregistered ONT Screen	282
34.7 The ONT WAN Screen	283
Chapter 35	
Static Route.....	285
35.1 Static Routing Overview	285
35.1.1 What You Can Do	285
35.2 Static Routing	285
Chapter 36	
DHCP.....	288
36.1 DHCP Overview	288
36.1.1 What You Can Do	288
36.1.2 What You Need to Know	288
36.2 DHCP Status	289
36.2.1 DHCP Status Detail	289
36.3 DHCPv4 Relay	291
36.3.1 DHCPv4 Relay Agent Information	291
36.3.2 Configuring DHCPv4 Global Relay	292
36.3.3 Global DHCP Relay Configuration Example	293
36.4 Configuring DHCP VLAN Settings	294
36.5 DHCP L2 Agent	295
36.6 ONT Option	299

Chapter 37	
Maintenance.....	301
37.1 Overview	301
37.1.1 What You Can Do	301
37.2 The Maintenance Screen	301
37.3 Load Factory Default	302
37.4 Save Configuration	302
37.5 Reboot System	303
37.6 Firmware Upgrade	303
37.7 Restore Configuration	304
37.8 Backup Configuration	304
37.9 Technical Reference	305
37.9.1 FTP Command Line	305
37.9.2 Filename Conventions	305
37.9.3 FTP Command Line Procedure	306
37.9.4 GUI-based FTP Clients	307
37.9.5 FTP Restrictions	307
Chapter 38	
Access Control.....	308
38.1 Access Control Overview	308
38.1.1 What You Can Do	308
38.2 The Access Control Main Screen	308
38.3 Configuring SNMP	309
38.3.1 Configuring SNMP Trap Group	310
38.3.2 Configuring SNMP User	311
38.4 Logins	313
38.5 Service Access Control	314
38.6 Remote Management	315
38.7 Technical Reference	316
38.7.1 About SNMP	316
38.7.2 SSH Overview	324
38.7.3 Introduction to HTTPS	326
38.7.4 Google Chrome Warning Messages	330
Chapter 39	
Diagnostic.....	332
39.1 Overview	332
39.2 Diagnostic	332
Chapter 40	
Syslog Setup	334
40.1 Syslog Overview	334

Table of Contents

40.1.1 What You Can Do	334
40.2 Syslog Setup	334
40.3 Syslog Server Setup	335
40.4 Syslog Upload Setup	336
Chapter 41	
MAC Table	339
41.1 MAC Table Overview	339
41.1.1 What You Can Do	339
41.1.2 What You Need to Know	339
41.2 Viewing the MAC Table	340
Chapter 42	
IP Table	342
42.1 IP Table Overview	342
42.2 Viewing the IP Table	343
Chapter 43	
ARP Table	344
43.1 ARP Table Overview	344
43.1.1 What You Can Do	344
43.1.2 What You Need to Know	344
43.2 Viewing the ARP Table	344
Chapter 44	
Routing Table	346
44.1 Overview	346
44.2 Viewing the Routing Table Status	346
Chapter 45	
Battery	347
45.1 Overview	347
45.2 The Battery Setup Screen	347
Part III: CLI Commands.....	350
About This CLI Reference Guide.....	351
Document Conventions	352
Chapter 46	
How to Access and Use the CLI.....	354

Table of Contents

46.1 Accessing the CLI	354
46.1.1 Console Port	354
46.1.2 Local Telnet	354
46.1.3 Remote Telnet	354
46.1.4 SSH	355
46.2 Logging in	355
46.3 Using Shortcuts and Getting Help	355
46.4 Dual Image Files	356
46.5 Dual Configuration Files	356
46.6 Saving Your Configuration	356
46.7 Logging Out	356

Chapter 47

Privilege Level and Command Mode.....	357
--	------------

47.1 Privilege Levels	357
47.1.1 Privilege Levels for Commands	357
47.1.2 Privilege Levels for Login Accounts	357
47.1.3 Privilege Levels for Sessions	358
47.2 Command Modes	359
47.2.1 Command Modes for Privilege Levels 0-12	359
47.2.2 Command Modes for Privilege Levels 13-14	360
47.3 Listing Available Commands	361

Chapter 48

Provisioning User Interfaces.....	364
--	------------

48.1 ONT Subscriber Port Provisioning Example Overview	364
48.2 ONT Subscriber Port Provisioning Example	364

Chapter 49

Basic Settings.....	370
----------------------------	------------

49.1 System Command	370
49.2 Multi-login Command	370
49.3 Date and Time Commands	371
49.4 Hardware Monitor Commands	373
49.5 External Alarm Commands	374
49.6 Switch Setup	375
49.7 IP Setup	375
49.7.1 Configure the Out-of-band Management IP Address Settings	376
49.7.2 Set the Out-of-band Management Default Gateway IP Address	376
49.7.3 Display IP Settings	377
49.8 Port Setup	377
49.8.1 Port Setup Commands Examples	378

Chapter 50	
IPv6	381
50.1 IPv6 Overview	381
50.1.1 IPv6 Addressing	381
50.1.2 IPv6 Terms	382
50.2 IPv6 Commands	387
50.3 IPv6 Command Examples	395
50.4 Example - Enabling IPv6 on Windows 7/10	397
Chapter 51	
VLAN.....	400
51.1 Introduction to VLANs	400
51.2 Introduction to IEEE 802.1Q Tagged VLANs	400
51.2.1 Forwarding Tagged and Untagged Frames	401
51.3 Static VLAN	401
51.4 VLAN Configuration Overview	401
51.5 VLAN Commands	402
51.5.1 VLAN Command Examples	404
51.6 Port VLAN Trunking	405
51.6.1 VLAN Trunking Setup Commands Example	406
51.7 Subnet Based VLANs	406
51.8 Subnet Based VLAN Commands	407
51.8.1 Subnet-based VLAN Command Examples	408
51.9 Protocol Based VLANs	408
51.9.1 Protocol Based VLAN Commands	409
51.9.2 Protocol Based VLAN Command Examples	410
Chapter 52	
Static MAC Forwarding.....	411
52.1 Static MAC Forwarding Overview	411
52.2 Static MAC Forwarding Commands	411
Chapter 53	
Static Multicast Forwarding.....	413
53.1 Static Multicast Forwarding Overview	413
53.2 Static Multicast Forwarding Commands	414
53.3 Static Multicast Forwarding Command Examples	415
Chapter 54	
AAA	417
54.1 AAA Overview	417
54.2 AAA Commands	418

Chapter 55	
TACACS+.....	421
55.1 TACACS+ Commands Summary	421
Chapter 56	
Display Commands	423
56.1 Display Commands Summary	423
Chapter 57	
Filtering.....	424
57.1 MAC Filtering Overview	424
57.2 MAC Filtering Commands	424
57.3 MAC Filtering Commands Examples	424
57.3.1 Command Example: Filter Source	425
Chapter 58	
Spanning Tree Protocol	426
58.1 STP/RSTP Overview	426
58.1.1 STP Terminology	426
58.1.2 How STP Works	427
58.1.3 STP Port States	427
58.1.4 Multiple STP	428
58.2 STP and RSTP Commands	430
58.2.1 STP and RSTP Command Examples	431
58.3 MSTP Commands	433
58.3.1 MSTP Command Examples	435
Chapter 59	
Bandwidth Control	438
59.1 Bandwidth Control Commands	438
Chapter 60	
MTU	440
60.1 MTU Commands	440
Chapter 61	
Broadcast Storm Control	441
61.1 Broadcast Storm Control Overview	441
61.2 Broadcast Storm Control Commands	441
61.3 Broadcast Storm Control Examples	442
Chapter 62	
Port Mirroring	444

62.1 Port Mirroring Overview	444
62.2 Port Mirroring Commands	444
62.3 Port Mirroring Command Examples	445
Chapter 63	
Link Aggregation	446
63.1 Link Aggregation Overview	446
63.2 Dynamic Link Aggregation	446
63.2.1 Link Aggregation ID	447
63.3 Link Aggregation Commands	447
63.4 Link Aggregation Commands Examples	448
Chapter 64	
RADIUS.....	451
64.1 RADIUS Commands	451
64.2 RADIUS Command Examples	452
Chapter 65	
Port Security.....	453
65.1 Port Security Overview	453
65.2 Port Security Commands	453
65.3 Port Security Command Examples	454
Chapter 66	
Classifier.....	456
66.1 Classifier and QoS Overview	456
66.2 QoS Commands	457
66.2.1 Show QoS Commands	458
66.3 Classifier Commands	459
66.4 Classifier Command Examples	461
Chapter 67	
RMON	462
67.1 RMON Overview	462
67.2 RMON Commands	463
Chapter 68	
Policy Rule	466
68.1 Policy Rules Overview	466
68.2 Policy Commands	466
68.3 Policy Command Examples	468
68.4 Two Rate Three Color Marker Traffic Policing	469
68.4.1 TRTCM - Color-blind Mode	469

68.4.2 TRTCM - Color-aware Mode	469
68.5 TRTCM Commands	470
68.6 TRTCM Command Examples	470
Chapter 69	
Queuing Method.....	472
69.1 Queuing Method Overview	472
69.1.1 Strictly Priority	472
69.1.2 Weighted Fair Queueing	472
69.2 Port by Port Queueing Commands	472
69.3 Port by Port Queueing Command Examples	473
69.4 System-Wide Queueing Commands	474
69.5 System-Wide Queueing Command Examples	474
Chapter 70	
VLAN Stacking and Translation	475
70.1 VLAN Stacking Overview	475
70.1.1 VLAN Stacking Port Roles	475
70.2 VLAN Translation Overview	476
70.2.1 VLAN Translation Example	476
70.3 VLAN Tag Format	476
70.3.1 Frame Format	477
70.4 Port-based Q-in-Q	477
70.5 Selective Q-in-Q	477
70.6 VLAN Stacking Commands	478
70.7 VLAN Stacking Command Examples	478
70.8 VLAN Translation Commands	481
70.9 VLAN Translation Command Examples	484
Chapter 71	
Multicast.....	485
71.1 Multicast Overview	485
71.1.1 IP Multicast Addresses	485
71.1.2 IGMP Snooping	485
71.2 Multicast Status	486
71.3 IGMP Proxy Commands	486
71.4 IGMP Snooping/Multicast Commands	487
71.5 IGMP CDR Commands	493
71.6 IGMP Snooping VLAN Commands	493
Chapter 72	
IP Source Guard.....	494
72.1 IP Source Guard Binding Commands	494

Table of Contents

72.2 IP Source Guard Binding Command Examples	494
72.3 DHCP Snooping & DHCP VLAN Commands	495
72.4 DHCP Snooping & DHCP VLAN Command Examples	498
72.5 ARP Inspection Commands	499
72.6 ARP Inspection Command Examples	502
Chapter 73	
 VoIP	505
73.1 VoIP Overview	505
73.2 VoIP Common Profile Commands	505
73.3 VoIP SIP Profile Commands	509
73.4 VoIP Dial Plan Profile Commands	512
73.4.1 Dial Plan Rule Details	513
73.5 UNI Port VoIP Service Settings	515
73.6 VoIP Show Commands	516
73.7 VoIP Configuration Supported on the PMG5318	516
73.8 ONT Subscriber VoIP Port Provisioning Example	519
73.8.1 Show the OLT VoIP Setup and Status	521
73.9 PMG5318 VoIP Setup Example	523
Chapter 74	
 Loop Guard	526
74.1 Loop Guard Overview	526
74.2 Loopguard Commands	528
74.3 Loopguard Command Examples	529
Chapter 75	
 Static Route.....	531
75.1 Static Route Commands	531
75.2 Static Route Command Examples	532
Chapter 76	
 DHCP	533
76.1 DHCP Overview	533
76.1.1 DHCP Modes	533
76.1.2 DHCP Configuration Options	533
76.2 DHCP Relay	533
76.2.1 DHCP Relay Agent Information	534
76.3 DHCP Commands	534
76.4 DHCP Command Examples	541
76.5 Configuring DHCP VLAN	542
Chapter 77	
 File Management.....	543

Table of Contents

77.1 FTP Command Line	543
77.1.1 Filename Conventions	543
77.1.2 FTP Command Line Procedure	544
77.2 GUI-based FTP Clients	544
77.2.1 FTP Restrictions	544
Chapter 78 Access Control.....	546
78.1 Access Control Overview	546
78.2 About SNMP	546
78.2.1 SNMP v3 and Security	547
78.2.2 Supported MIBs	547
78.3 SNMP Server Commands	548
78.4 SNMP Command Examples	551
78.5 Setting Up Login Accounts	551
78.6 Inactive Management Session Timeout Commands	552
78.7 Login Account Commands	552
78.8 Login Account Command Examples	553
78.9 Password Encryption	553
78.10 Password Commands	553
78.11 SSH Overview	554
78.12 How SSH works	554
78.13 SSH Implementation on the OLT	555
78.13.1 Requirements for Using SSH	556
78.14 Service Access Control Commands	556
78.15 Service Access Control Command Example	557
78.16 Remote Management Commands	557
78.17 Remote Management Command Example	558
Chapter 79 Diagnostics	559
79.1 Diagnostics Commands	559
79.2 Diagnostics Commands Examples	561
Chapter 80 Syslog	563
80.1 Syslog Overview	563
80.2 Syslog Commands	563
Chapter 81 MAC Address	565
81.1 MAC Address Table Overview	565
81.2 MAC Address Commands	566

81.3 MAC Address Command Examples	567
Chapter 82	
ARP Table	568
82.1 ARP Table Overview	568
82.1.1 How ARP Works	568
82.2 ARP Commands	568
82.3 ARP Command Examples	569
Chapter 83	
Routing Table.....	570
83.1 Routing Table Overview	570
83.2 Routing Table Commands	570
83.3 Routing Table Command Examples	571
Chapter 84	
Running Configuration.....	572
84.1 Running Configuration File	572
84.2 Running Configuration Commands	572
84.3 Running Configuration Command Examples	574
Chapter 85	
OLT Configuration	575
85.1 OLT Configuration Commands	575
Chapter 86	
PON Port Status.....	579
86.1 PON Port Status Commands	579
Chapter 87	
Remote ONT	580
87.1 Remote ONT Configuration Overview	580
87.2 ONT	580
87.3 UNI Port Settings	592
87.3.1 UNI Port General Commands	592
87.3.2 UNI Port Queue Settings	593
87.3.3 UNI Port VLAN Settings	596
87.3.4 UNI Port Protocol-based VLAN Settings	598
87.3.5 UNI Port PVID Settings	600
87.3.6 UNI Port IGMP Channel Settings	601
87.3.7 UNI Port MAC Limit Settings	604
87.3.8 UNI Port CFM MEP Settings	605

Chapter 88	
Port Protection Switching.....	606
88.1 Downlink Port Protection Switching	606
Chapter 89	
WRED	608
Chapter 90	
PPPoE IA	609
90.1 PPPoE Intermediate Agent Overview	609
90.1.1 Port State	609
90.2 PPPoE Intermediate Agent Commands	610
90.3 PPPoE IA Configuration	613
90.3.1 Activating PPPoE IA	613
90.3.2 PPPoE IA Access Loop Identification Settings	614
Chapter 91	
Port Bridge	615
91.1 Port Bridge Commands	615
Chapter 92	
IP and MAC Anti-Spoofing	616
92.1 IP and MAC Anti-Spoofing Overview	616
92.2 IP and MAC Anti-Spoofing Configuration	617
92.2.1 Activating IP and MAC Anti-Spoofing	617
92.2.2 VLAN and MAC Spoofing Settings	617
92.3 IP/MAC Anti-Spoofing Commands	618
92.4 Anti-MAC-Spoofing Commands	619
Chapter 93	
CPU Protection and DDoS	620
93.1 CPU Protection Overview	620
93.2 DDoS Overview	620
93.3 DDoS Setup	621
93.4 CPU Protection and DDoS Commands	621
Chapter 94	
Error-Disable Recovery.....	623
94.1 Error-Disable Recovery Overview	623
94.2 Error-Disable Recovery Commands	623
Chapter 95	
Battery.....	625

Table of Contents

95.1 Battery Commands	625
Chapter 96	
Additional Commands.....	626
96.1 Command Summary	626
	627
Chapter 97	
Product Specifications.....	628
97.1 System Specifications	628
97.2 Firmware Naming Conventions	629
Appendix A Customer Support	630
Appendix B Common Services.....	636
Appendix C Legal Information	639
Index	644

PART I

Introduction and

Hardware Installation

CHAPTER 1

System Introduction

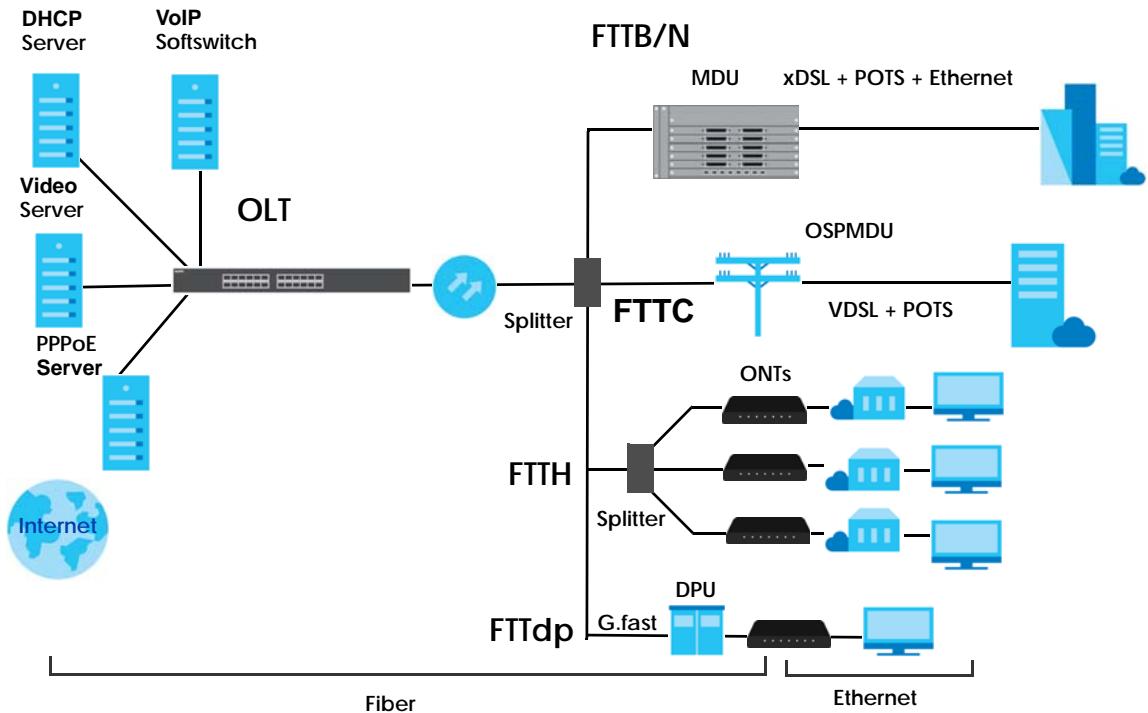
This chapter introduces the features of the OLT.

1.1 System Description

The OLT (Optical Line Terminal) connects and manages the end to end GPON (Gigabit Passive Optical Network) solution for delivering broadband data, high-quality voice, and IP television services. The OLT provides:

- Fiber to the building (FTTB) or neighborhood (FTTN) connections for Multi-Dwelling Units (MDUs).
- Fiber to the curb (FTTC) connections for standalone VDSL Outside Plant (OSP) MDUs.
- Fiber to the home (FTTH) connections for Optical Network Terminal (ONT) subscriber devices.
- Fiber to the distribution point (FTTdp) connections for G.Fast distribution point units (DPU). G.fast provides gigabit speeds over traditional copper twisted wires at distances of up to 100 meters from subscribers.

Figure 1 Network Overview



The OLT is 1 U and can be installed in a standard 19-inch (482 mm) equipment rack. The OLT supports SFP/SFP+ slots for backbone or subtending connections. The OLT has AC, DC, and battery power supplies. See [Section 3.1.7 on page 48](#) for more information about power connections. .

CHAPTER 2

Hardware Installation

This chapter describes how to connect the OLT.

2.1 General Installation Instructions

Perform the installation as follows:

- Make sure no power supplies are connected to the OLT. The OLT has AC, DC, and battery power supplies. See Section 3.1.7 on page 50 for more information about power connections.
- Install the OLT as detailed in [Section 2.2 on page 32](#), making sure you connect the frame grounds before you make any other connections.
- See [Section Figure 4 on page 34](#) to make power connections and turn on the OLT.
- To install the OLT in street cabinets or data centers, qualified service personnel is required.

2.2 Rack Mounting

The OLT can be mounted on an EIA standard size, 19-inch rack or in a wiring closet with other equipment. Follow the steps below to mount your OLT on a standard EIA rack using a rack-mounting kit.

2.2.1 Installation Requirements

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

The following table shows the items needed for the rack-mounting installation.

Table 1 Mounting Information

Attaching the Mounting Brackets to the OLT	
Mounting Brackets	Two
M4 Flat Head Screws	Four
Mounting the OLT on a rack	
Screws	Four Check with your rack vendor for the screws specification.

Failure to use the proper screws may damage the unit.

2.2.2 Precautions

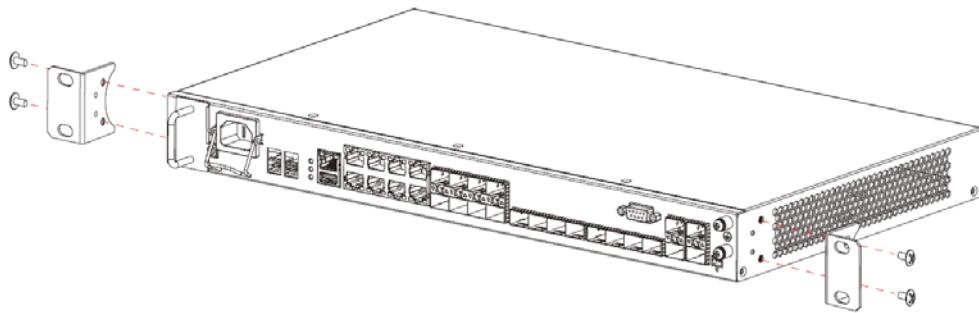
- Make sure the rack will safely support the combined weight of all the equipment it contains.

- Make sure the position of the OLT does not make the rack unstable or top-heavy. Take all necessary precautions to anchor the rack securely before installing the unit.

2.2.3 Attaching the Mounting Brackets to the OLT

- 1 Position a mounting bracket on one side of the OLT, lining up the two screw holes on the bracket with the screw holes on the side of the OLT.

Figure 2 Attaching the Mounting Brackets

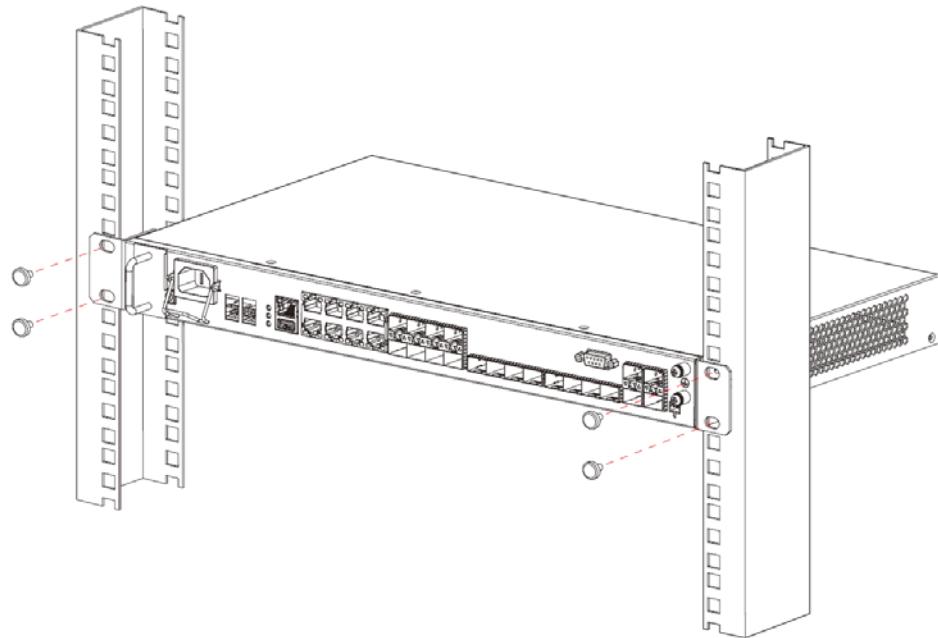


- 2 Using a screwdriver, install the M4 flat head screws through the mounting bracket holes into the OLT.
- 3 Repeat steps 1 and 2 to install the second mounting bracket on the other side of the OLT.
- 4 You may now mount the OLT on a rack. Proceed to the next section.

2.2.4 Mounting the OLT on a Rack

- 1 Position a mounting bracket (that is already attached to the OLT) on one side of the rack, lining up the two screw holes on the bracket with the screw holes on the side of the rack.

Figure 3 Mounting the OLT on a Rack



- 2 Using a screwdriver, install the screws through the mounting bracket holes into the rack.
- 3 Repeat steps 1 and 2 to attach the second mounting bracket on the other side of the rack.

2.3 Connecting the OLT Frame Grounds

Frame ground helps to protect against lightning and interference functions. Connect one of the frame ground M4 screws on the front panel to the building's protective earthing terminals.

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

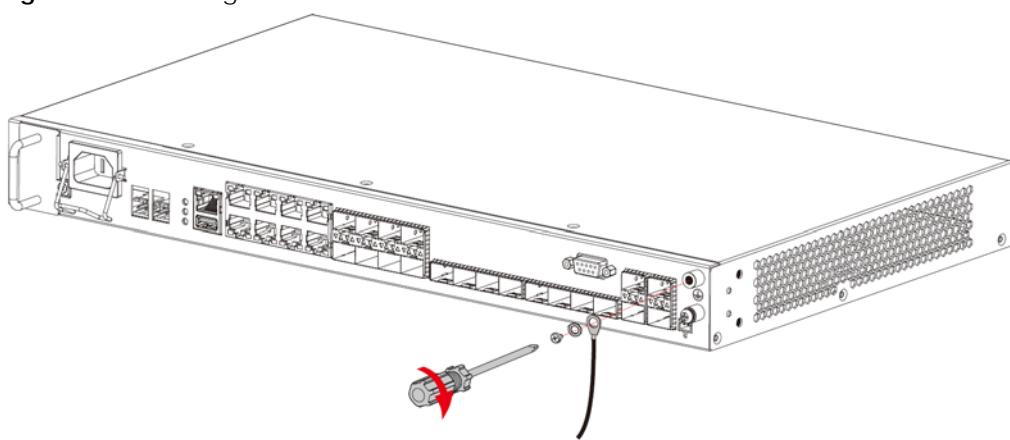
- 1 Remove one of the M4 ground screws from the OLT's front panel.
- 2 Secure a ground cable of the gauge specified in [Chapter 97 on page 628](#) to the OLT's front panel using the M4 ground screw.
- 3 Attach the other end of the cable to the ground, either to the same ground electrode as the rack you installed the device on or to the main grounding electrode of the building.

Follow your country's regulations and safety instructions to electrically ground the device properly.

If you are uncertain that suitable grounding is available, contact the appropriate electrical inspection authority or an electrician.

Warning! Connect the ground cable before you connect any other cables or wiring.

Figure 4 Grounding



2.4 Connect the DC Power

The OLT has a DC slot on the front panel for redundant power supply.

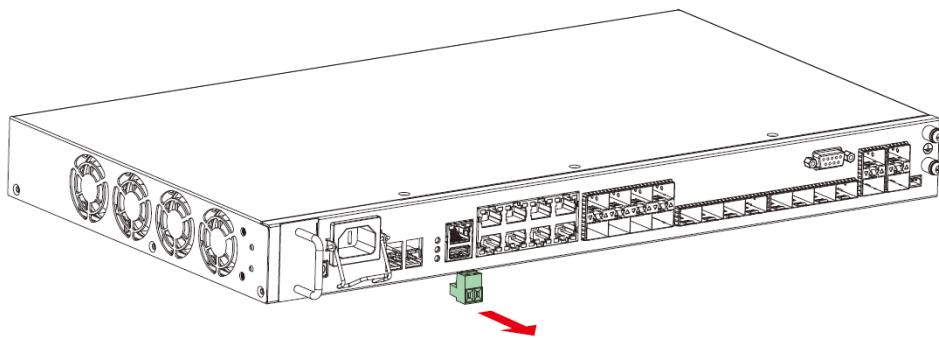
When connecting the OLT power wires to the power module, push the wires firmly into the terminals as deep as possible and make sure that no exposed (bare) wires can be seen or touched.

Use wires of the gauge specified in [Chapter 97 on page 628](#) to connect each DC input to a DC power supply to supply the operating voltage for the OLT.

For supply connections, use wires suitable for at least 90°C.

- 1 Remove the green power connector block from the front of the power module.

Figure 5 Remove the Power Connector Block

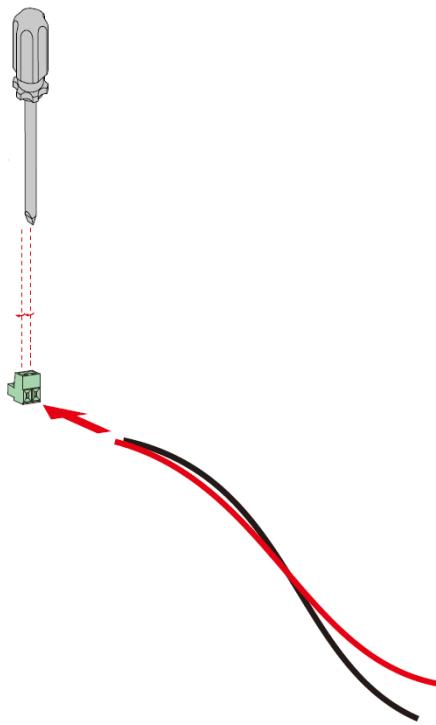


- 2 Connect a power wire to the **RTN** power terminal on the power connector block and tighten the terminal screw.

Do not insert the power wires while the power connector block is still connected to the OLT.

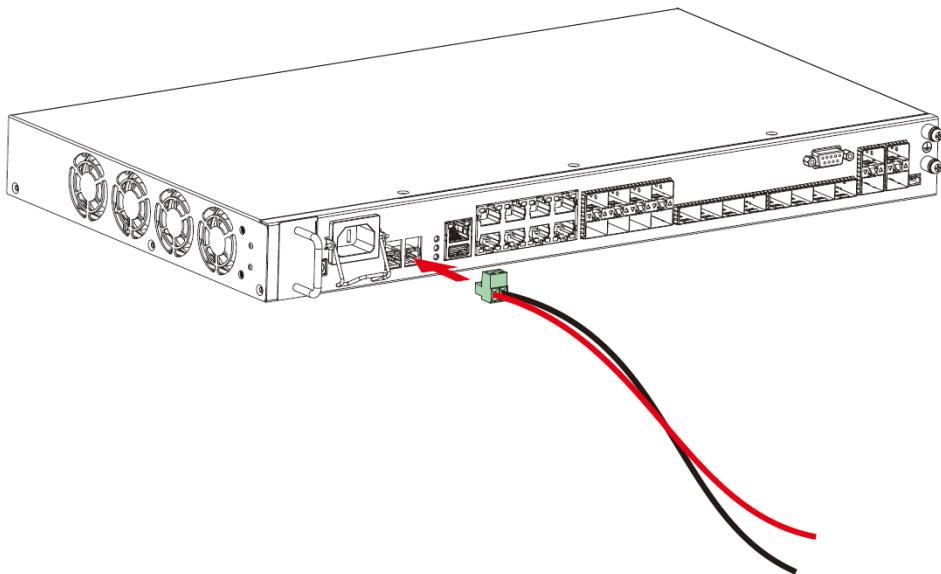
- 3 Connect a power wire to the **-48V** power terminal on the power connector block and tighten the terminal screw.

Figure 6 Connect the Power Wires



- 4 Connect the other end of the RTN power wire to the positive terminal on the power supply.
- 5 Connect the other end of the -48 V power wire to the negative terminal on the power supply.
- 6 Push the power connector block back into the power input.

Figure 7 Push the Power Connector Block Back into the Power Input



- 7 Turn on the power supply.

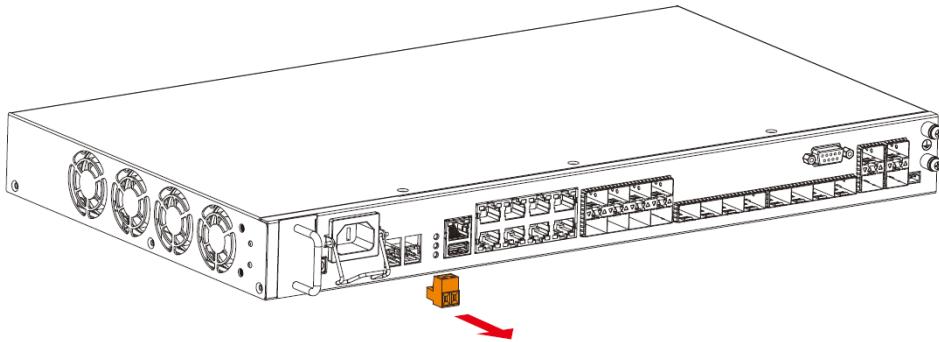
2.5 Battery

Use wires of the gauge specified in [Chapter 97 on page 628](#) to connect the battery input to a battery to supply the operating voltage for the OLT.

When connecting the OLT power wires to the battery input, push the wires firmly into the terminals as deep as possible and make sure that no exposed (bare) wires can be seen or touched.

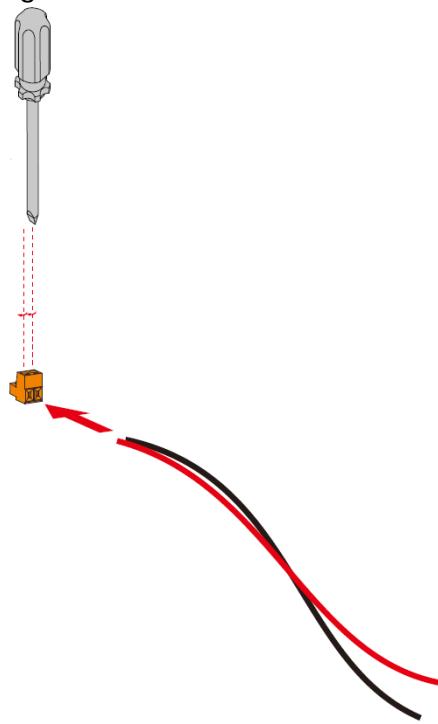
- 1 Remove the orange power connector block from the battery input.

Figure 8 Remove the Power Connector Block

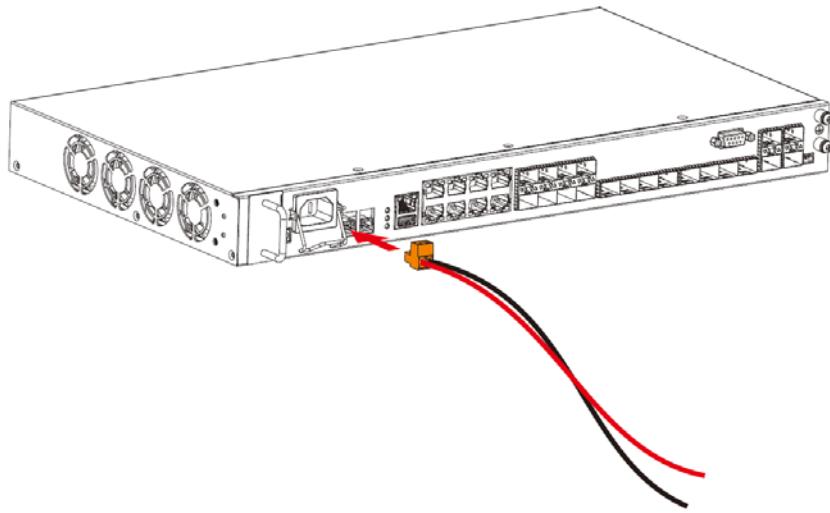


- 2 Connect power wires to the power terminals on the power connector block and tighten the terminal screws.

Do not insert the power wires while the power connector block is still connected to the OLT.

Figure 9 Connect the Power Wires

- 3 Connect the other end of the **BAT+** power wire to the positive terminals on the battery.
- 4 Connect the other end of the **BAT-** power wire to the negative terminals on the power supplies.
- 5 Push the power connector block into the OLT battery input.

Figure 10 Push the Power Connector Block Back into the Power Input

2.5.1 Battery Charge

The battery can only be recharged through the AC power connection. If the battery and DC power supplies are the only ones connected to the OLT, the DC power connection will not supply power to the battery charger.

To recharge the battery, make sure:

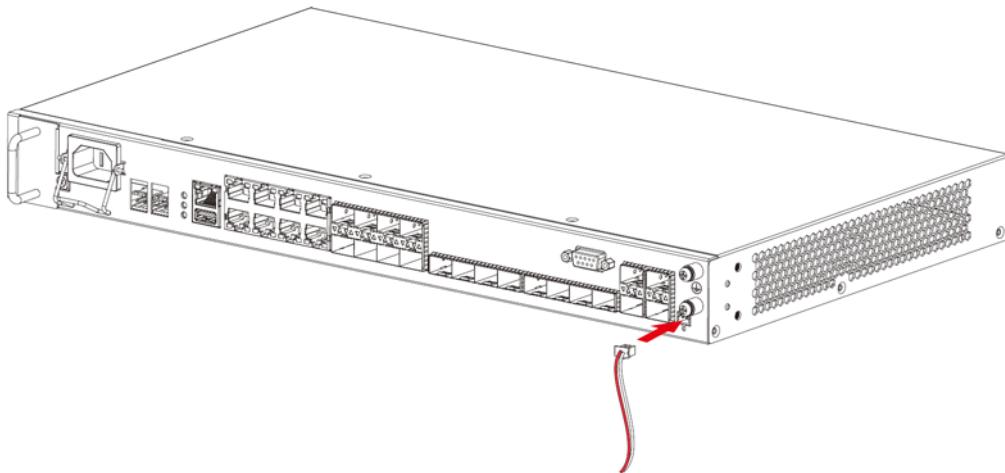
- The OLT has an AC power connection.
- The OLT's battery **SENSOR** port must be properly connected to the battery. See [Section 2.5.2 on page 39](#).
- The battery's temperature must be between the temperatures set in the **Management > Battery** screen (default is between 0°C and 40°C). Modify the temperature range according to your battery's specifications.
- The battery's capacity must be set in the **Management > Battery** screen. Modify this value according to your battery's specifications.
- The battery voltage is between 11V~14.6V.

2.5.2 Battery Sensor Connection

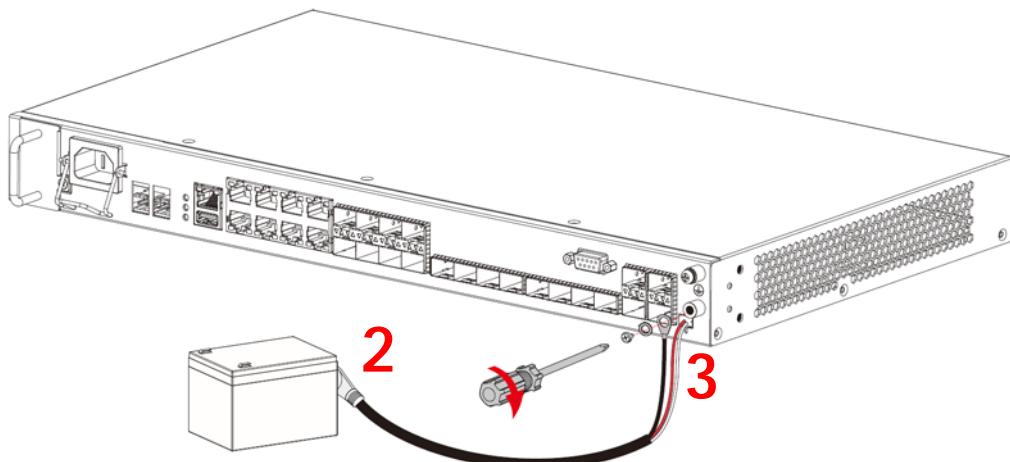
Use the OLT battery sensor to monitor the temperature of the battery supplying power to the OLT. In order to charge the battery, the battery sensor must be properly connected. Follow these steps to connect the battery sensor:

- 1 Plug the sensor cable into the OLT battery **SENSOR** port.

Figure 11 Connect the Sensor Cable to the SENSOR Port



- 2 Attach one temperature sensor lug of the sensor cable to the battery with an adhesive, or to a battery's stud (read your battery's specifications).
- 3 Attach the other temperature sensor lug of the sensor cable to one of the M4 ground screws.

Figure 12 Attach Temperature Sensor Lugs

2.6 Fan Module

This section describes how to change the fan module on the OLT.

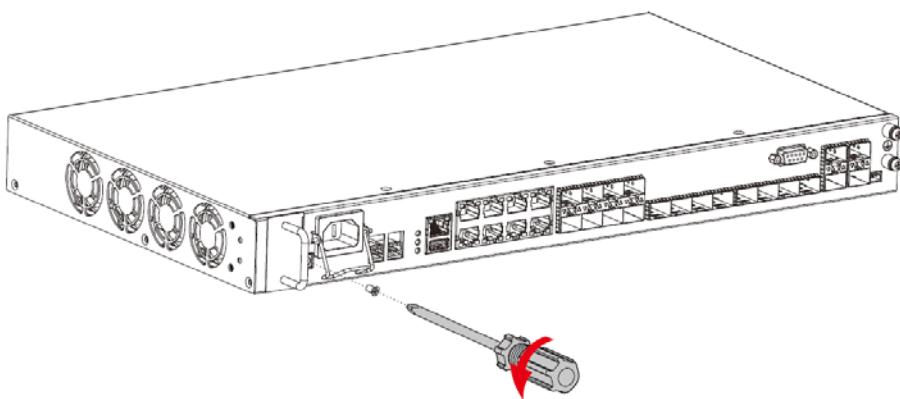
2.6.1 Remove and Install the Fan Module

The OLT 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 fans 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 fans or change the fan module.

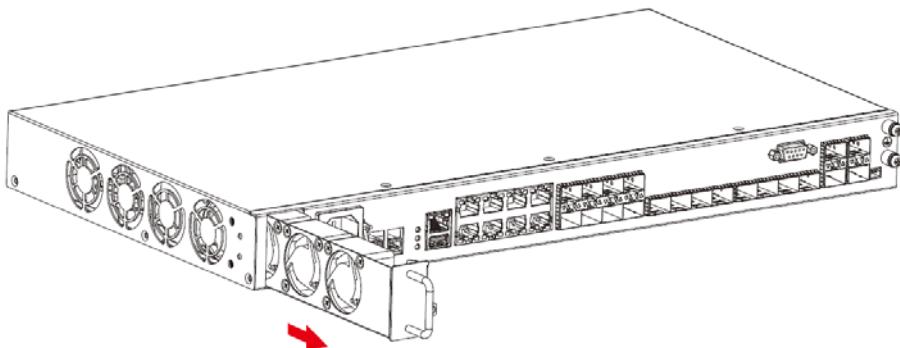
Install the fan module or a spare one shortly after it's removed to prevent the OLT from overheating. Overheating could affect the performance of your OLT, or even damage it.

- 1 Loosen the screw on the front of the fan module.

Figure 13 Loosen the Fan Module Screw

- 2** Slide out the fan module.

Figure 14 Remove the Fan Module



- 3** Clean the fans.
- 4** Slide the fan module back into the fan module slot (Or use a different fan module from the manufacturer).
- 5** Tighten the screw.

CHAPTER 3

Hardware Panels

This chapter describes the front panels of the OLT.

To protect yourself from the OLT's high operating temperatures, wear protective gloves before you touch the OLT.

3.1 Front Panel

The following figure shows the front panels of the OLT.

Figure 15 OLT1404A Front Panel

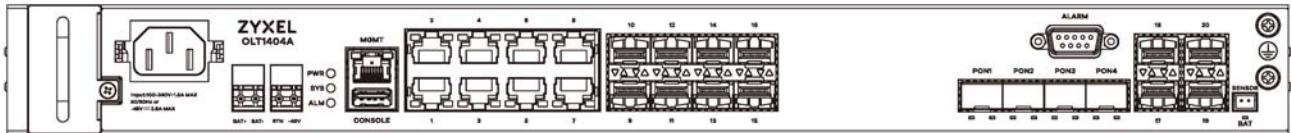
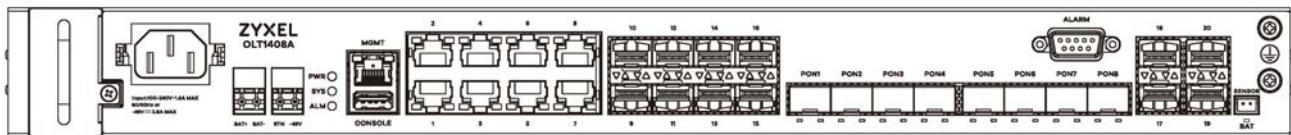


Figure 16 OLT1408A Front Panel



The following table describes the port labels on the front panel.

Table 2 Front Panel Connections

LABEL	DESCRIPTION
Fan Module	Install the fan module to prevent the OLT from overheating.
Power Connections	Connect an appropriate power supply to each power input.
MGMT	Connect to a computer using an RJ-45 Ethernet cable for local configuration of the OLT.
CONSOLE	Connect to a computer using a USB type A cable for local configuration of the OLT.
Gigabit Ethernet	Connect computers or other Ethernet devices to Ethernet ports for uplink connections or Internet access.
SFP (Port 9-16)	Use these 1/2.5 Gbps SFP slots for uplink and subtending connections.
SFP+ (Port 17-20)	Use these 1/2.5/10 Gbps SFP+ slots for uplink and subtending connections.
PON	Connect to an ONT using a fiber optic cable to configure settings on the ONT.
ALARM	This port is for alarm input/output.
SENSOR	This port is for the OLT sensor to measure the battery temperature.

3.1.1 Gigabit Ethernet Ports

The OLT has 1000Base-T auto-negotiating, auto-crossover Ethernet ports. In 100/1000 Mbps Gigabit Ethernet, the speed can be 100 Mbps or 1000 Mbps. The duplex mode can be full duplex.

An auto-negotiating port can detect and adjust to the optimum Ethernet speed (100/1000 Mbps) and duplex mode (full duplex) of the connected device.

An auto-crossover (auto-MDI/MDI-X) port automatically works with a straight-through or crossover Ethernet cable.

When auto-negotiation is turned on, an Ethernet port negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer Ethernet port does not support auto-negotiation or turns off this feature, the OLT determines the connection speed by detecting the signal on the cable. When the OLT's auto-negotiation is turned off, an Ethernet port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer Ethernet port are the same in order to connect.

3.1.1.1 Auto-crossover

All ports are auto-crossover, that is auto-MDIX ports (Media Dependent Interface Crossover), so you may use either a straight-through Ethernet cable or crossover Ethernet cable for all Gigabit port connections. Auto-crossover ports automatically sense whether they need to function as crossover or straight ports, so crossover cables can connect both computers and switches/hubs.

3.1.2 SFP/SFP+ Slots

These slots house 10G SFP+ or SFP transceivers. A transceiver is a single unit that includes a transmitter and a receiver. The OLT does not come with transceivers.

The SFP+ slots can function in either uplink or subtending mode. Connect a port in uplink mode to a backbone Ethernet switch or router.

Use the subtending mode to daisy-chain other MSAN devices or Ethernet switches. The OLT allows traffic between the ports in subtending mode and the ports in uplink mode. It does not allow traffic between the ports in subtending mode.

You can use different transceivers while the OLT is operating.

- Type: SFP or SFP+ connection interface
- Connection speed: 1/2.5/10 Gigabit per second (Gbps)

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

3.1.2.1 Supported SFP+ and SFP Transceivers

Table 3 Supported SFP+ and SFP Transceivers

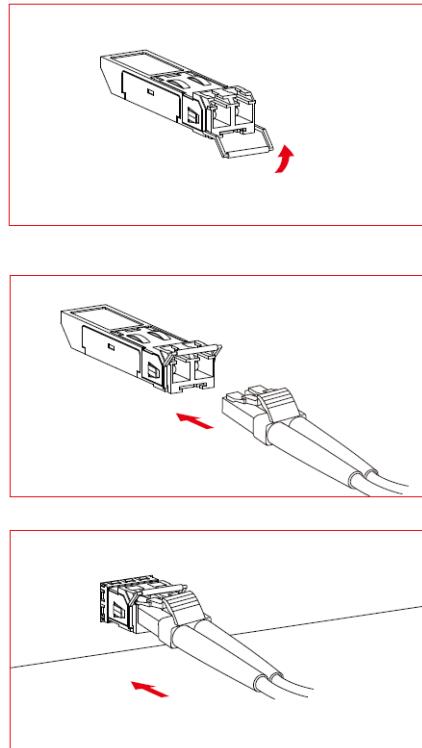
SPEED	MODEL	PN	DESCRIPTION
10 Gigabit SFP+	SFP10G-LR-DS	SFP10G-LR-DS-ZZ01V1F	SFP+ 10G LR wavelength=1310, 10 km (10936 yd) commercial type transceiver, DDMI version
Gigabit (with DDMI)	SFP-SX-DS	SFP-SX-DS-ZZ01V1F	GbE SFP SX Multi-Mode 550 m (1804 ft) commercial type transceiver, DDMI version
	SFP-LX-5DS	SFP-LX-5DS-ZZ01V1F	GbE SFP LX 5 km (5468 yd) commercial type transceiver, DDMI version
	SFP-LX-15DS	SFP-LX-15DS-ZZ01V1F	GbE SFP LX 15~20 km (16404~21872 yd) commercial type transceiver, DDMI version
	SFP-BXA-20DS	SFP-BXA-20DS-ZZ01V1F	GbE SFP BX 20km (21872 yd) Bidirectional Type-A 1310~1550Tx, DDMI version
	SFP-BXB-20DS	SFP-BXB-20DS-ZZ01V1F	GbE SFP BX 20km (21872 yd) Bidirectional Type-B 1550~1310Tx, DDMI version
	SFP-BXC-20DS	SFP-BXC-20DS-ZZ01V1F	GbE SFP BX 20km (21872 yd) Bidirectional Type-C 1310~1490Tx, DDMI version
	SFP-BXD-20DS	SFP-BXD-20DS-ZZ01V1F	GbE SFP BX 20km (21872 yd) Bidirectional Type-D 1490~1310Tx, DDMI version
	SFP-LHX-40DS	SFP-LHX-40DS-ZZ01V1F	GbE SFP LHX wavelength=1310, 40 km (43744 yd) commercial type transceiver, DDMI version
	SFP-ZX-80DS	SFP-ZX-80DS-ZZ01V1F	GbE SFP ZX wavelength=1550, 80 km (87488 yd) commercial type transceiver, DDMI version

3.1.2.2 Transceiver Installation

Use the following steps to install an SFP or SFP+ module in a slot.

- 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 the cable dust covers).
- 4 Insert the transceiver into the slot.
- 5 Press the transceiver firmly until it clicks into place.

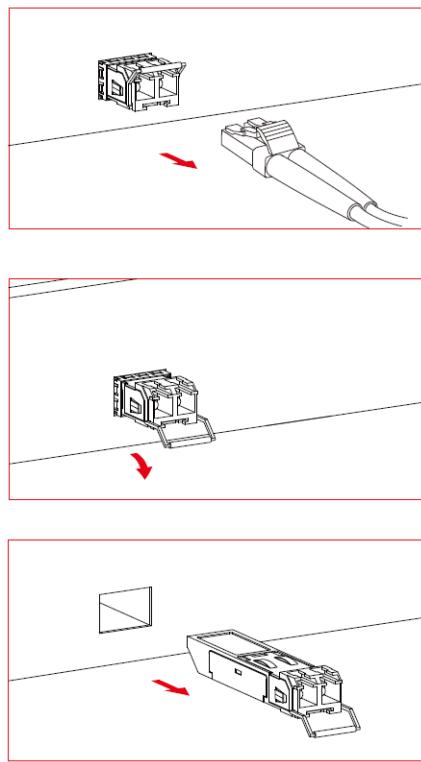
Figure 17 Transceiver Installation Example



3.1.2.3 Transceiver Removal

Use the following steps to remove an SFP or SFP+ module from a 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 18 Transceiver Removal Example

3.1.3 GPON SFP Slots

The OLT provides 4/8 GPON SFP slots compliant with ITU-T G.984. Each SFP slot supports up to 128 PON subscribers.

3.1.3.1 GPON SFP Slots Connectors

The GPON SFP slots have SFP MSA compliant connectors that support Class B+ or Class C+ GPON transceivers.

Supported Transceiver Specifications

ITEM	CLASS B+	CLASS C+
Link Budget	28 dB	32 dB
Downstream Speed	2.488 Gbps	
Upstream Speed	1.244 Gbps	
Wavelength for downstream	1490 nm	
Wavelength for upstream	1310 nm	
Max Distance	20 km	60 km
Splitter Ratio	1:128	

3.1.3.2 Supported Transceivers

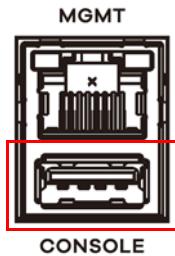
The GPON SFP slots support the following transceivers.

67-007-901001B (SFP Series, ROHS, LTE3680P-BH+ SFP GPON OLT Transceiver Class C+ 2488/ 1244Mb/s with Digital RSSI Industrial, HISENSE)

3.1.4 Console Port

Connect one end of a USB Type A cable to the **CONSOLE** port of the OLT. Connect the other end to a USB port on your computer.

Figure 19 OLT Console Port



For local management, you can use a computer with terminal emulation software configured to the following parameters:

- VT100
- Terminal emulation
- 115200 bps
- No parity, 8 data bits, 1 stop bit
- No flow control

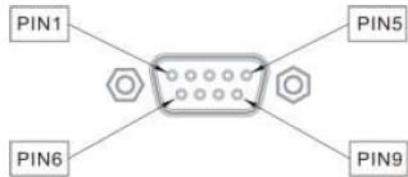
3.1.5 Management Port

The **MGMT** (management) port is used for local management. Connect directly to this port using an Ethernet cable. The default out-of-band IP address of the management port is 192.168.0.1 with a subnet mask of 255.255.255.0.

3.1.6 ALARM Port

The ALARM port is a male 9-pin connector. The following figure shows the pin assignments.

Figure 20 Alarm Port: Pin Assignment



The following table describes the alarm pins.

Table 4 Alarm Port Input: Pin Assignment

ALARM INPUT	PIN	DESCRIPTION
1	Pin 3 and Pin 7	An open circuit for pins 3 and 7 indicates no alarm status. A closed circuit indicates an alarm status.
2	Pin 3 and Pin 8	An open circuit for pins 3 and 8 indicates no alarm status. A closed circuit indicates an alarm status.
3	Pin 4 and Pin 9	An open circuit for pins 4 and 9 indicates no alarm status. A closed circuit indicates an alarm status.
4	Pin 4 and Pin 5	An open circuit for pins 4 and 5 indicates no alarm status. A closed circuit indicates an alarm status.

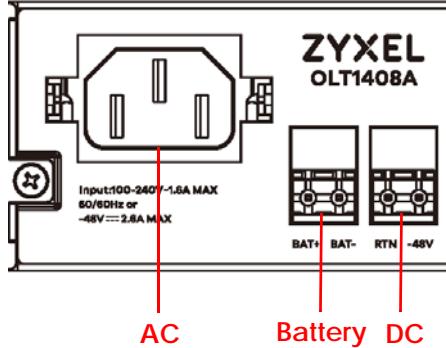
Table 5 Alarm Port Output: Pin Assignment

ALARM OUTPUT	PIN	DESCRIPTION
Alarm out asserted	Pin 2 and Pin 6	A closed circuit for pins 2 and 6 indicates an alarm output status.
Alarm out deasserted	Pin 1 and Pin 6	A closed circuit for pins 1 and 6 indicates no alarm output status.

3.1.7 OLT Power Connections

The OLT can have all AC, DC and battery power supplies connected at the same time. However, only one of them supplies power to the OLT at a time. If all three are connected the priority for power supply is **AC > DC > Battery**.

Figure 21 OLT Power Terminals



3.2 LEDs

After you connect the power to the OLT, view the LEDs to ensure proper functioning of the OLT and as an aid in troubleshooting.

Table 6 LED Descriptions

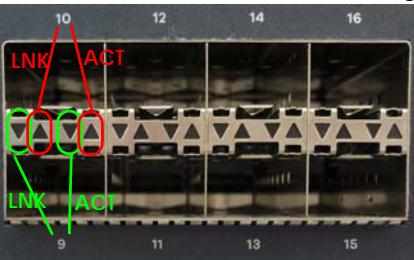
LED	COLOR	STATUS	DESCRIPTION
PWR	Green	On	The OLT is receiving power.
		Off	The OLT is not receiving power.

Table 6 LED Descriptions (continued)

LED	COLOR	STATUS	DESCRIPTION
SYS	Green	On	The OLT is on and functioning properly.
		Blinking	The OLT is initializing.
		Off	The OLT is not functioning.
ALM	Red	On	The OLT has an alarm.
		Off	The OLT is operating normally.
MGMT	Green (Left)	On	A 10 Mbps Ethernet link is up.
		Blinking	The port is transmitting/receiving to/from a 10 Mbps Ethernet device.
		Off	The Ethernet link is down.
	Amber (Right)	On	A 100 Mbps Ethernet link is up.
		Blinking	The port is transmitting/receiving to/from a 100 Mbps Ethernet network.
		Off	The Ethernet link is down.
Gigabit Ethernet	Green (Left)	On	The link to a 1000 Mbps Ethernet network is up.
		Blinking	The OLT is transmitting/receiving to/from a 1000 Mbps Ethernet network.
		Off	The link to a 1000 Mbps Ethernet network is down.
	Amber (Right)	On	The link to a 100 Mbps Ethernet network is up.
		Blinking	The OLT is transmitting/receiving to/from a 100 Mbps Ethernet network.
		Off	The link to a 100 Mbps Ethernet network is down.
SFP/SFP+	Green (LNK)	On	An optical network is up.
		Off	An optical network is down.
	Green (ACT)	Blinking	The OLT is transmitting/receiving to/from the optical network.
		Off	The OLT is not transmitting/receiving to/from the optical network.

The downward arrows are for the port at the bottom. The upward arrows are for the port at the top.

The left arrow is the LNK LED, and the right arrow is the ACT LED.



PON	Green (Left)	On	The OLT recognizes a GPON transceiver through the PON port.
	Green (Right)	On	A PON link is up.
BAT	Green	On	The voltage of the connected battery is normal, or the battery is float charging mode.
		Blinking	A battery is connected to the OLT, and it's charging.
		Off	A battery is not connected to the OLT, or the connected battery is abnormal.

PART II

Web Configurator

CHAPTER 4

The Web Configurator

4.1 Overview

This section introduces the configuration and functions of the web configurator.

The Web Configurator is an HTML-based management interface that allows easy system setup and management via Internet browser. Use Internet Explorer 6.0 or later. 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).

4.2 System Login

- 1 Start your web browser.
- 2 Type "http://" and the IP address of the OLT 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 22 Web Configurator: Login



- 4 Click **OK** to enter the OLT's Web Configurator **Status** screen.

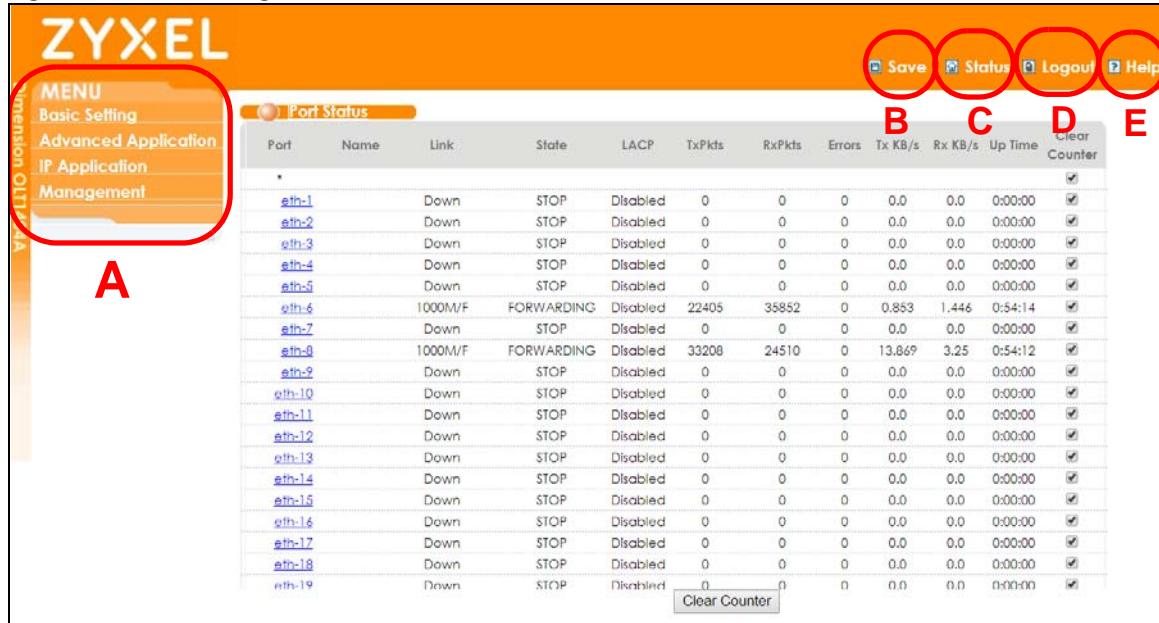
4.3 The Status Screen

The **Status** screen is the first screen that displays when you access the web configurator.

This guide uses the OLT1404A screens as an example. The screens may very slightly for different models.

The following figure shows the navigating components of a web configurator screen.

Figure 23 Web Configurator Home Screen (Status)



A - Click the menu items to open submenu links, and then click on a submenu link to open the screen in the main window.

B, C, D, E - These are quick links which allow you to perform certain tasks no matter which screen you are currently working in.

B - Click this link to save your configuration into the OLT's nonvolatile memory. Nonvolatile memory is the configuration of your OLT that stays the same even if the OLT's power is turned off.

C - Click this link to go to the status page of the OLT.

D - Click this link to log out of the web configurator.

E - Click this link to display web help pages. The help pages provide descriptions for all of the configuration screens.

In the navigation panel, click a main link to reveal a list of submenu links.

Table 7 Navigation Panel Sub-links Overview

BASIC SETTING	ADVANCED APPLICATION	IP APPLICATION	MANAGEMENT
MENU Basic Setting Advanced Application IP Application Management System Info General Setup Switch Setup IP Setup Port Setup	MENU Basic Setting Advanced Application IP Application Management VLAN Static MAC Forwarding Static Multicast Forwarding Filtering Spanning Tree Protocol Bandwidth Control Broadcast Storm Control Mirroring Link Aggregation Port Authentication Port Security Classifier Policy Rule Queuing Method VLAN Stacking Multicast AAA IP Source Guard Loop Guard PPPoE Errdisable ONT VoIP PON DDMI File Transfer Ont PM Counter Qos Profile OLT Registration ONT Template ONT Quick Setup	MENU Basic Setting Advanced Application IP Application Management Static Routing DHCP	MENU Basic Setting Advanced Application IP Application Management Maintenance Access Control Diagnostic Syslog MAC Table IP Table ARP Table Routing Table Battery

The following table describes the links in the navigation panel.

Table 8 Navigation Panel Links

LINK	DESCRIPTION
Basic Settings	
System Info	This link takes you to a screen that displays general system information.
General Setup	This link takes you to a screen where you can configure general identification information about the OLT.
Switch Setup	This link takes you to a screen where you can set up global OLT parameters such as VLAN type, GARP and priority queues.
IP Setup	This link takes you to a screen where you can configure the IP address and subnet mask (necessary for OLT management) and set up to 64 IP routing domains.
Port Setup	This link takes you to a screen where you can configure settings for individual OLT ports.
Advanced Application	
VLAN	This link takes you to screens where you can configure 802.1Q VLAN. You can also configure a protocol based VLAN or a subnet based VLAN in these screens.

Table 8 Navigation Panel Links (continued)

LINK	DESCRIPTION
Static MAC Forwarding	This link takes you to a screen where you can configure static MAC addresses for a port. These static MAC addresses do not age out.
Static Multicast Forwarding	This link takes you to a screen where you can configure static multicast MAC addresses for port(s). These static multicast MAC addresses do not age out.
Filtering	This link takes you to a screen to set up filtering rules.
Spanning Tree Protocol	This link takes you to screens where you can configure the RSTP/MRSTP/MSTP to prevent network loops.
Bandwidth Control	This link takes you to a screen where you can configure bandwidth limits on the OLT.
Broadcast Storm Control	This link takes you to a screen to set up broadcast filters.
Mirroring	This link takes you to screens where you can copy traffic from one port or ports to another port in order that you can examine the traffic from the first port without interference.
Link Aggregation	This link takes you to screens where you can logically aggregate physical links to form one logical, higher-bandwidth link.
Port Security	This link takes you to screens where you can activate MAC address learning and set the maximum number of MAC addresses to learn on a port.
Classifier	This link takes you to screens where you can configure the OLT to group packets based on the specified criteria.
Policy Rule	This link takes you to a screen where you can configure the OLT to perform special treatment on the grouped packets.
Queuing Method	This link takes you to a screen where you can configure queuing with associated queue weights for each port.
VLAN Stacking	This link takes you to screens where you can activate and configure VLAN stacking.
Multicast	This link takes you to screens where you can configure various multicast features, IGMP snooping, MLD snooping-proxy and create multicast VLANs.
AAA	This link takes you to a screen where you can configure authentication, authorization and accounting services via external servers. The external servers can be either RADIUS (Remote Authentication Dial-In User Service) or TACACS+ (Terminal Access Controller Access-Control System Plus).
IP Source Guard	This link takes you to screens where you can configure filtering of unauthorized DHCP and ARP packets in your network.
Loop Guard	This link takes you to a screen where you can configure protection against network loops that occur on the edge of your network.
PPPoE	This link takes you to screens where you can configure intermediate agent settings in port, VLAN, and PPPoE.
Errdisable	This link takes you to screens where you can view errdisable status and configure errdisable settings in CPU protection, errdisable detect, and errdisable recovery.
ONT VoIP	This link takes you to screens where you can configure VoIP settings for the subscriber Optical Network Terminal (ONT) devices.
PON DDMI	This link takes you to screens where you can configure profiles of ONT alarm thresholds. You can also configure high and low parameter limits for your OLT's SFP transceivers in this screen.
File Transfer	This link takes you to a screen where you can transfer a config.xml file between a specific URL and an ONT using FTP.
Ont PM Counter	This link takes you to a screen where you can view the performance monitoring counters for the specified subscriber Ethernet interface.
Qos Profile	This link takes you to screens where you can configure Quality of Service settings for the ONT devices, and thresholds for the TCA profile.

Table 8 Navigation Panel Links (continued)

LINK	DESCRIPTION
OLT Registration	This link takes you to screens where you can configure the ONT registration settings on the OLT, configure the thresholds for the TCA profile, and view the status of ONTs for each GPON interface.
ONT Template	This link takes you to screens where you can configure ONT templates to manage ONT settings.
ONT Quick Setup	This link takes you to screens where you can create, modify, and delete an ONT configuration.
IP Application	
Static Routing	This link takes you to a screen where you can configure IPv4 static routes. A static route defines how the OLT should forward traffic by configuring the TCP/IP parameters manually.
DHCP	This link takes you to screens where you can configure the DHCP settings.
Management	
Maintenance	This link takes you to screens where you can perform firmware and configuration file maintenance as well as reboot the system.
Access Control	This link takes you to screens where you can change the system login password and configure SNMP and remote management.
Diagnostic	This link takes you to a screen where you can ping IP addresses, run traceroute, test port(s) and show the OLT's location.
Syslog	This link takes you to a screen where you can view system logs.
Syslog Setup	This link takes you to a screen where you can setup system logs and a system log server.
MAC Table	This link takes you to a screen where you can view the MAC addresses (and types) of devices attached to what ports and VLAN IDs.
IP Table	This link takes you to a screen where you can view the IP addresses and VLAN ID of a device attached to a port. You can also view what kind of device it is.
ARP Table	This link takes you to a screen where you can view the MAC addresses – IP address resolution table.
Routing Table	This link takes you to a screen where you can view the routing table.
Battery	This link takes you to a screen where you can set up the OLT battery capacity and temperature threshold, and view its status.

4.3.1 Change Your Password

After you log in for the first time, it is recommended you change the default administrator password. Click **Management > Access Control > Logins** to display the next screen.

Figure 24 Change Administrator Login Password

Logins

Administrator

Old Password
New Password
Retype to confirm

Please record your new password whenever you change it. The system will lock you out if you have forgotten your password.

Edit Logins

Login	User Name	Password	Retype to confirm	Privilege
1				0 ▾
2				0 ▾
3				0 ▾
4				0 ▾

Apply Cancel

4.4 Saving Your Configuration

When you are done modifying the settings in a screen, click **Apply** to save your changes back to the run-time memory. Settings in the run-time memory are lost when the OLT's power is turned off.

Click the **Save** link in the upper right hand corner of the web configurator to save your configuration to nonvolatile memory. Nonvolatile memory refers to the OLT's storage that remains even if the OLT's power is turned off.

Note: Use the **Save** link when you are done with a configuration session.

4.5 Lockout

You could block yourself (and all others) from managing the OLT if you do one of the following:

- 1 Delete the management VLAN (default is VLAN 1).
- 2 Delete all port-based VLANs with the CPU port as a member. The "CPU port" is the management port of the OLT.
- 3 Filter all traffic to the CPU port.
- 4 Disable all ports.
- 5 Misconfigure the text configuration file.
- 6 Forget the password and/or IP address.
- 7 Prevent all services from accessing the OLT.

- 8 Change a service port number but forget it.

Note: Be careful not to lock yourself and others out of the OLT.

4.6 Resetting the OLT

If you lock yourself (and others) from the OLT or forget the administrator password, you will need to reload the factory-default configuration file or reset the OLT back to the factory defaults.

4.6.1 Reload the Configuration File

Uploading the factory-default configuration file replaces the current configuration file with the factory-default configuration file. This means that you will lose all previous configurations and the speed of the console port will be reset to the default of 115200 bps with 8 data bits, no parity, one stop bit and flow control set to none. The password will also be reset to "1234". The default in-band management IP address will be reset to 192.168.1.1 and the default out-of-band (management port) IP address to 192.168.0.1.

To upload the configuration file, do the following:

- 1 Connect to the console port using a computer with terminal emulation software.
- 2 Disconnect and reconnect the OLT's power to begin a session. When you reconnect the OLT's power, you will see the initial screen.
- 3 When you see the message "Press any key to enter Debug Mode within 1 seconds..." press any key to enter debug mode.
- 4 Type at1c after the "Enter Debug Mode" message.
- 5 Wait for the "Starting XMODEM upload" message before activating XMODEM upload on your terminal.
- 6 After a configuration file upload, type atgo to restart the OLT.

The OLT is now reinitialized with a default configuration file including the default password of "1234".

4.7 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 for security reasons.

Figure 25 Web Configurator: Logout Screen



4.8 Help

The web configurator's online help has descriptions of individual screens and some supplementary information.

Click the **Help** link from a web configurator screen to view an online help description of that screen.

CHAPTER 5

Initial Setup Example

5.1 Overview

This chapter shows how to set up the OLT for an example network.

The following lists the configuration steps for the initial setup:

- Create a VLAN
- Set port VLAN ID
- Configure the OLT IP management address

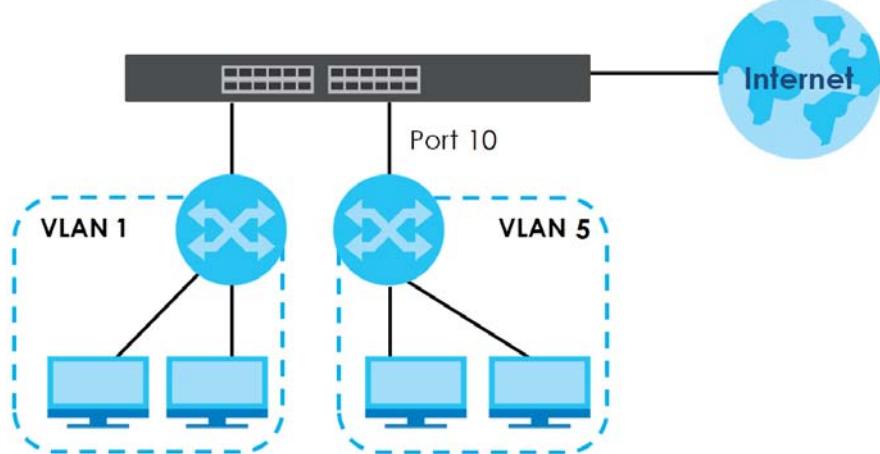
5.1.1 Creating a VLAN

VLANs confine broadcast frames to the VLAN group in which the port(s) belongs. You can do this with port-based VLAN or tagged static VLAN with fixed port members.

In this example, you want to configure port 10 as a member of VLAN 5.

See Table 21 on page 86 about mappings of VLAN ports and physical ports.

Figure 26 Initial Setup Network Example: VLAN



- 1 Click **Advanced Application > VLAN > Static VLAN** in the navigation panel.

- 2** In the **Static VLAN** screen, select **ACTIVE**, enter a descriptive name in the **Name** field, enter 2 in the **VLAN Group ID** field for the **VLAN5** network, and use the default VLAN type, **Normal**, in the **VLAN Type** field.

Port	Control	Tagging
1	Normal	<input checked="" type="checkbox"/> Tx Tagging
2	Normal	<input checked="" type="checkbox"/> Tx Tagging
3	Normal	<input checked="" type="checkbox"/> Tx Tagging
4	Normal	<input checked="" type="checkbox"/> Tx Tagging
5	Normal	<input checked="" type="checkbox"/> Tx Tagging
6	Normal	<input checked="" type="checkbox"/> Tx Tagging
7	Normal	<input checked="" type="checkbox"/> Tx Tagging
8	Normal	<input checked="" type="checkbox"/> Tx Tagging
9	Normal	<input checked="" type="checkbox"/> Tx Tagging
10	Normal	<input type="checkbox"/> Tx Tagging
11	Normal	<input checked="" type="checkbox"/> Tx Tagging
12	Normal	<input checked="" type="checkbox"/> Tx Tagging
21	Normal	<input checked="" type="checkbox"/> Tx Tagging
22	Normal	<input checked="" type="checkbox"/> Tx Tagging
23	Normal	<input checked="" type="checkbox"/> Tx Tagging
24	Normal	<input checked="" type="checkbox"/> Tx Tagging

Note: The **VLAN Group ID** field in this screen and the **VID** field in the **IP Setup** screen refer to the same VLAN ID.

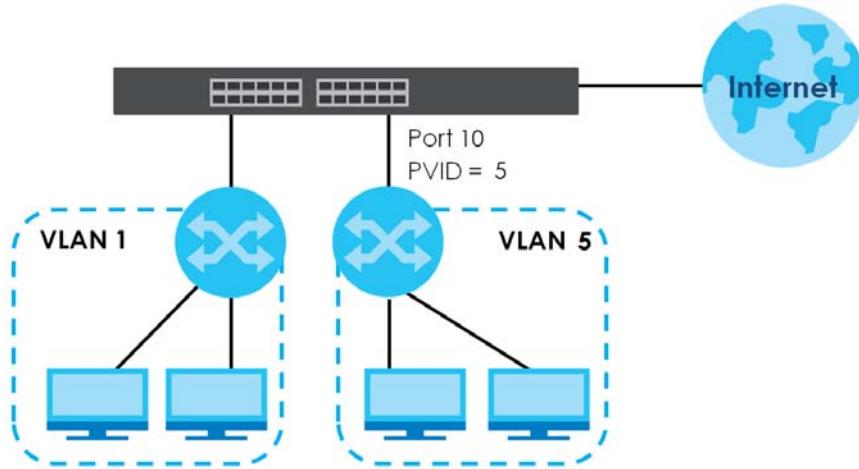
- 3** Since the **VLAN5** network is connected to port 10 on the OLT, select **Fixed** to configure port 10 to be a permanent member of the VLAN only.
- 4** To ensure that VLAN-unaware devices (such as computers and hubs) can receive frames properly, clear the **Tx Tagging** check box to set the OLT to remove VLAN tags before sending.
- 5** Click **Add** to save the settings to the run-time memory. Settings in the run-time memory are lost when the OLT's power is turned off.

5.1.2 Setting Port VID

Use PVID to add a tag to incoming untagged frames received on that port so that the frames are forwarded to the VLAN group that the tag defines.

In the example network, configure 5 as the port VID on port 10 so that any untagged frames received on that port get sent to VLAN 5.

See Table 21 on page 86 about mappings of VLAN ports and physical ports.

Figure 27 Initial Setup Network Example: Port VID

- 1 Click **Advanced Applications > VLAN > VLAN Port Setting** in the navigation panel.
- 2 Enter 5 in the **PVID** field for port 10 and click **Apply** to save your changes back to the run-time memory. Settings in the run-time memory are lost when the OLT's power is turned off.

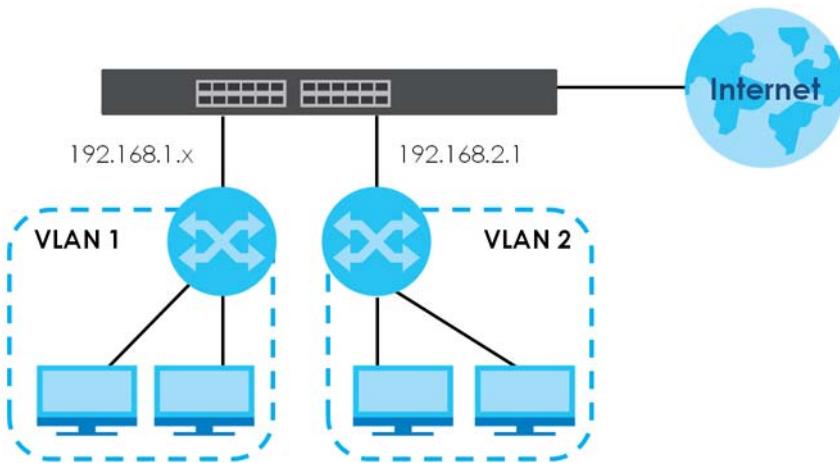
VLAN Port Setting

Port	Ingress Check	PVID	GVRP	Acceptable Frame Type	VLAN Trunking
*				All	
1		1		All	
2		1		All	
3		1		All	
4		1		All	
5		1		All	
6		1		All	
7		1		All	
8		1		All	
9		1		All	
10		5		All	
11		1		All	
12		1		All	
21		1		All	
22		1		All	
23		1		All	
24		1		All	

Apply Cancel

5.2 Configuring OLT Management IP Address

192.168.1.1 is the default in-band management IP address. You can configure another IP address in a different subnet for management purposes. The following figure shows an example.

Figure 28 Initial Setup Example: Management IP Address

- 1 Connect your computer to any Ethernet port on the OLT. Make sure your computer is in the same subnet as the OLT.
- 2 Open your web browser and enter 192.168.1.1 (the default in-band IP address) in the address bar to access the web configurator. See [Section 4.2 on page 51](#) for more information.
- 3 Click **Basic Setting > IP Setup** in the navigation panel.
- 4 Configure the related fields in the **IP Setup** screen.
- 5 For the **VLAN2** network, enter 192.168.2.1 as the IP address and 255.255.255.0 as the subnet mask.
- 6 In the **VID** field, enter the ID of the VLAN group to which you want this management IP address to belong. This is the same as the VLAN ID you configure in the **Static VLAN** screen.
- 7 Click **Add** to save your changes back to the run-time memory. Settings in the run-time memory are lost when the OLT's power is turned off.

Index	IP Address	IP Subnet Mask	VID	Delete
1	1.0.0.1	255.255.0.0	2	<input type="checkbox"/>
2	10.214.80.211	255.255.255.0	1	<input type="checkbox"/>
3	192.168.1.1	255.255.255.0	1	<input type="checkbox"/>

CHAPTER 6

Tutorials

6.1 Overview

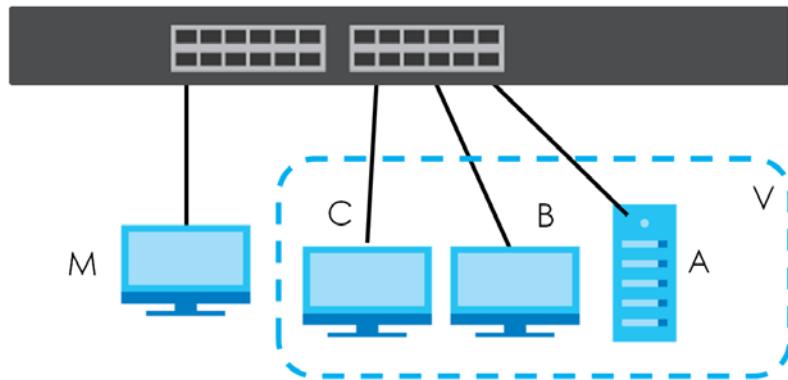
This chapter provides some examples of using the web configurator to set up and use the OLT. The tutorials include:

- How to Use DHCPv4 Snooping on the OLT
- How to Use DHCPv4 Relay on the OLT
- How to Use VLAN Stacking on PON Ports
- How to Use VLAN Stacking on ONTs
- How to Upgrade ONTs to the Latest Firmware via the OLT

6.2 How to Use DHCPv4 Snooping on the OLT

You only want DHCP server **A** connected to port 10 to assign IP addresses to all devices in VLAN network (**V**). Create a VLAN containing ports 10, 11 and 12. Connect a computer **M** to the OLT for management.

Figure 29 Tutorial: DHCP Snooping Tutorial Overview



Note: For related information about DHCP snooping, see [Section 23.1 on page 192](#).

The settings in this tutorial are as the following.

Table 9 Tutorial: Settings in this Tutorial

HOST	PORT CONNECTED	VLAN	PVID	DHCP SNOOPING PORT TRUSTED
DHCP Server (A)	10	1 and 100	100	Yes
DHCP Client (B)	11	1 and 100	100	No
DHCP Client (C)	12	1 and 100	100	No

- 1 Access the OLT through <http://192.168.1.1> by default. Log into the OLT by entering the username (default: **admin**) and password (default: **1234**).
- 2 Go to **Advanced Application > VLAN > Static VLAN**, and create a VLAN with ID of 100. Add ports 10, 11 and 12 in the VLAN by selecting **Fixed** in the **Control** field as shown.

Deselect **Tx Tagging** because you don't want outgoing traffic to contain this VLAN tag.

Click **Add**.

Figure 30 Tutorial: Create a VLAN and Add Ports to It

ACTIVE				VLAN Status
Name	VLAN-100			
VLAN Group ID	100			
Port	Control	Tagging		
*	Normal	<input checked="" type="checkbox"/> Tx Tagging		
1	Normal	<input type="radio"/>	Forbidden	<input checked="" type="checkbox"/> Tx Tagging
2	Normal	<input type="radio"/>	Forbidden	<input checked="" type="checkbox"/> Tx Tagging
3	Normal	<input type="radio"/>	Forbidden	<input checked="" type="checkbox"/> Tx Tagging
4	Normal	<input type="radio"/>	Forbidden	<input checked="" type="checkbox"/> Tx Tagging
5	Normal	<input type="radio"/>	Forbidden	<input checked="" type="checkbox"/> Tx Tagging
6	Normal	<input type="radio"/>	Forbidden	<input checked="" type="checkbox"/> Tx Tagging
7	Normal	<input type="radio"/>	Forbidden	<input checked="" type="checkbox"/> Tx Tagging
8	Normal	<input type="radio"/>	Forbidden	<input checked="" type="checkbox"/> Tx Tagging
9	Normal	<input type="radio"/>	Forbidden	<input checked="" type="checkbox"/> Tx Tagging
10	Normal	<input checked="" type="radio"/> Fixed	Forbidden	<input type="checkbox"/> Tx Tagging
11	Normal	<input checked="" type="radio"/> Fixed	Forbidden	<input type="checkbox"/> Tx Tagging
12	Normal	<input checked="" type="radio"/> Fixed	Forbidden	<input type="checkbox"/> Tx Tagging
13	Normal	<input type="radio"/>	Forbidden	<input checked="" type="checkbox"/> Tx Tagging
21	Normal	<input type="radio"/>	Forbidden	<input checked="" type="checkbox"/> Tx Tagging
22	Normal	<input type="radio"/>	Forbidden	<input checked="" type="checkbox"/> Tx Tagging
23	Normal	<input type="radio"/>	Forbidden	<input checked="" type="checkbox"/> Tx Tagging
24	Normal	<input type="radio"/>	Forbidden	<input checked="" type="checkbox"/> Tx Tagging

Add Cancel Clear

- 3 Go to **Advanced Application > VLAN > VLAN Configuration > VLAN Port Setting**, and set the PVID of the ports 10, 11 and 12 to 100. This tags untagged incoming frames on ports 10, 11 and 12 with the tag 100.

Figure 31 Tutorial: Tag Untagged Frames

Port	Ingress Check	PVID	GVRP	Acceptable Frame Type	VLAN Trunking
*	<input type="checkbox"/>		<input type="checkbox"/>	All	<input type="checkbox"/>
1	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
2	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
3	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
4	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
5	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
6	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
7	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
8	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
9	<input type="checkbox"/>			All	<input type="checkbox"/>
10	<input type="checkbox"/>	100	<input type="checkbox"/>	All	<input type="checkbox"/>
11	<input type="checkbox"/>	100	<input type="checkbox"/>	All	<input type="checkbox"/>
12	<input type="checkbox"/>	100	<input type="checkbox"/>	All	<input type="checkbox"/>
13	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
22	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
23	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
24	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>

Apply **Cancel**

- 4 Go to **Advanced Application > IP Source Guard > DHCP Snooping > Configure**, activate and specify VLAN 100 as the DHCP VLAN as shown. Click **Apply**.

Figure 32 Tutorial: Specify DHCP VLAN

DHCP Snooping Configure

<input checked="" type="checkbox"/> Active	<input type="radio"/> Disable
DHCP Vlan <input type="text" value="100"/>	

Database

Agent URL		
Timeout interval	300	seconds
Write delay interval	300	seconds

Renew DHCP Snooping URL

- 5 Click the **Port** link at the top right corner.

Port **VLAN** **DHCP Snooping**

- 6 The **DHCP Snooping Port Configure** screen appears. Select **Trusted** in the **Server Trusted state** field for port 10 because the DHCP server is connected to port 10. Keep ports 11 and 12 **Untrusted** because they are connected to DHCP clients. Click **Apply**.

Figure 33 Tutorial: Set the DHCP Server Port to Trusted

Port	Server Trusted state	Rate (pps)
*	Untrusted ▾	
1	Untrusted ▾	0
2	Untrusted ▾	0
3	Untrusted ▾	0
4	Untrusted ▾	0
5	Untrusted ▾	0
6	Untrusted ▾	0
7	Untrusted ▾	0
8	Untrusted ▾	0
9	Untrusted ▾	0
10	Trusted ▾	0
11	Untrusted ▾	0
12	Untrusted ▾	0
13	Untrusted ▾	0
21	Untrusted ▾	0
22	Untrusted ▾	0
23	Untrusted ▾	0
24	Untrusted ▾	0

Apply | **Cancel**

- 7 Go to **Advanced Application > IP Source Guard > DHCP Snooping > Configure > VLAN**, show VLAN 100 by entering 100 in the **Start VID** and **End VID** fields and click **Apply**. Then select **Yes** in the **Enabled** field of the VLAN 100 entry shown at the bottom section of the screen.

If you want to add more information in the DHCP request packets such as source VLAN ID or system name, you can also select an **Option82 Profile** in the entry. See [Section 23.10.1.3 on page 210](#).

Figure 34 Tutorial: Enable DHCP Snooping on this VLAN

Show VLAN	Start VID	End VID
	100	100

Apply

VID	Enabled	Option82	Information
*	No ▾	<input type="checkbox"/>	<input type="checkbox"/>
100	Yes ▾	<input type="checkbox"/>	<input type="checkbox"/>

Apply | **Cancel**

- 8 Click **Save** at the top right corner of the web configurator to save the configuration permanently.



- 9 Connect your DHCP server to port 10 and a computer (as DHCP client) to either port 11 or 12. The computer should be able to get an IP address from the DHCP server. If you put the DHCP server on port 11 or 12, the computer will not be able to get an IP address.
- 10 To check if DHCP snooping works, go to **Advanced Application > IP Source Guard > IPv4 Source Guard Setup**, you should see an IP assignment with the type **DHCP-Snooping** as shown.

Figure 35 Tutorial: Check the Binding If DHCP Snooping Works

Index	MAC Address	IP Address	Lease	Type	VLAN	Port
1	00:02:00:00:00:1C	10.10.1.16	6d23h17m0s	dhcp-snooping	100	7

You can also telnet or log into the OLT's console. Use the command "show dhcp snooping binding" to see the DHCP snooping binding table as shown next.

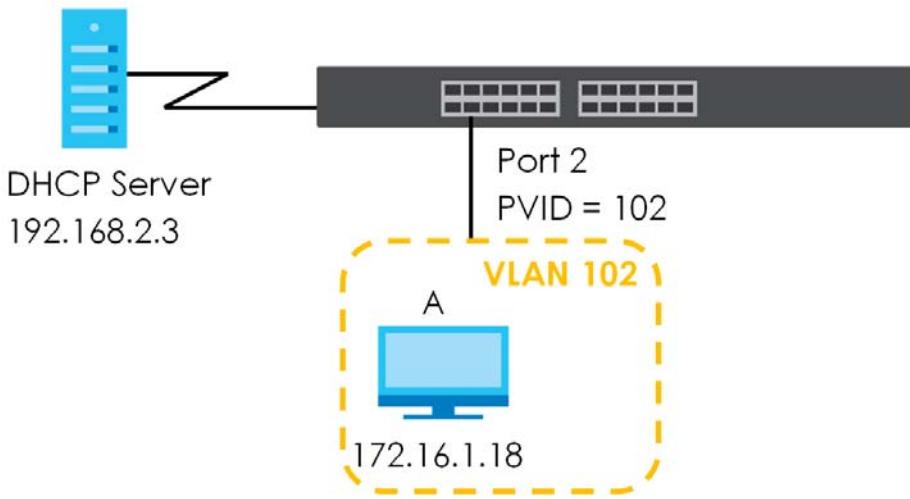
```
sysname# show dhcp snooping binding
MacAddress          IpAddress          Lease           Type      VLAN    Port
-----
00:02:00:00:00:1c   10.10.1.16       6d23h59m20s  dhcp-snooping 100     11
Total number of bindings: 1
```

6.3 How to Use DHCPv4 Relay on the OLT

This tutorial describes how to configure your OLT to forward DHCP client requests to a specific DHCP server. The DHCP server can then assign a specific IP address based on the information in the DHCP requests.

6.3.1 DHCP Relay Tutorial Introduction

In this example, you have configured your DHCP server (192.168.2.3) and want to have it assign a specific IP address (say 172.16.1.18) to DHCP client **A** based on the system name, VLAN ID and port number in the DHCP request. Client **A** connects to the OLT's port 2 in VLAN 102.

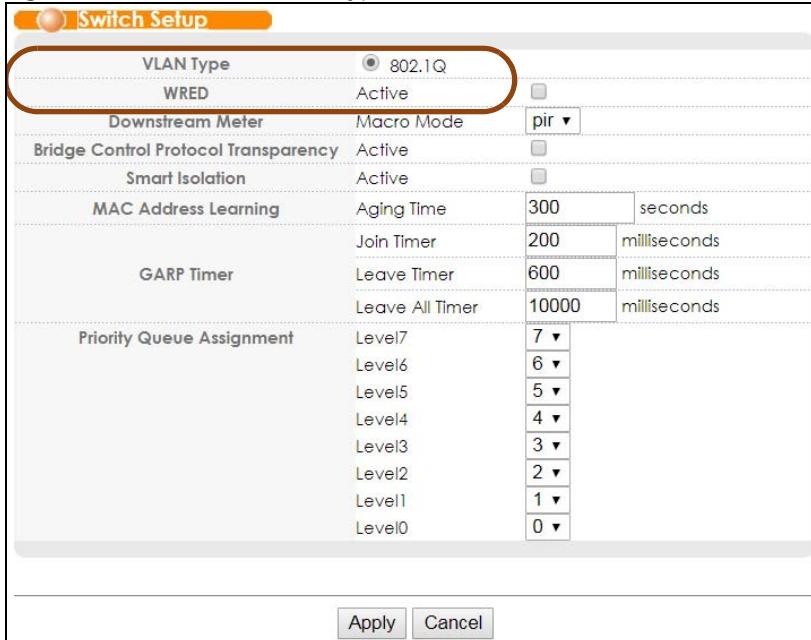
Figure 36 Tutorial: DHCP Relay Scenario

6.3.2 Creating a VLAN

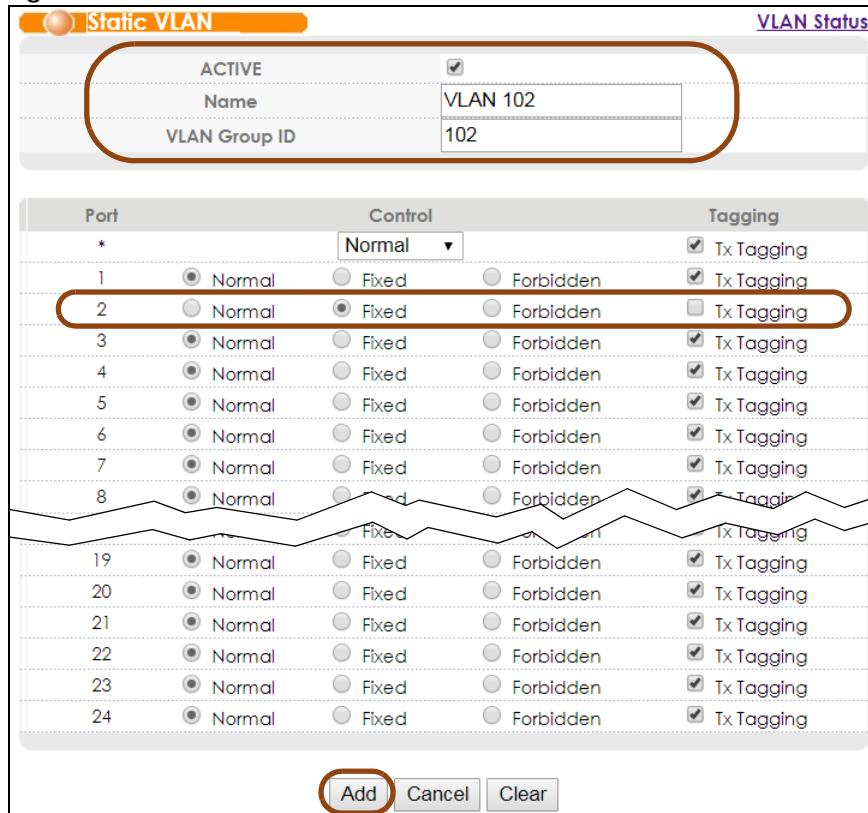
Follow the steps below to configure port 2 as a member of VLAN 102.

- 1 Access the web configurator through the OLT's management port.
- 2 Go to **Basic Setting > Switch Setup** and set the VLAN type to **802.1Q**. Click **Apply** to save the settings to the run-time memory.

Figure 37 Tutorial: Set VLAN Type to 802.1Q



- 3 Click **Advanced Application > VLAN > Static VLAN**.
- 4 In the **Static VLAN** screen, select **ACTIVE**, enter a descriptive name (VLAN 102 for example) in the **Name** field and enter 102 in the **VLAN Group ID** field. Select **Fixed** to configure port 2 to be a permanent member of this VLAN.
- 5 Clear the **TX Tagging** check box to set the OLT to remove VLAN tags before sending.
- 6 Click **Add** to save the settings to the run-time memory. Settings in the run-time memory are lost when the OLT's power is turned off.

Figure 38 Tutorial: Create a Static VLAN

- 7 Click the **VLAN Port Setting** link in the **VLAN Status** screen.
- 8 Enter 102 in the **PVID** field for port 2 to add a tag to incoming untagged frames received on that port so that the frames are forwarded to the VLAN group that the tag defines.
- 9 Click **Apply** to save your changes back to the run-time memory.

Figure 39 Tutorial: Add Tag for Frames Received on Port 2

VLAN Port Setting	Subnet Based Vlan	Protocol Based Vlan	VLAN Status		
GVRP	<input type="checkbox"/>				
Port Isolation	<input type="checkbox"/>				
<hr/>					
Port	Ingress Check	PVID	GVRP	Acceptable Frame Type	VLAN Trunking
*	<input type="checkbox"/>		<input type="checkbox"/>	All	<input type="checkbox"/>
1	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
2	<input checked="" type="checkbox"/>	102	<input type="checkbox"/>	All	<input type="checkbox"/>
3	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
4	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
5	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
6	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
7	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
8	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
19	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
20	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
21	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
22	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
23	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
24	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>

Apply **Cancel**

- Click the **Save** link in the upper right corner of the web configurator to save your configuration permanently.

6.3.3 Configuring DHCPv4 Relay

Follow the steps below to enable DHCP relay on the OLT and allow the OLT to add relay agent information (such as the VLAN ID) to DHCP requests.

- Click **IP Application > DHCP** and then the **Global** link to open the **DHCP Relay** screen.
- Select the **Active** check box.
- Enter the DHCP server's IP address (192.168.2.3 in this example) in the **Remote DHCP Server 1** field.
- Click **Apply** to save your changes back to the run-time memory.

Figure 40 Tutorial: Set DHCP Server and Relay Information

DHCP Relay		Status
Active		<input checked="" type="checkbox"/>
Remote DHCP Server 1	192.168.2.3	
Remote DHCP Server 2	0.0.0.0	
Remote DHCP Server 3	0.0.0.0	
Relay Agent Information		
Format	<input type="checkbox"/> Option 82 <input type="checkbox"/> Format <input type="checkbox"/> OLT1404A	
Information		
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

- 5 Click the **Save** link in the upper right corner of the web configurator to save your configuration permanently.
- 6 The DHCP server can then assign a specific IP address based on the DHCP request.

6.3.4 Troubleshooting

Check the client **A**'s IP address. If it did not receive the IP address 172.16.1.18, make sure:

- 1 Client **A** is connected to the OLT's port 2 in VLAN 102.
- 2 You configured the correct VLAN ID, port number and system name for DHCP relay on both the DHCP server and the OLT.
- 3 You clicked the **Save** link on the OLT to have your settings take effect.

6.4 How to Use VLAN Stacking on PON Ports

This tutorial introduces how to configure VLAN stacking for all VLANs and specified VLAN on PON ports.

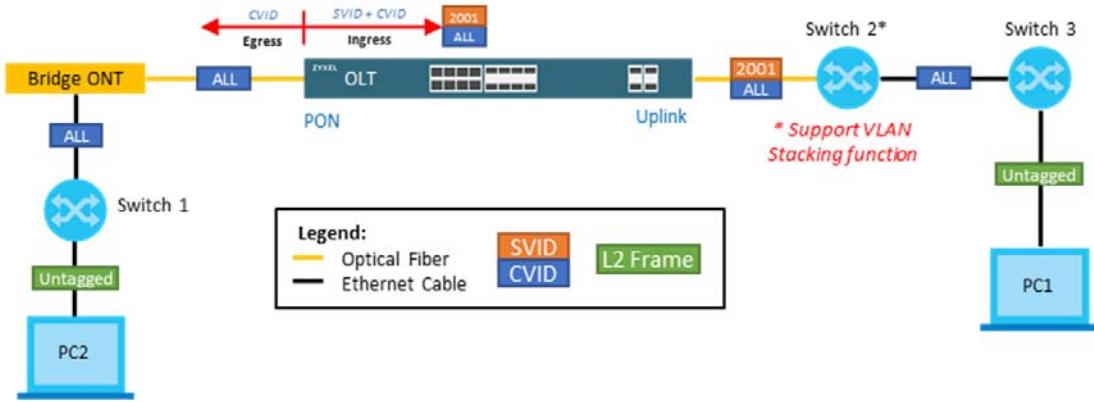
6.4.1 Apply VLAN Stacking to All VLANs

Scenario

PC2 transmits untagged VLAN traffic to **Switch 1**. **Switch 1** adds the VLAN tag and forwards the tagged packets to the ONT. The ONT forwards the tagged packets that are VLAN members on the UNI port to the OLT. The OLT receives the single-tagged packets from multiple VLANs. The OLT will add an outer tag (**2001**) to the incoming packets and forward the double-tagged packets to the uplink.

The OLT will only process the outer VLAN ID (**2001**). All inner VLAN IDs will be transparent in the OLT forwarding process.

Figure 41 Tutorial: VLAN Stacking for All VLANs on PON Ports



- 1 Create the VLAN in the OLT and assign member ports.

```
(config)# vlan 2001
(config-vlan)# fixed eth-1
(config-vlan)# fixed pon-1
(config-vlan)# untagged pon-1
(config-vlan)# exit
```

- 2 Enter the SPVID (service provider VLAN ID) 2001 on a PON port, and have it act as an access port.

```
# configure
(config)# interface port-channel pon-1
(config-interface)# vlan-stacking SPVID 2001
(config-interface)# vlan-stacking role access
(config-interface)# exit
```

- 3 Have an uplink port act as a tunnel port.

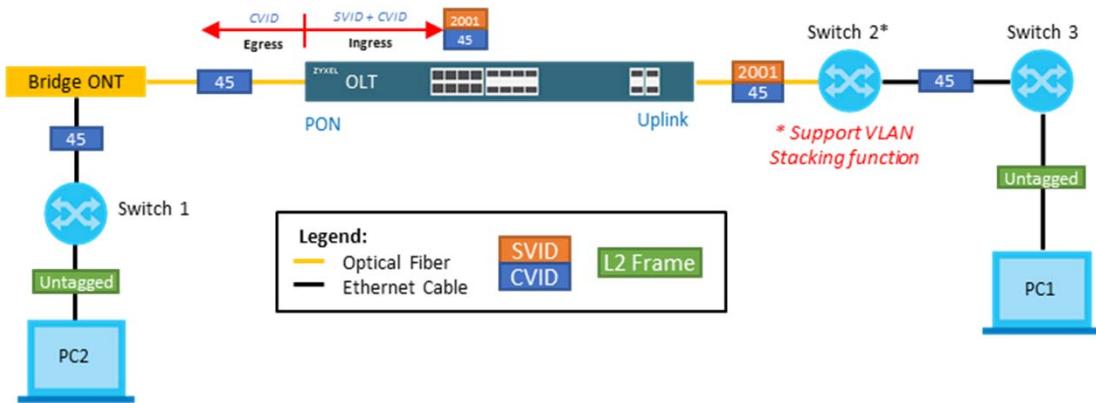
```
(config)# interface port-channel eth-1
(config-interface)# vlan-stacking role tunnel
(config-interface)# exit
(config)# exit
```

6.4.2 Apply VLAN Stacking to Specific VLANs

Scenario

PC2 transmits untagged VLAN traffic to **Switch 1**. **Switch 1** adds the VLAN tag and forwards the tagged packets to the ONT. The ONT forwards the tagged packets that are VLAN members on the UNI port to the OLT. The OLT receives the single-tagged packets from the specified VLAN (VID 45). The OLT will add an outer tag (**2001**) to the incoming packets and forward the double-tagged packets to the uplink.

The OLT will only process the outer VLAN ID (**2001**). The inner VLAN ID **45** will be transparent in the OLT forwarding process.

Figure 42 Tutorial: VLAN Stacking for All VLANs on PON Ports

- 1 Create the VLAN in the OLT and assign member ports.

```
(config)# vlan 2001
(config-vlan)# fixed eth-1
(config-vlan)# fixed pon-1
(config-vlan)# exit
```

- 2 Configure VLAN translation on a UNI port of the OLT.

```
# configure
(config)# interface uni-port pon-1
(config-uniport)# vlan-translation name vlan45to2001:45 ing-ovid 45 egr-svid
2001 egr-cvid 45
(config-uniport)# vlan-translation
```

6.5 How to Use VLAN Stacking on ONTs

This tutorial introduces how to configure VLAN stacking for all VLANs and specified VLAN on the ONTs connected to the PON ports.

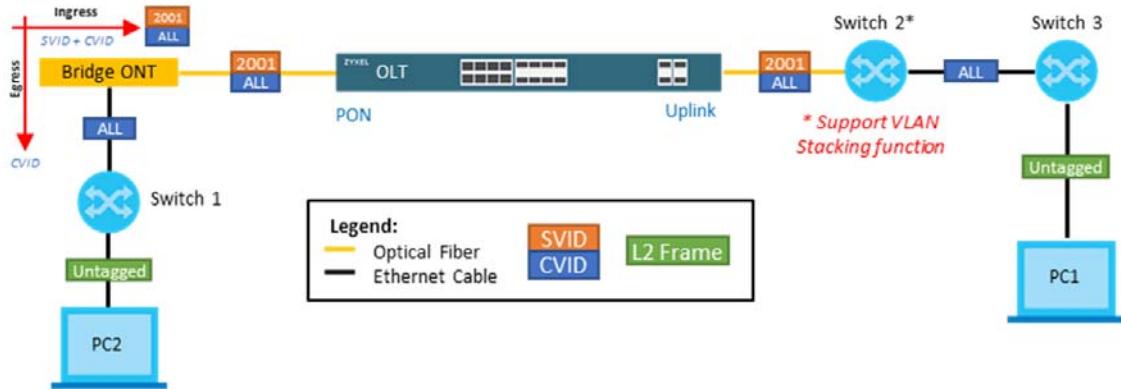
6.5.1 Apply VLAN Stacking to All VLANs

Scenario

PC2 transmits untagged VLAN traffic to **Switch 1**. **Switch 1** adds the VLAN tag and forwards the tagged packets to the ONT.

The ONT receives the single-tagged packets from multiple VLANs. The ONT verifies that the single-tagged packets are the VLAN members on the UNI port. The ONT will add an outer tag (2001) to the incoming packets and forward the double-tagged packets to the OLT.

The OLT will only process the outer VLAN ID (2001). All inner VLAN IDs will be transparent in the OLT forwarding process.

Figure 43 Tutorial: VLAN Stacking for All VLANs on ONTs

- Configure VLAN stacking on a remote UNI port.

```
# config
(config)# remote uniport uniport-1-1-1-1
(config-remote-giga-uniport)# queue tc 1 p 0 w 0 us DEFVAL ds DEFVAL dsopt
olt bw 1
(config-remote-giga-uniport)# vlan all network 2001:all ing DEFVAL
(config-remote-giga-uniport)# no inactive
(config-remote-giga-uniport)# exit
```

- Create the VLAN in the OLT and assign member ports.

```
(config)# vlan 2001
(config-vlan)# fixed eth-1
(config-vlan)# fixed pon-1
(config-vlan)# exit
```

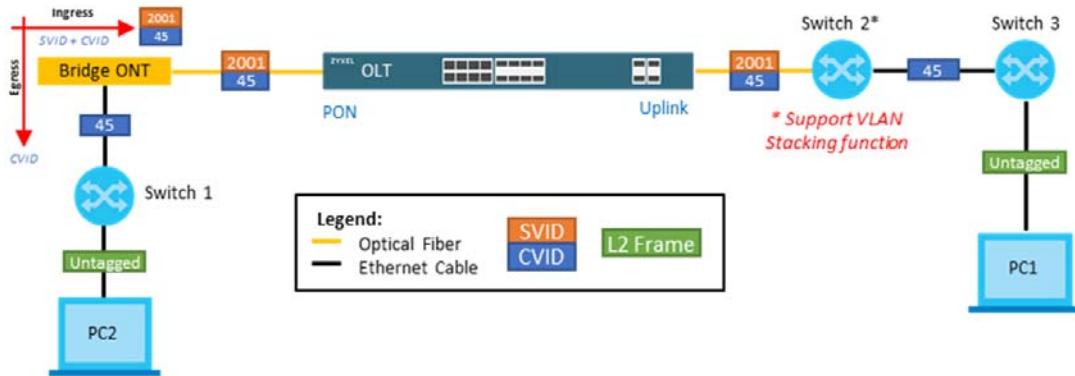
6.5.2 Apply VLAN Stacking to Specific VLANs

Scenario

PC2 transmits untagged VLAN traffic to **Switch 1**. **Switch 1** adds the VLAN tag and forwards the tagged packets to the ONT.

The ONT receives the single-tagged packets from the specified VLAN (VID 45). The ONT verifies that the single-tagged packets are the VLAN members on the UNI port. The ONT will add an outer tag (2001) to the incoming packets and forward the double-tagged packets to the OLT.

The OLT will only process the outer VLAN ID (2001). The inner VLAN ID 45 will be transparent in the OLT forwarding process.

Figure 44 Tutorial: VLAN Stacking for All VLANs on ONTs

- 1 Configure VLAN stacking on a remote UNI port.

```
# config
(config)# remote uniport uniport-1-1-1-1
(config-remote-giga-uniport)# queue tc 1 p 0 w 0 us DEFVAL ds DEFVAL dsopt
olt bw 1
(config-remote-giga-uniport)# vlan 45 network 2001:45 ing DEFVAL
(config-remote-giga-uniport)# no inactive
(config-remote-giga-uniport)# exit
```

Note: If VLANs are not defined in the UNI port, incoming packets will be dropped.

- 2 Create the VLAN in the OLT and assign member ports.

```
(config)# vlan 2001
(config-vlan)# fixed eth-1
(config-vlan)# fixed pon-1
(config-vlan)# exit
```

6.6 How to Upgrade ONTs to the Latest Firmware via the OLT

This tutorial introduces you how to upgrade an ONT or the ONTs connected to a PON port to the latest firmware via the OLT.

- 1 Select **Start > All Programs > Accessories > Command Prompt**.
- 2 The OLT is an FTP server. Use the `ftp <ip address>` command and enter the OLT IP address to have your computer ping the OLT. In this example, we use the default out-of-band IP address (**192.168.0.1**) for the OLT IP address.

Use the default in-band management IP address (192.168.1.1), DHCP-assigned IP address, static IP address, or the default out-of-band IP address (192.168.0.1). It doesn't matter which IP address you use as long as your computer can ping the OLT.

- 3 Enter the login username and password of the OLT. The default username is **admin** and associated default password is **1234**.
- 4 Enter the `put <file name> ont` command to upload the ONT firmware file to the OLT.

Figure 45 Tutorial: Upload an ONT Firmware File to the OLT

```
C:\Documents and Settings\BBASW4>ftp 192.168.0.1
Connected to 192.168.0.1.
220 OLT2412 FTP version 1.0 ready at Thu Jan 1 00:16:56 1970
User (192.168.0.1:(none)): admin
331 Enter PASS command
Password:
230 Logged in
ftp> put "ont.img" ont
200 Port command okay
150 Opening data connection for STOR ont
226 File received OK
ftp: 12646372 bytes sent in 5.36Seconds 2359.40Kbytes/sec.
ftp> by
```

- 5 Use the `mgmt-ont-img set image-version <version>` command to set the image version of the ONT firmware file uploaded to the OLT. In this example, we use **testVersion** as the image version. Enter a string of up to 14 characters.
See [Table 307 on page 588](#) for more information about this command.
- 6 Use the `mgmt-ont-img disp image-info` to check if the image version of the ONT firmware file was updated successfully.

Figure 46 Tutorial: Set Image Version

```
OLT1408A(mgmt-ont-img)# set image-version testVersion
OLT1408A(mgmt-ont-img)# disp image-info
The onu image version
Image head address: 47784300
Image version: testVersion
Image size: c0f7e4
Image content address: 27051956
OLT1408A(mgmt-ont-img)# exit
```

- 7 Use the `remote ont <aid> plan-version <version>` command to set the ONT planned version. We use an ONT 1 of **PON3** as an example.
See [Table 306 on page 581](#) for more information about this command.
The `<version>` values of the following commands must be identical, so the ONT can download firmware via the OLT.

- `mgmt-ont-img set imageversion <version>`
- `remote ont <aid> plan-version <version>`

Figure 47 Tutorial: Set ONT's Planned Version

```
OLT1408A# config
OLT1408A(config)# interface olt pon-3
OLT1408A(config-olt)# register-method A
OLT1408A(config-olt)# exit
OLT1408A(config-ont)# remote ont ont-3-1
OLT1408A(config-ont)# sn 414C434C00000082
OLT1408A(config-ont)# password 44454641554C544D4455
OLT1408A(config-ont)# plan-version testVersion
OLT1408A(config-ont)# no inactive
OLT1408A(config-ont)# exit
OLT1408A(config)# exit
```

- 8** Use the `remote ont <aid> check-version` command to upgrade the ONT to the latest firmware via the OLT.

See [Table 307 on page 588](#) for more information about this command.

Figure 48 Tutorial: Upgrade Firmware

```
OLT1408A# remote ont ont-3-1 check-version
OLT1408A# ONU[3- 1] Start do software download to image(1):
testVersion!
```

- 9** Use the `mgmt-ont-img disp queue` command to check the waiting queue's status for firmware upgrades.

Figure 49 Tutorial: Waiting Queue's Status

```
OLT1408A# mgmt-ont-img
OLT1408A# disp queue
+-----+
| | software download table |
+-----+
| 1 || ont-3-1 | downloading |
+-----+
There are Total 1 ont in queue, show queue size is 128.
```

- 10** Use the `mgmt-ont-img disp upgrade-status <aid>` command to check the firmware upgrade result.

See [Table 307 on page 588](#) for more information about this command.

Figure 50 Tutorial: Firmware Upgrade Result

```
OLT1408A# mgmt-ont-img  
OLT1408A# disp upgrade-status ont-3-1
```

Upgrade Status Table	
+	+
	Successful
+	+

If there are ont want to be did fw-upgrade again and the ont status is

"Already successful", "Already changed to image(1) or "Already changed to image(2)".

then you must clear the ont status by the cli

"(mgmt-ont-img)# clear upgrade-status" and the ont can be did fw-upgrade again.

- 11** Use the `remote ont <aid> onu-reboot <cr>|<1>|<2>` command to reboot the ONT, and select the firmware that was updated when the ONT was downloading firmware via the OLT.
Note that the standby firmware of the ONT will be updated when the ONT is downloading firmware via the OLT.

Figure 51 Tutorial: ONT Reboot

```
OLT1408A# remote ont ont-3-1 onu-reboot  
ont-3-1 Waiting ONU reboot
```

CHAPTER 7

Status

7.1 Overview

This chapter describes the screen for System Status.

7.1.1 What You Can Do

- Use the **Status** screen (Section 7.2 on page 79) to see the port statistics.

7.2 Status

The **Status** screen displays when you log into the OLT or click **Status** at the top right corner of the web configurator. The **Status** screen displays a port statistical summary with links to each port showing statistical details.

Figure 52 Status

Port Status											
Port	Name	Link	State	LACP	TxPkts	RxPkts	Errors	Tx KB/s	Rx KB/s	Up Time	Clear Counter
*											<input checked="" type="checkbox"/>
eth-1		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00	<input checked="" type="checkbox"/>
eth-2		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00	<input checked="" type="checkbox"/>
eth-3		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00	<input checked="" type="checkbox"/>
eth-4		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00	<input checked="" type="checkbox"/>
eth-5		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00	<input checked="" type="checkbox"/>
eth-6		1000M/F	FORWARDING	Disabled	27025	50038	0	0.217	0.326	3:11:12	<input checked="" type="checkbox"/>
eth-7		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00	<input checked="" type="checkbox"/>
eth-8		1000M/F	FORWARDING	Disabled	38464	28379	0	12.52	2.52	0:43:53	<input checked="" type="checkbox"/>
eth-9		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00	<input checked="" type="checkbox"/>
eth-10		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00	<input checked="" type="checkbox"/>
eth-11		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00	<input checked="" type="checkbox"/>
eth-12		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00	<input checked="" type="checkbox"/>
eth-13		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00	<input checked="" type="checkbox"/>
eth-14		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00	<input checked="" type="checkbox"/>
eth-15		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00	<input checked="" type="checkbox"/>
eth-16		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00	<input checked="" type="checkbox"/>
eth-17		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00	<input checked="" type="checkbox"/>
eth-18		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00	<input checked="" type="checkbox"/>
eth-19		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00	<input checked="" type="checkbox"/>

The following table describes the labels in this screen.

Table 10 Port Status

LABEL	DESCRIPTION
Port	This identifies the Ethernet and PON ports. Click a port number to display the Port Details screen (refer to Figure 53 on page 81).
Name	This is the name you assigned to this port in the Basic Setting > Port Setup screen.
Link	This field displays the speed (either 100M for 100Mbps, 1000M for 1000Mbps, 2.5G for 2.5 Gbps, or 10G for 10 Gbps) and the duplex (F for full duplex or H for half). This field displays Down if the port is not connected to any device.
State	If STP (Spanning Tree Protocol) is enabled, this field displays the STP state of the port. See page 131 for more information. If STP is disabled, this field displays FORWARDING if the link is up, otherwise, it displays STOP . When LACP (Link Aggregation Control Protocol), STP, and dot1x are in blocking state, it displays Blocking .
LACP	This field displays whether LACP (Link Aggregation Control Protocol) has been enabled on the port.
TxPkts	This field shows the number of transmitted frames on this port.
RxPkts	This field shows the number of received frames on this port.
Errors	This field shows the number of received errors on this port.
Tx KB/s	This field shows the number of kilobytes per second transmitted on this port.
Rx KB/s	This field shows the number of kilobytes per second received on this port.
Up Time	This field shows the total amount of time in hours, minutes and seconds the port has been up.
Clear Counter	Select Port , enter a port number and then click Clear Counter to erase the recorded statistical information for that port, or select Any to clear statistics for all ports.

7.2.1 Port Details

Click a number in the **Port** column in the **Port Status** screen to display individual port statistics. Use this screen to check status and detailed performance data about an individual port on the OLT.

Figure 53 Port Status: Port Details

Port Details		Port Status
Port Info	Port NO.	eth-1
	Name	
	Link	Down
	Status	STOP
	LACP	Disabled
	TxPkts	0
	RxPkts	0
	Errors	0
	Tx KBs/s	0.0
	Rx KBs/s	0.0
	Up Time	0:00:00
TX Packet	Unicast	0
	Multicast	0
	Broadcast	0
	Pause	0
	Tagged	0
RX Packet	Unicast	0
	Multicast	0
	Broadcast	0
	Pause	0
	Control	0
TX Collision	Single	0
	Multiple	0
	Excessive	0
	Late	0
Error Packet	RX CRC	0
	Length	0
	Runt	0
Distribution	64	0
	65 to 127	0
	128 to 255	0
	256 to 511	0
	512 to 1023	0
	1024 to 1518	0
	Giant	0

The following table describes the labels in this screen.

Table 11 Port Status: Port Details

LABEL	DESCRIPTION
Port Info	
Port NO.	This field displays the port number you are viewing.
Name	This field displays the name of the port.
Link	This field displays the speed (such as 100M for 100Mbps, 1000M for 1000 Mbps, 2.5G for 2.5 Gbps, or 10G for 10 Gbps) and the duplex (F for full duplex or H for half). This field displays Down if the port is not connected to any device.
State	If STP (Spanning Tree Protocol) is enabled, this field displays the STP state of the port (see Chapter 13 on page 116 for more information). If STP is disabled, this field displays FORWARDING if the link is up, otherwise, it displays STOP .
LACP	This field shows if LACP is enabled on this port or not.
TxPkts	This field shows the number of transmitted frames on this port
RxPkts	This field shows the number of received frames on this port

Table 11 Port Status: Port Details (continued)

LABEL	DESCRIPTION
Errors	This field shows the number of received errors on this port.
Tx KBs/s	This field shows the transmission speed of data sent on this port in kilobytes per second.
Rx KBs/s	This field shows the transmission speed of data received on this port in kilobytes per second.
Up Time	This field shows the total amount of time the connection has been up.
Tx Packet	The following fields display detailed information about packets transmitted.
Unicast	This field shows the number of good unicast packets transmitted.
Multicast	This field shows the number of good multicast packets transmitted.
Broadcast	This field shows the number of good broadcast packets transmitted.
Pause	This field shows the number of 802.3x Pause packets transmitted.
Tagged	This field shows the number of packets with VLAN tags transmitted.
Rx Packet	The following fields display detailed information about packets received.
Unicast	This field shows the number of good unicast packets received.
Multicast	This field shows the number of good multicast packets received.
Broadcast	This field shows the number of good broadcast packets received.
Pause	This field shows the number of 802.3x Pause packets received.
Control	This field shows the number of control packets received (including those with CRC error) but it does not include the 802.3x Pause packets.
TX Collision	The following fields display information on collisions while transmitting.
Single	This is a count of successfully transmitted packets for which transmission is inhibited by exactly one collision.
Multiple	This is a count of successfully transmitted packets for which transmission was inhibited by more than one collision.
Excessive	This is a count of packets for which transmission failed due to excessive collisions. Excessive collision is defined as the number of maximum collisions before the retransmission count is reset.
Late	This is the number of times a late collision is detected, that is, after 512 bits of the packets have already been transmitted.
Error Packet	The following fields display detailed information about packets received that were in error.
RX CRC	This field shows the number of packets received with CRC (Cyclic Redundant Check) error(s).
Length	This field shows the number of packets received with a length that was out of range.
Runt	This field shows the number of packets received that were too short (shorter than 64 octets), including the ones with CRC errors.
Distribution	
64	This field shows the number of packets (including bad packets) received that were 64 octets in length.
65 to 127	This field shows the number of packets (including bad packets) received that were between 65 and 127 octets in length.
128 to 255	This field shows the number of packets (including bad packets) received that were between 128 and 255 octets in length.
256 to 511	This field shows the number of packets (including bad packets) received that were between 256 and 511 octets in length.

Table 11 Port Status: Port Details (continued)

LABEL	DESCRIPTION
512 to 1023	This field shows the number of packets (including bad packets) received that were between 512 and 1023 octets in length.
1024 to 1518	This field shows the number of packets (including bad packets) received that were between 1024 and 1518 octets in length.
Giant	This field shows the number of packets (including bad packets) received that were between 1519 octets and the maximum frame size. The maximum frame size varies depending on your OLT model.

CHAPTER 8

Basic Setting

8.1 Overview

This chapter describes how to configure the **System Info**, **General Setup**, **Switch Setup**, **IP Setup**, and **Port Setup** screens.

8.1.1 What You Can Do

- Use the **System Info** screen ([Section 8.2 on page 84](#)) to check the firmware version number. Also, you can check the hardware status, such as the temperature, fan speed, and power supply voltage of the OLT.
- Use the **General Setup** screen ([Section 8.3 on page 86](#)) to configure general settings such as the system name and time.
- Use the **Switch Setup** screen ([Section 8.5 on page 88](#)) to choose your VLAN type, set the GARP timers and assign priorities to queues.
- Use the **IP Setup** screen ([Section 8.6 on page 90](#)) to configure the OLT IP address, default gateway device, and the management VLAN ID.
- Use the **Port Setup** screen ([Section 8.7 on page 92](#)) to configure OLT port settings.

8.2 System Information

In the navigation panel, click **Basic Setting** > **System Info** to display the screen as shown. Use this screen to view general system information. You can check the firmware version number. Also, you can check the hardware status, such as the temperature, fan speed, and power supply voltage of the OLT.

Figure 54 Basic Setting > System Info

System Info									
System Name		OLT1404A							
Product Model		OLT1404A							
ZyNOS F/W Version		V4.02(AAJB.1) 2018-06-04							
Ethernet Address		5cf:4:ab:9c:e7:58							
Hardware Monitor									
Temperature Unit C ▾									
Temperature (C)	Current	MAX	MIN	Threshold	Status				
CPU	65.0	65.0	34.0	95.0	Normal				
PON_MAC	65.0	66.0	26.0	92.0	Normal				
SWITCH	89.0	89.0	31.0	94.0	Normal				
FAN Speed (RPM)	Current	MAX	MIN	Threshold	Status				
FAN1	< 41	0	0	2600	Error				
FAN2	< 41	0	0	2600	Error				
FAN3	< 41	0	0	2600	Error				
FAN4	< 41	0	0	2600	Error				
Voltage (V)	Current	MAX	MIN	Threshold	Status				
+1V	1.035	1.035	1.035	+/-7%	Normal				
+1V_PON	1.013	1.013	1.013	+/-7%	Normal				
+1.8V	1.809	1.835	1.809	+/-7%	Normal				
+3.3V	3.342	3.342	3.342	+/-7%	Normal				
+15V	14.936	14.936	14.812	+/-7%	Normal				

The following table describes the labels in this screen.

Table 12 Basic Setting > System Info

LABEL	DESCRIPTION
System Name	This field displays the descriptive name of the OLT for identification purposes.
Product Model	This field displays the product model of the OLT. Use this information when searching for firmware upgrade or looking for other support information in the website.
ZyNOS F/W Version	This field displays the version number of the OLT's current firmware including the date created.
Ethernet Address	This field refers to the Ethernet MAC (Media Access Control) address of the OLT.
Hardware Monitor	
Temperature Unit	The OLT has temperature sensors that are capable of detecting and reporting if the temperature rises above the threshold. You may choose the temperature unit (Centigrade or Fahrenheit) in this field.
Temperature (C)	CPU, PON_MAC and SWITCH refer to the location of the temperature sensors on the OLT printed circuit board.
Current	This shows the current temperature at this sensor.
MAX	This field displays the maximum temperature measured at this sensor when the OLT was first turned on.
MIN	This field displays the minimum temperature measured at this sensor when the OLT was first turned on.
Threshold	This field displays the upper temperature limit at this sensor.
Status	This field displays Normal for temperatures below the threshold and Error for those above.
Fan Speed (RPM)	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 is capable of detecting and reporting if the fan speed falls below the threshold shown.
Current	This field displays this fan's current speed in Revolutions Per Minute (RPM).
MAX	This field displays this fan's maximum speed measured in Revolutions Per Minute (RPM) when the OLT was first turned on.

Table 12 Basic Setting > System Info (continued)

LABEL	DESCRIPTION
MIN	This field displays this fan's minimum speed measured in Revolutions Per Minute (RPM) when the OLT was first turned on. "<41" is displayed for speeds too small to measure (under 2000 RPM).
Threshold	This field displays the minimum speed at which a normal fan should work.
Status	Normal indicates that this fan is functioning above the minimum speed. Error indicates that this fan is functioning below the minimum speed.
Voltage(V)	The power supply for each voltage has a sensor that is capable of detecting and reporting if the voltage falls out of the tolerance range.
Current	This is the current voltage reading.
MAX	This field displays the maximum voltage measured when the OLT was first turned on.
MIN	This field displays the minimum voltage measured when the OLT was first turned on.
Threshold	This field displays the percentage tolerance of the voltage with which the OLT still works.
Status	Normal indicates that the voltage is within an acceptable operating range at this point; otherwise Error is displayed.

8.3 General Setup

Use this screen to configure general settings such as the system name and time. Click **Basic Setting > General Setup** in the navigation panel to display the screen as shown.

Figure 55 Basic Setting > General Setup

The screenshot shows the 'General Setup' configuration page. At the top, there is a title bar with the text 'General Setup'. Below the title bar, there are several input fields and dropdown menus:

- System Name:** OLT1404A
- Location:** (empty field)
- Contact Person's Name:** (empty field)
- Use Time Server when Bootup:** None (dropdown menu)
- Time Server IP Address:** 0.0.0.0
- Current Time:** 02 : 11 : 30 UTC
- New Time (hh:mm:ss):** 02 : 11 : 30
- Current Date:** 2037 - 02 - 08
- New Date (yyyy-mm-dd):** 2037 - 02 - 08
- Time Zone:** UTC (dropdown menu)
- Daylight Saving Time:** (checkbox)
- Start Date:** First Sunday of January at 0:00
- End Date:** First Sunday of January at 0:00

A note at the bottom states: "It will take 60 seconds if time server is unreachable."

At the bottom right, there are 'Apply' and 'Cancel' buttons.

The following table describes the labels in this screen.

Table 13 Basic Setting > General Setup

LABEL	DESCRIPTION
System Name	Choose a descriptive name for identification purposes. This name consists of up to 64 printable characters; spaces are allowed.
Location	Enter the geographic location of your OLT. You can use up to 32 printable ASCII characters; spaces are allowed.
Contact Person's Name	Enter the name of the person in charge of this OLT. You can use up to 32 printable ASCII characters; spaces are allowed.
Use Time Server when Bootup	<p>Enter the time service protocol that your time server uses. Not all time servers 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.</p> <p>When you select the Daytime (RFC 867) format, the OLT 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.</p> <p>Time (RFC-868) format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0.</p> <p>NTP (RFC-1305) is similar to Time (RFC-868).</p> <p>None is the default value. Enter the time manually. Each time you turn on the OLT, the time and date will be reset to 1970-1-1 0:0:0.</p>
Time Server IP Address	Enter the IP address or domain name of your timeserver. The OLT 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	<p>Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.</p> <p>Select this option if you use Daylight Saving Time.</p>
Start Date	<p>Configure the day and time when Daylight Saving Time starts if you selected Daylight Saving Time. The time is displayed in the 24 hour format. Here are a couple of examples:</p> <p>Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select Second, Sunday, March and 2:00.</p> <p>Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select Last, Sunday, March and the last field depends on your time zone. In Germany for instance, you would select 2:00 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).</p>

Table 13 Basic Setting > General Setup (continued)

LABEL	DESCRIPTION
End Date	Configure the day and time when Daylight Saving Time ends if you selected Daylight Saving Time . The time field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select First, Sunday, November and 2:00 . Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select Last, Sunday, October and the last field depends on your time zone. In Germany for instance, you would select 2:00 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Apply	Click Apply to save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

8.4 Introduction to VLANs

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(s); the traffic must first go through a router.

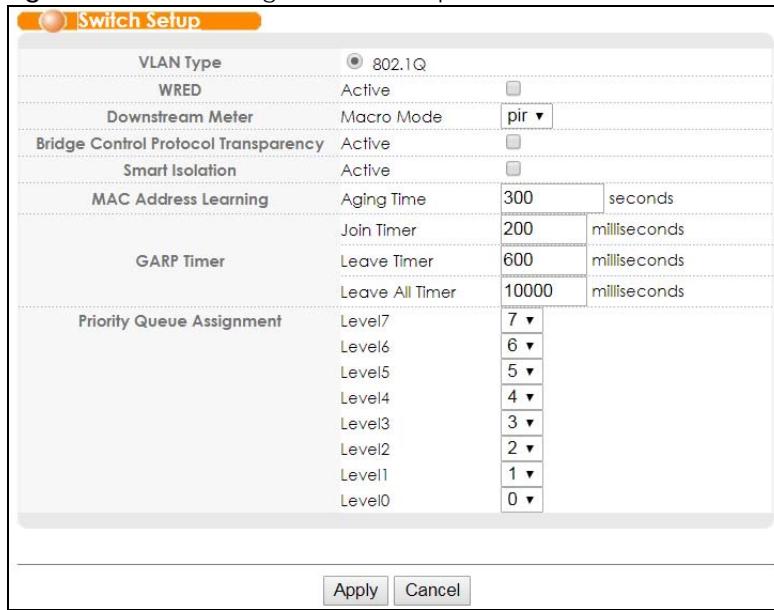
In MTU (Multi-Tenant Unit) applications, VLAN is vital in providing isolation and security among the subscribers. When properly configured, VLAN prevents one subscriber from accessing the network resources of another on the same LAN, thus a user will not see the printers and hard disks of another user in the same building.

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.

See [Chapter 9 on page 95](#) for information on port-based and 802.1Q tagged VLANs.

8.5 Switch Setup

Click **Basic Setting > Switch Setup** in the navigation panel to display the screen as shown. Refer to [Chapter 9 on page 95](#) for more information on VLAN.

Figure 56 Basic Setting > Switch Setup

The following table describes the labels in this screen.

Table 14 Basic Setting > Switch Setup

LABEL	DESCRIPTION
VLAN Type	Choose 802.1Q . See Chapter 9 on page 95 for more information.
WRED	Select Active to enable QoS Weighted Random Early Detection (WRED). It's a congestion avoidance technique that makes early detection of traffic congestion possible and provides queueing scheduling for multiple classes of traffic.
Downstream Meter	Set the downstream macro meter rate limit sharing mode. Select pir (Peak Information Rate) to take bandwidth first. Select cir (Committed Information Rate) to take bandwidth first.
Bridge Control Protocol Transparency	Select Active to allow the OLT to handle bridging control protocols (STP, for example). You also need to define how to treat a BPDU in the Basic Setting > Port Setup screen.
Smart Isolation	Select Active to enable smart isolation on the OLT. The designated port(s) then becomes the isolated port. Smart isolation allows you to prevent isolated ports on different switches from transmitting traffic to each other. Note: To use smart isolation, you should have configured 802.1Q VLAN port isolation or private VLAN and (M)RSTP on the OLT. Smart isolation does not work with MSTP.
MAC Address Learning	MAC address learning reduces outgoing traffic broadcasts. For MAC address learning to occur on a port, the port must be active.
Aging Time	Enter a time from 10 to 1000000 seconds. This is how long all dynamically learned MAC addresses remain in the MAC address table before they age out (and must be relearned).
GARP Timer	Switches join VLANs by making a declaration. A declaration is made by issuing a Join message using GARP. Declarations are withdrawn by issuing a Leave message. A Leave All message terminates all registrations. GARP timers set declaration timeout values. See the chapter on VLAN setup for more background information.
Join Timer	Join Timer sets the duration of the Join Period timer for GVRP in milliseconds. Each port has a Join Period timer. The allowed Join Time range is between 100 and 65535 milliseconds; the default is 200 milliseconds. See the chapter on VLAN setup for more background information.

Table 14 Basic Setting > Switch Setup (continued)

LABEL	DESCRIPTION																				
Leave Timer	Leave Time sets the duration of the Leave Period timer for GVRP in milliseconds. Each port has a single Leave Period timer. Leave Time must be two times larger than Join Timer ; the default is 600 milliseconds.																				
Leave All Timer	Leave All Timer sets the duration of the Leave All Period timer for GVRP in milliseconds. Each port has a single Leave All Period timer. Leave All Timer must be larger than Leave Timer.																				
Priority Queue Assignment	<p>IEEE 802.1p defines up to eight 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 next fields to configure the priority level-to-physical queue mapping.</p> <p>The OLT has eight physical queues that you can map to the 8 priority levels. On the OLT, traffic assigned to higher index queues gets through faster while traffic in lower index queues is dropped if the network is congested.</p> <p>To map a priority level to a physical queue, select a physical queue from the drop-down menu on the right.</p> <p>Priority Level (The following descriptions are based on the traffic types defined in the IEEE 802.1d standard (which incorporates the 802.1p)).</p> <table border="1"> <tbody> <tr> <td>Level 7</td><td>Typically used for network control traffic such as router configuration messages.</td></tr> <tr> <td>Level 6</td><td>Typically used for voice traffic that is especially sensitive to jitter (jitter is the variations in delay).</td></tr> <tr> <td>Level 5</td><td>Typically used for video that consumes high bandwidth and is sensitive to jitter.</td></tr> <tr> <td>Level 4</td><td>Typically used for controlled load, latency-sensitive traffic such as SNA (Systems Network Architecture) transactions.</td></tr> <tr> <td>Level 3</td><td>Typically used for "excellent effort" or better than best effort and would include important business traffic that can tolerate some delay.</td></tr> <tr> <td>Level 2</td><td>This is for "spare bandwidth".</td></tr> <tr> <td>Level 1</td><td>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.</td></tr> <tr> <td>Level 0</td><td>Typically used for best-effort traffic.</td></tr> <tr> <td>Apply</td><td>Click Apply to save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.</td></tr> <tr> <td>Cancel</td><td>Click Cancel to reset the fields.</td></tr> </tbody> </table>	Level 7	Typically used for network control traffic such as router configuration messages.	Level 6	Typically used for voice traffic that is especially sensitive to jitter (jitter is the variations in delay).	Level 5	Typically used for video that consumes high bandwidth and is sensitive to jitter.	Level 4	Typically used for controlled load, latency-sensitive traffic such as SNA (Systems Network Architecture) transactions.	Level 3	Typically used for "excellent effort" or better than best effort and would include important business traffic that can tolerate some delay.	Level 2	This is for "spare bandwidth".	Level 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.	Level 0	Typically used for best-effort traffic.	Apply	Click Apply to save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.	Cancel	Click Cancel to reset the fields.
Level 7	Typically used for network control traffic such as router configuration messages.																				
Level 6	Typically used for voice traffic that is especially sensitive to jitter (jitter is the variations in delay).																				
Level 5	Typically used for video that consumes high bandwidth and is sensitive to jitter.																				
Level 4	Typically used for controlled load, latency-sensitive traffic such as SNA (Systems Network Architecture) transactions.																				
Level 3	Typically used for "excellent effort" or better than best effort and would include important business traffic that can tolerate some delay.																				
Level 2	This is for "spare bandwidth".																				
Level 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.																				
Level 0	Typically used for best-effort traffic.																				
Apply	Click Apply to save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.																				
Cancel	Click Cancel to reset the fields.																				

8.6 IP Setup

Use the **IP Setup** screen to configure the OLT IP address, default gateway device, and the management VLAN ID. The default gateway specifies the IP address of the default gateway (next hop) for outgoing traffic.

Management IP Addresses

The OLT needs an IP address for it to be managed over the network. 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. The subnet mask specifies the network number portion of an IP address. The factory default subnet mask is 255.255.255.0.

You can configure up to 32 IP addresses which are used to access and manage the OLT from the ports belonging to the pre-defined VLAN(s).

Note: You must configure a VLAN first. Each VLAN can have multiple management IP addresses, and you can log into the OLT via different management IP addresses simultaneously.

Use this screen to configure the default gateway device, the default domain name server and add IP domains.

Figure 57 Basic Setting > IP Setup

Index	IP Address	IP Subnet Mask	VID	Delete
1	1.0.0.1	255.255.0.0	2	<input type="checkbox"/>
2	10.214.80.211	255.255.255.0	1	<input type="checkbox"/>
3	192.168.1.1	255.255.255.0	1	<input type="checkbox"/>

The following table describes the labels in this screen.

Table 15 Basic Setting > IP Setup

LABEL	DESCRIPTION
Default Gateway	Type the IP address of the default outgoing gateway in dotted decimal notation, for example 192.168.1.254.
Domain Name Server	Enter a domain name server IPv4 address in order to be able to use a domain name instead of an IP address.
Default Management	Specify which traffic flow (In-Band or Out-of-band) the OLT is to send packets originating from itself (such as SNMP traps). Select In-Band to have the OLT send the packets to all ports except the management port (labelled MGMT) to which connected device(s) do not receive these packets. Select Out-of-band to have the OLT send the packets to the management port labelled MGMT . This means that device(s) connected to the other port(s) do not receive these packets.
Management IP Address	Use these fields to set the settings for the out-of-band management port.

Table 15 Basic Setting > IP Setup

LABEL	DESCRIPTION
IP Address	Enter the out-of-band management IP address of your OLT in dotted decimal notation. For example, 192.168.0.1.
IP Subnet Mask	Enter the IP subnet mask of your OLT 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, for example, 192.168.0.254
Apply	Click Apply to save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields to your previous configuration.
IP Interface	
Use these fields to create or edit IP routing domains on the OLT.	
IP Address	Enter the IP address of your OLT in dotted decimal notation, for example, 192.168.1.1. This is the IP address of the OLT in an IP routing domain.
IP Subnet Mask	Enter the IP subnet mask of an IP routing domain in dotted decimal notation, for example, 255.255.255.0.
VID	Enter the VLAN identification number to which an IP routing domain belongs.
Add	Click this to create a new entry. This saves your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields to your previous configuration.
Index	This field displays the index number of an entry.
IP Address	This field displays IP address of the OLT in the IP domain.
IP Subnet Mask	This field displays the subnet mask of the OLT in the IP domain.
VID	This field displays the VLAN identification number of the IP domain on the OLT.
Delete	Click Delete to remove the selected entry from the summary table. Note: Deleting all IP subnets locks you out of the OLT.
Cancel	Click Cancel to clear the check boxes.

8.7 Port Setup

Use this screen to configure OLT port settings. Click **Basic Setting > Port Setup** in the navigation panel to display the configuration screen.

Figure 58 Basic Setting > Port Setup

Port Setup							
Port	Active	Name	Type	Speed / Duplex	Flow Control	802.1p Priority	BPDU Control
*	<input type="checkbox"/>		-	Auto ▼	<input type="checkbox"/>	0 ▼	Peer ▼
eth-1	<input checked="" type="checkbox"/>		100/1000M	Auto ▼	<input type="checkbox"/>	0 ▼	Peer ▼
eth-2	<input checked="" type="checkbox"/>		100/1000M	Auto ▼	<input type="checkbox"/>	0 ▼	Peer ▼
eth-3	<input checked="" type="checkbox"/>		100/1000M	Auto ▼	<input type="checkbox"/>	0 ▼	Peer ▼
eth-4	<input checked="" type="checkbox"/>		100/1000M	Auto ▼	<input type="checkbox"/>	0 ▼	Peer ▼
eth-5	<input checked="" type="checkbox"/>		100/1000M	Auto ▼	<input type="checkbox"/>	0 ▼	Peer ▼
eth-6	<input checked="" type="checkbox"/>		100/1000M	Auto ▼	<input type="checkbox"/>	0 ▼	Peer ▼
eth-7	<input checked="" type="checkbox"/>		100/1000M	Auto ▼	<input type="checkbox"/>	0 ▼	Peer ▼
eth-8	<input checked="" type="checkbox"/>		100/1000M	Auto ▼	<input type="checkbox"/>	0 ▼	Peer ▼
eth-9	<input checked="" type="checkbox"/>		1000/2500M	Auto ▼	<input type="checkbox"/>	0 ▼	Peer ▼
eth-10	<input checked="" type="checkbox"/>		1000/2500M	Auto ▼	<input type="checkbox"/>	0 ▼	Peer ▼
eth-11	<input checked="" type="checkbox"/>		1000/2500M	Auto ▼	<input type="checkbox"/>	0 ▼	Peer ▼
eth-12	<input checked="" type="checkbox"/>		1000/2500M	Auto ▼	<input type="checkbox"/>	0 ▼	Peer ▼
eth-13	<input checked="" type="checkbox"/>		1000/2500M	Auto ▼	<input type="checkbox"/>	0 ▼	Peer ▼
eth-14	<input checked="" type="checkbox"/>		1000/2500M	Auto ▼	<input type="checkbox"/>	0 ▼	Peer ▼
eth-15	<input checked="" type="checkbox"/>		1000/2500M	Auto ▼	<input type="checkbox"/>	0 ▼	Peer ▼
eth-16	<input checked="" type="checkbox"/>		1000/2500M	Auto ▼	<input type="checkbox"/>	0 ▼	Peer ▼
eth-17	<input checked="" type="checkbox"/>		1000M/2500M/10G	Auto ▼	<input type="checkbox"/>	0 ▼	Peer ▼
eth-18	<input checked="" type="checkbox"/>		1000M/2500M/10G	Auto ▼	<input type="checkbox"/>	0 ▼	Peer ▼
eth-19	<input checked="" type="checkbox"/>		1000M/2500M/10G	Auto ▼	<input type="checkbox"/>	0 ▼	Peer ▼
eth-20	<input checked="" type="checkbox"/>		1000M/2500M/10G	Auto ▼	<input type="checkbox"/>	0 ▼	Peer ▼
pon-1	<input checked="" type="checkbox"/>		2500M	2500M / Full Duplex ▼	<input type="checkbox"/>	0 ▼	Peer ▼
pon-2	<input checked="" type="checkbox"/>		2500M	2500M / Full Duplex ▼	<input type="checkbox"/>	0 ▼	Peer ▼
pon-3	<input checked="" type="checkbox"/>		2500M	2500M / Full Duplex ▼	<input type="checkbox"/>	0 ▼	Peer ▼
pon-4	<input checked="" type="checkbox"/>		2500M	2500M / Full Duplex ▼	<input type="checkbox"/>	0 ▼	Peer ▼

The following table describes the labels in this screen.

Table 16 Basic Setting > Port Setup

LABEL	DESCRIPTION
Port	This is the port index number. * means all ports. An entry that starts with eth is for an Ethernet port. An entry that starts with pon is for a GPON port.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to enable a port. 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 enter up to 64 alpha-numerical characters. Note: Due to space limitation, the port name may be truncated in some web configurator screens.
Type	This field displays the capacity that the port can support.

Table 16 Basic Setting > Port Setup (continued)

LABEL	DESCRIPTION
Speed/Duplex	Select the speed and the duplex mode of the Ethernet connection on this port. Choices are Auto-1000M, 100M/Half Duplex, 100M/Full Duplex, 1000M/Full Duplex, 2500M/Full Duplex , and 10G/Full Duplex (Gigabit connections only). Selecting Auto-1000M (auto-negotiation) allows one port to negotiate with a peer port automatically to obtain the connection speed (of up to 1000M) and duplex mode that both ends support. When auto-negotiation is turned on, a port on the OLT negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer port does not support auto-negotiation or turns off this feature, the OLT determines the connection speed by detecting the signal on the cable and using half duplex mode. When the OLT's auto-negotiation is turned off, a port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer port are the same in order to connect.
Flow Control	A concentration of traffic on a port decreases port bandwidth and overflows buffer memory causing packet discards and frame losses. Flow Control is used to regulate transmission of signals to match the bandwidth of the receiving port. The OLT uses IEEE802.3x flow control in full duplex mode and backpressure flow control in half duplex mode. IEEE802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill. Back Pressure flow control is typically used in half duplex mode to send a "collision" signal to the sending port (mimicking a state of packet collision) causing the sending port to temporarily stop sending signals and resend later. Select Flow Control to enable it.
802.1p Priority	This priority value is added to incoming frames without a (802.1p) priority queue tag. See Priority Queue Assignment in Table 14 on page 89 for more information.
BPDU Control	Configure the way to treat BPDUs received on this port. You must activate bridging control protocol transparency in the Basic Setting > Switch Setup screen first. Select Peer to process any BPDU (Bridge Protocol Data Units) received on this port. Select Tunnel to forward BPDUs received on this port. Select Discard to drop any BPDU received on this port. Select Network to process a BPDU with no VLAN tag and forward a tagged BPDU.
Apply	Click Apply to save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

CHAPTER 9

VLAN

9.1 Overview

This chapter shows you how to configure 802.1Q tagged and port-based VLANs. The type of screen you see here depends on the **VLAN Type** you selected in the **Switch Setup** screen.

9.1.1 What You Can Do

- Use the **VLAN Status** screen ([Section 9.2 on page 98](#)) to view and search all VLAN groups.
- Use the **VLAN Detail** screen ([Section 9.2.1 on page 98](#)) to view detailed port settings and status of the VLAN group.
- Use the **VLAN Port Setting** screen ([Section 9.3 on page 99](#)) to configure the static VLAN (IEEE 802.1Q) settings on a port.
- Use the **Subnet Based VLANs** screen ([Section 9.3.1.1 on page 103](#)) to set up VLANs that allow you to group traffic into logical VLANs based on the source IP subnet you specify.
- Use the **Protocol Based VLAN** screen ([Section 9.3.2.1 on page 105](#)) to set up VLANs that allow you to group traffic into logical VLANs based on the protocol you specify.
- Use the **Static VLAN** screen ([Section 9.4 on page 106](#)) to configure and view 802.1Q VLAN parameters for the OLT.

9.1.2 What You Need to Know

Read this section to know more about VLAN and how to configure the screens.

IEEE 802.1Q Tagged VLANs

A 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

Forwarding Tagged and Untagged Frames

Each port on the OLT 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 OLT 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 OLT 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.

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.

9.1.2.1 Automatic VLAN Registration

GARP and GVRP are the protocols used to automatically register VLAN membership across switches.

GARP

GARP (Generic Attribute Registration Protocol) allows network switches to register and de-register attribute values with other GARP participants within a bridged LAN. GARP is a protocol that provides a generic mechanism for protocols that serve a more specific application, for example, GVRP.

GARP Timers

Switches join VLANs by making a declaration. A declaration is made by issuing a Join message using GARP. Declarations are withdrawn by issuing a Leave message. A Leave All message terminates all registrations. GARP timers set declaration timeout values.

GVRP

GVRP (GARP VLAN Registration Protocol) is a registration protocol that defines a way for switches to register necessary VLAN members on ports across the network. Enable this function to permit VLAN groups beyond the local OLT.

Please refer to the following table for common IEEE 802.1Q VLAN terminology.

Table 17 IEEE 802.1Q VLAN Terminology

VLAN PARAMETER	TERM	DESCRIPTION
VLAN Type	Permanent VLAN	This is a static VLAN created manually.
	Dynamic VLAN	This is a VLAN configured by a GVRP registration/deregistration process.

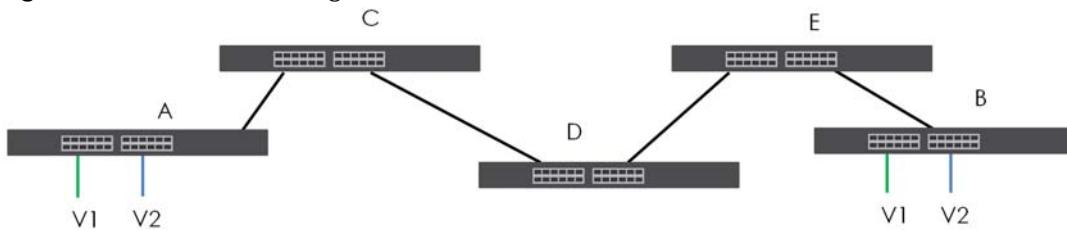
Table 17 IEEE 802.1Q VLAN Terminology (continued)

VLAN PARAMETER	TERM	DESCRIPTION
VLAN Administrative Control	Registration Fixed	Fixed registration ports are permanent VLAN members.
	Registration Forbidden	Ports with registration forbidden are forbidden to join the specified VLAN.
	Normal Registration	Ports dynamically join a VLAN using GVRP.
VLAN Tag Control	Tagged	Ports belonging to the specified VLAN tag all outgoing frames transmitted.
	Untagged	Ports belonging to the specified VLAN don't tag all outgoing frames transmitted.
VLAN Port	Port VID	This is the VLAN ID assigned to untagged frames that this port received.
	Acceptable Frame Type	You may choose to accept both tagged and untagged incoming frames, just tagged incoming frames or just untagged incoming frames on a port.
	Ingress filtering	If set, the OLT discards incoming frames for VLANs that do not have this port as a member

9.1.2.2 Port VLAN Trunking

Enable **VLAN Trunking** on a port to allow frames belonging to unknown VLAN groups to pass through that port. This is useful if you want to set up VLAN groups on end devices without having to configure the same VLAN groups on intermediary devices.

Refer to the following figure. Suppose you want to create VLAN groups 1 and 2 (V1 and V2) on devices A and B. Without **VLAN Trunking**, you must configure VLAN groups 1 and 2 on all intermediary switches C, D and E; otherwise they will drop frames with unknown VLAN group tags. However, with **VLAN Trunking** enabled on a port(s) in each intermediary switch you only need to create VLAN groups in the end devices (A and B). C, D and E automatically allow frames with VLAN group tags 1 and 2 (VLAN groups that are unknown to those switches) to pass through their VLAN trunking port(s).

Figure 59 Port VLAN Trunking

9.1.2.3 Static VLAN

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 outgoing frames (that were previously untagged) from a port with the specified VID.

9.2 VLAN Status

Use this screen to view and search all VLAN groups. Click **Advanced Application > VLAN** from the navigation panel to display the **VLAN Status** screen as shown next.

Figure 60 Advanced Application > VLAN: VLAN Status

VLAN Status		VLAN Port Setting	Static VLAN
VLAN Search by VID		<input type="text"/>	Search
The Number of VLAN: 2.			
Index	VID	Elapsed Time	Status
1	1	1:10:10	Static
2	2	1:10:10	Static
Change Pages Previous Next			

The following table describes the labels in this screen.

Table 18 Advanced Application > VLAN: VLAN Status

LABEL	DESCRIPTION
VLAN Search by VID	Enter an existing VLAN ID number(s) (separated by a comma) and click Search to display only the specified VLAN(s) in the list below. Leave this field blank and click Search to display all VLANs configured on the OLT.
The Number of VLAN	This is the number of VLANs configured on the OLT.
The Number of Search Results	This is the number of VLANs that match the searching criteria and display in the list below. This field displays only when you use the Search button to look for certain VLANs.
Index	This is the VLAN index number. Click on an index number to view more VLAN details.
VID	This is the VLAN identification number that was configured in the Static VLAN screen.
Elapsed Time	This field shows how long it has been since a normal VLAN was registered or a static VLAN was set up.
Status	This field shows how this VLAN was added to the OLT. Dynamic: using GVRP Static: added as a permanent entry
Change Pages	Click Previous or Next to show the previous/next screen if all status information cannot be seen in one screen.

9.2.1 VLAN Details

Use this screen to view detailed port settings and status of the VLAN group. Click on an index number in the **VLAN Status** screen to display VLAN details.

Figure 61 Advanced Application > VLAN > VLAN Detail

The following table describes the labels in this screen.

Table 19 Advanced Application > VLAN > VLAN Detail

LABEL	DESCRIPTION
VLAN Status	Click this to go to the VLAN Status screen.
VID	This is the VLAN identification number that was configured in the Static VLAN screen.
Port Number	This column displays the ports that are participating in a VLAN. A tagged port is marked as T, an untagged port is marked as U and ports not participating in a VLAN are marked as “-”.
Elapsed Time	This field shows how long it has been since a normal VLAN was registered or a static VLAN was set up.
Status	This field shows how this VLAN was added to the OLT.
	Dynamic: using GVRP
	Static: added as a permanent entry

9.3 Configure VLAN Port Settings

Use the VLAN Port Setup screen to configure the static VLAN (IEEE 802.1Q) settings on a port. Click the **VLAN Port Setting** link in the **VLAN Status** screen.

Figure 62 Advanced Application > VLAN > VLAN Status > VLAN Port Setting

VLAN Port Setting		Subnet Based Vlan	Protocol Based Vlan	VLAN Status	
	GVRP	<input type="checkbox"/>			
	Port Isolation	<input type="checkbox"/>			
Port Ingress Check PVID GVRP Acceptable Frame Type VLAN Trunking					
*	<input type="checkbox"/>	1	<input type="checkbox"/>	All ▾	<input type="checkbox"/>
1	<input type="checkbox"/>	1	<input type="checkbox"/>	All ▾	<input type="checkbox"/>
2	<input type="checkbox"/>	1	<input type="checkbox"/>	All ▾	<input type="checkbox"/>
3	<input type="checkbox"/>	1	<input type="checkbox"/>	All ▾	<input type="checkbox"/>
4	<input type="checkbox"/>	1	<input type="checkbox"/>	All ▾	<input type="checkbox"/>
5	<input type="checkbox"/>	1	<input type="checkbox"/>	All ▾	<input type="checkbox"/>
6	<input type="checkbox"/>	1	<input type="checkbox"/>	All ▾	<input type="checkbox"/>
7	<input type="checkbox"/>	1	<input type="checkbox"/>	All ▾	<input type="checkbox"/>
8	<input type="checkbox"/>	1	<input type="checkbox"/>	All ▾	<input type="checkbox"/>
9	<input type="checkbox"/>	1	<input type="checkbox"/>	All ▾	<input type="checkbox"/>
10	<input type="checkbox"/>	1	<input type="checkbox"/>	All ▾	<input type="checkbox"/>
20	<input type="checkbox"/>	1	<input type="checkbox"/>	All ▾	<input type="checkbox"/>
21	<input type="checkbox"/>	1	<input type="checkbox"/>	All ▾	<input type="checkbox"/>
22	<input type="checkbox"/>	1	<input type="checkbox"/>	All ▾	<input type="checkbox"/>
23	<input type="checkbox"/>	1	<input type="checkbox"/>	All ▾	<input type="checkbox"/>
24	<input type="checkbox"/>	1	<input type="checkbox"/>	All ▾	<input type="checkbox"/>

Apply **Cancel**

The following table describes the labels in this screen.

Table 20 Advanced Application > VLAN > VLAN Status> VLAN Port Setting

LABEL	DESCRIPTION
GVRP	GVRP (GARP VLAN Registration Protocol) is a registration protocol that defines a way to register necessary VLAN members on ports across the network. Select this check box to permit VLAN groups beyond the local OLT.
Port Isolation	Select this checkbox so the PON ports in the same VLAN group won't communicate with each other. Traffic coming from the PON ports will be forwarded to the other ports of the OLT. This option is the most limiting but also the most secure. Note: Port isolation only works on the PON ports.
Port	This field displays the port number. The first 4-8 ports maps with the physical PON ports of OLT1404A and 14048A, and the rest maps with the other physical ports on the OLT's front panel. See Table 21 on page 101 for more detailed information.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Ingress Check	If this check box is selected, the OLT discards incoming frames on a port for VLANs that do not include this port in its member set. Clear this check box to disable ingress filtering.

Table 20 Advanced Application > VLAN > VLAN Status> VLAN Port Setting

LABEL	DESCRIPTION
PVID	A PVID (Port VLAN ID) is a tag that adds to incoming untagged frames received on a port so that the frames are forwarded to the VLAN group that the tag defines. Enter a number between 1 and 4094 as the port VLAN ID.
GVRP	Select this check box to allow GVRP on this port.
Acceptable Frame Type	Specify the type of frames allowed on a port. Choices are All , Tag Only and Untag Only . Select All from the drop-down list box to accept all untagged or tagged frames on this port. This is the default setting. Select Tag Only to accept only tagged frames on this port. All untagged frames will be dropped. Select Untag Only to accept only untagged frames on this port. All tagged frames will be dropped.
VLAN Trunking	Enable VLAN Trunking on ports connected to other switches or routers (but not ports directly connected to end users) to allow frames belonging to unknown VLAN groups to pass through the OLT.
Apply	Click Apply to save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

The following table introduces the port mappings of the VLAN ports and the physical ports.

Table 21 Mapping of VLAN Ports and Physical Ports

OLT1408A		OLT1404A	
VLAN PORT	PHYSICAL PORT	VLAN PORT	PHYSICAL PORT
1	PON1	1	PON1
2	PON2	2	PON2
3	PON3	3	PON3
4	PON4	4	PON4
5	PON5	5	Port 1
6	PON6	6	Port 2
7	PON7	7	Port 3
8	PON8	8	Port 4
9	Port 1	9	Port 5
10	Port 2	10	Port 6
11	Port 3	11	Port 7
12	Port 4	12	Port 8
13	Port 5	13	Port 9
14	Port 6	14	Port 10
15	Port 7	15	Port 11
16	Port 8	16	Port 12
17	Port 9	17	Port 13
18	Port 10	18	Port 14
19	Port 11	19	Port 15
20	Port 12	20	Port 16

Table 21 Mapping of VLAN Ports and Physical Ports

OLT1408A		OLT1404A	
VLAN PORT	PHYSICAL PORT	VLAN PORT	PHYSICAL PORT
21	Port 13	21	Port 17
22	Port 14	22	Port 18
23	Port 15	23	Port 19
24	Port 16	24	Port 20
25	Port 17		
26	Port 18		
27	Port 19		
28	Port 20		

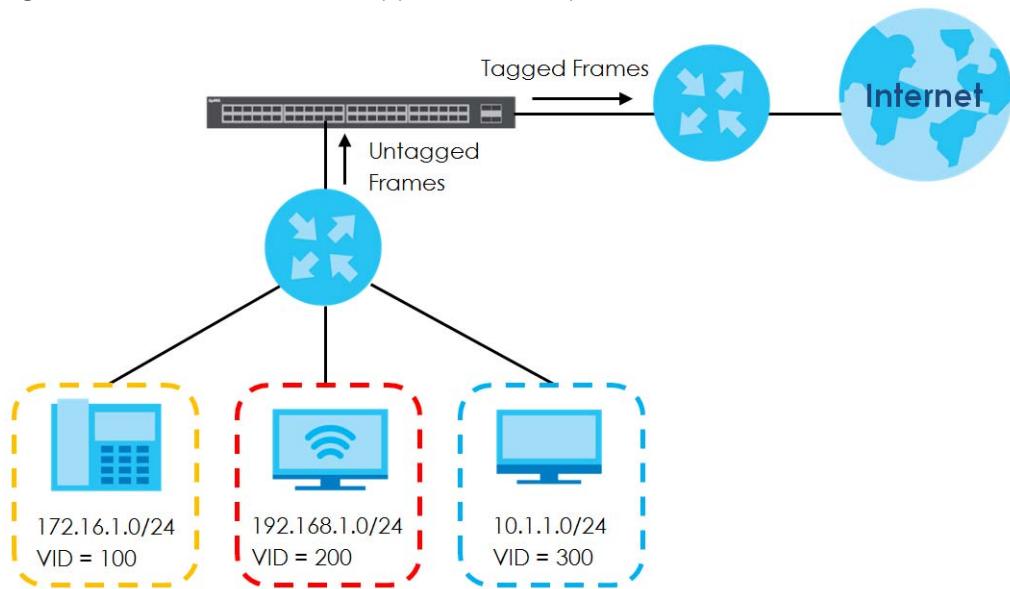
9.3.1 Subnet Based VLANs

Subnet based VLANs allow you to group traffic into logical VLANs based on the source IP subnet you specify. When a frame is received on a port, the OLT checks if a tag is added already and the IP subnet it came from. The untagged packets from the same IP subnet are then placed in the same subnet based VLAN. One advantage of using subnet based VLANs is that priority can be assigned to traffic from the same IP subnet.

Note: Subnet based VLAN applies to un-tagged packets and is applicable only when you use IEEE 802.1Q tagged VLAN.

For example, an ISP (Internet Service Provider) may divide different types of services it provides to customers into different IP subnets. Traffic for voice services is designated for IP subnet 172.16.1.0/24, video for 192.168.1.0/24 and data for 10.1.1.0/24. The OLT can then be configured to group incoming traffic based on the source IP subnet of incoming frames.

You can then configure a subnet based VLAN with priority 6 and VID of 100 for traffic received from IP subnet 172.16.1.0/24 (voice services). You can also have a subnet based VLAN with priority 5 and VID of 200 for traffic received from IP subnet 192.168.1.0/24 (video services). Lastly, you can configure VLAN with priority 3 and VID of 300 for traffic received from IP subnet 10.1.1.0/24 (data services). All untagged incoming frames will be classified based on their source IP subnet and prioritized accordingly. That is, video services receive the highest priority and data the lowest.

Figure 63 Subnet Based VLAN Application Example

9.3.1.1 Configuring Subnet Based VLAN

Click the **Subnet Based Vlan** link in the **VLAN Port Setting** screen to display the configuration screen as shown.

Figure 64 Advanced Application > VLAN > VLAN Port Setting > Subnet Based Vlan

Subnet Based VLAN		VLAN Port Setting												
<input checked="" type="checkbox"/> Active	<input type="checkbox"/>													
DHCP-Vlan Override														
<input type="button" value="Apply"/>														
<table border="1"> <tr> <td><input checked="" type="checkbox"/> Active</td> <td><input type="checkbox"/></td> </tr> <tr> <td>Name</td> <td><input type="text"/></td> </tr> <tr> <td>IP</td> <td><input type="text"/></td> </tr> <tr> <td>Mask-Bits</td> <td><input type="text"/></td> </tr> <tr> <td>VID</td> <td><input type="text"/></td> </tr> <tr> <td>Priority</td> <td><input type="text"/></td> </tr> </table>			<input checked="" type="checkbox"/> Active	<input type="checkbox"/>	Name	<input type="text"/>	IP	<input type="text"/>	Mask-Bits	<input type="text"/>	VID	<input type="text"/>	Priority	<input type="text"/>
<input checked="" type="checkbox"/> Active	<input type="checkbox"/>													
Name	<input type="text"/>													
IP	<input type="text"/>													
Mask-Bits	<input type="text"/>													
VID	<input type="text"/>													
Priority	<input type="text"/>													
<input type="button" value="Add"/> <input type="button" value="Cancel"/>														
Index	Active	Name	IP	Mask-Bits	VID	Priority	Delete							
							<input type="button" value="Delete"/> <input type="button" value="Cancel"/>							

The following table describes the labels in this screen.

Table 22 Advanced Application > VLAN > VLAN Port Setting > Subnet Based Vlan

LABEL	DESCRIPTION
Active	Select this check box to activate this subnet based VLANs on the OLT.
DHCP-Vlan Override	When DHCP snooping is enabled DHCP clients can renew their IP address through the DHCP VLAN or via another DHCP server on the subnet based VLAN. Select this checkbox to force the DHCP clients in this IP subnet to obtain their IP addresses through the DHCP VLAN.
Apply	Click Apply to save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Active	Select this check box to activate the IP subnet VLAN you are creating or editing.
Name	Enter up to 32 alphanumeric characters to identify this subnet based VLAN.
IP	Enter the IP address of the subnet for which you want to configure this subnet based VLAN.
Mask-Bits	Enter the bit number of the subnet mask. To find the bit number, convert the subnet mask to binary format and add all the 1's together. Take "255.255.255.0" for example. 255 converts to eight 1s in binary. There are three 255s, so add three eights together and you get the bit number (24).
VID	Enter the ID of a VLAN with which the untagged frames from the IP subnet specified in this subnet based VLAN are tagged. This must be an existing VLAN which you defined in the Advanced Application > VLAN > Static VLAN screen.
Priority	Select the priority level that the OLT assigns to frames belonging to this VLAN.
Add	Click this to create a new entry or to update an existing one. This saves your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Index	This is the index number identifying this subnet based VLAN. Click on any of these numbers to edit an existing subnet based VLAN.
Active	This field shows whether the subnet based VLAN is active or not.
Name	This field shows the name the subnet based VLAN.
IP	This field shows the IP address of the subnet for this subnet based VLAN.
Mask-Bits	This field shows the subnet mask in bit number format for this subnet based VLAN.
VID	This field shows the VLAN ID of the frames which belong to this subnet based VLAN.
Priority	This field shows the priority which is assigned to frames belonging to this subnet based VLAN.
Delete	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Click this to delete the subnet based VLANs which you marked for deletion.
Cancel	Click Cancel to clear the check boxes.

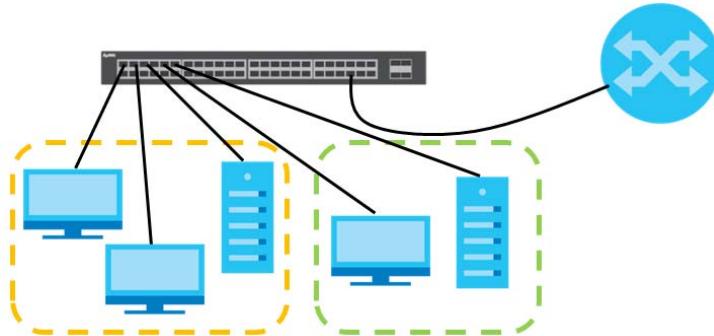
9.3.2 Protocol Based VLANs

Protocol based VLANs allow you to group traffic into logical VLANs based on the protocol you specify. When an upstream frame is received on a port (configured for a protocol based VLAN), the OLT checks if a tag is added already and its protocol. The untagged packets of the same protocol are then placed in the same protocol based VLAN. One advantage of using protocol based VLANs is that priority can be assigned to traffic of the same protocol.

Note: Protocol based VLAN applies to un-tagged packets and is applicable only when you use IEEE 802.1Q tagged VLAN.

For example, ports 1, 2, 3 and 4 belong to static VLAN 100, and ports 4, 5, 6, 7 belong to static VLAN 120. You can configure a protocol based VLAN A with priority 2 for ARP traffic received on port 1, 2 and 3. You can also have a protocol based VLAN B with priority 3 for Apple Talk traffic received on port 6 and 7. All upstream ARP traffic from port 1, 2 and 3 will be grouped together, and all upstream Apple Talk traffic from port 6 and 7 will be in another group and have higher priority than ARP traffic when they go through the uplink port to a backbone switch C.

Figure 65 Protocol Based VLAN Application Example



9.3.2.1 Configuring Protocol Based VLAN

Click the **Protocol Based Vlan** link in the **VLAN Port Setting** screen to display the configuration screen as shown.

Figure 66 Advanced Application > VLAN > VLAN Port Setting > Protocol Based Vlan

Protocol Based VLAN		Vlan Port Setting
<input checked="" type="checkbox"/> Active <input type="text"/> Port <input type="text"/> Name Ethernet-type <input checked="" type="radio"/> IP <input type="radio"/> Others <input type="text"/> (Hex) <input type="text"/> VID <input type="text"/> Priority		
<input type="button" value="Add"/> <input type="button" value="Cancel"/>		
<input type="button" value="Index"/>	<input type="button" value="Active"/>	<input type="button" value="Port"/>
<input type="button" value="Name"/>	<input type="button" value="Ethernet-type"/>	<input type="button" value="VID"/>
<input type="button" value="Priority"/>		<input type="button" value="Delete"/>
<input type="button" value="Delete"/> <input type="button" value="Cancel"/>		

The following table describes the labels in this screen.

Table 23 Advanced Application > VLAN > VLAN Port Setting > Protocol Based Vlan

LABEL	DESCRIPTION
Active	Select this check box to activate this protocol based VLAN.
Port	Type a port number to be included in this protocol based VLAN. This port must belong to a static VLAN in order to participate in a protocol based VLAN. See Chapter 9 on page 95 for more details on setting up VLANs.
Name	Enter up to 32 alphanumeric characters to identify this protocol based VLAN.
Ethernet-type	Use the drop down list box to select a predefined protocol to be included in this protocol based VLAN or select Others and type the protocol number in hexadecimal notation. For example, the IP protocol in hexadecimal notation is 0800, and Novell IPX protocol is 8137. Note: Protocols in the hexadecimal number range of 0x0000 to 0x05ff are not allowed to be used for protocol based VLANs.
VID	Enter the ID of a VLAN to which the port belongs. This must be an existing VLAN which you defined in the Advanced Application > VLAN > Static VLAN screen.
Priority	Select the priority level that the OLT will assign to frames belonging to this VLAN.
Add	Click this to create a new entry or to update an existing one. This saves your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Index	This is the index number identifying this protocol based VLAN. Click on any of these numbers to edit an existing protocol based VLAN.
Active	This field shows whether the protocol based VLAN is active or not.
Port	This field shows which port belongs to this protocol based VLAN.
Name	This field shows the name the protocol based VLAN.
Ethernet-type	This field shows which Ethernet protocol is part of this protocol based VLAN.
VID	This field shows the VLAN ID of the port.
Priority	This field shows the priority which is assigned to frames belonging to this protocol based VLAN.
Delete	Click this to delete the protocol based VLANs which you marked for deletion.
Cancel	Click Cancel to clear the check boxes.

9.4 Configure a Static VLAN

Use this screen to configure a static VLAN for the OLT. Click the **Static VLAN** link in the **VLAN Status** screen to display the screen as shown next.

Figure 67 Advanced Application > VLAN > VLAN Status > Static VLAN

VID	Active	Name	Delete
1	Yes	1	<input type="checkbox"/>
2	Yes	2	<input type="checkbox"/>
100	Yes	VLAN-100	<input type="checkbox"/>

The following table describes the related labels in this screen.

Table 24 Advanced Application > VLAN > VLAN Status > Static VLAN

LABEL	DESCRIPTION
ACTIVE	Select this check box to activate the VLAN settings.
Name	Enter a descriptive name for the VLAN group for identification purposes. This name consists of up to 64 printable characters. Spaces are allowed.
VLAN Group ID	Enter the VLAN ID for this static entry; the valid range is between 1 and 4094.
Port	<p>The port number identifies the port you are configuring.</p> <p>The first 4-8 ports maps with the physical PON ports of OLT1404A and 14048A, and the rest maps with the other physical ports on the OLT's front panel.</p> <p>See Table 21 on page 101 for more detailed information.</p>

Table 24 Advanced Application > VLAN > VLAN Status > Static VLAN (continued)

LABEL	DESCRIPTION
*	<p>Settings in this row apply to all ports.</p> <p>Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis.</p> <p>Note: Changes in this row are copied to all the ports as soon as you make them.</p>
Control	<p>Select Normal for the port to dynamically join this VLAN group using GVRP. This is the default selection.</p> <p>Select Fixed for the port to be a permanent member of this VLAN group.</p> <p>Select Forbidden if you want to prohibit the port from joining this VLAN group.</p>
Tagging	Select TX Tagging if you want the port to tag all outgoing frames transmitted with this VLAN Group ID.
Add	Click Add to save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to change the fields back to their last saved values.
Clear	Click Clear to start configuring the screen again.
VID	This field displays the ID number of the VLAN group. Click the number to edit the VLAN settings.
Active	This field indicates whether the VLAN settings are enabled (Yes) or disabled (No).
Name	This field displays the descriptive name for this VLAN group.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the check boxes.
Paging	
Prev/Next	Click Prev or Next to show the previous/next screen if all status information cannot be seen in one screen.

CHAPTER 10

Static MAC Forward Setup

10.1 Overview

This chapter discusses how to configure forwarding rules based on MAC addresses of devices on your network.

Use these screens to configure static MAC address forwarding.

10.1.1 What You Can Do

Use the **Static MAC Forwarding** screen ([Section 10.2 on page 109](#)) to assign static MAC addresses for a port.

10.2 Configuring Static MAC Forwarding

A static MAC address is an address that has been manually entered in the MAC address table. Static MAC addresses do not age out. When you set up static MAC address rules, you are setting static MAC addresses for a port. This may reduce the need for broadcasting.

Static MAC address forwarding together with port security allow only computers in the MAC address table on a port to access the OLT. See [Chapter 17 on page 146](#) for more information on port security.

Click **Advanced Application > Static MAC Forwarding** in the navigation panel to display the configuration screen as shown.

Figure 68 Advanced Application > Static MAC Forwarding

Index	Active	Name	MAC Address	VID	Port	Delete
						Delete
						Cancel

The following table describes the labels in this screen.

Table 25 Advanced Application > Static MAC Forwarding

LABEL	DESCRIPTION
Active	Select this check box to activate your rule. You may temporarily deactivate a rule without deleting it by clearing this check box.
Name	Enter a descriptive name for identification purposes for this static MAC address forwarding rule.
MAC Address	Enter the MAC address in valid MAC address format, that is, six hexadecimal character pairs. Note: Static MAC addresses do not age out.
VID	Enter the VLAN identification number.
Port	Enter the port where the MAC address entered in the previous field will be automatically forwarded.
Add	Click Add to save your rule to the OLT's run-time memory. The OLT loses this rule if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields to their last saved values.
Clear	Click Clear to begin configuring this screen afresh.
Index	Click an index number to modify a static MAC address rule for a port.
Active	This field displays whether this static MAC address forwarding rule is active (Yes) or not (No). You may temporarily deactivate a rule without deleting it.
Name	This field displays the descriptive name for identification purposes for this static MAC address-forwarding rule.
MAC Address	This field displays the MAC address that will be forwarded and the VLAN identification number to which the MAC address belongs.
VID	This field displays the ID number of the VLAN group.
Port	This field displays the port where the MAC address shown in the next field will be forwarded.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the check boxes.

CHAPTER 11

Static Multicast Forwarding

11.1 Static Multicast Forward Setup Overview

This chapter discusses how to configure forwarding rules based on multicast MAC addresses of devices on your network.

Use these screens to configure static multicast address forwarding.

11.1.1 What You Can Do

Use the **Static Multicast Forwarding** screen ([Section 11.2 on page 112](#)) to configure rules to forward specific multicast frames, such as streaming or control frames, to specific port(s).

11.1.2 What You Need To Know

A multicast MAC address is the MAC address of a member of a multicast group. A static multicast address is a multicast MAC address that has been manually entered in the multicast table. Static multicast addresses do not age out. Static multicast forwarding allows you (the administrator) to forward multicast frames to a member without the member having to join the group first.

If a multicast group has no members, then the switch will either flood the multicast frames to all ports or drop them. [Figure 69 on page 111](#) shows such unknown multicast frames flooded to all ports. With static multicast forwarding, you can forward these multicasts to port(s) within a VLAN group. [Figure 70 on page 112](#) shows frames being forwarded to devices connected to port 3. [Figure 71 on page 112](#) shows frames being forwarded to ports 2 and 3 within VLAN group 4.

Figure 69 No Static Multicast Forwarding

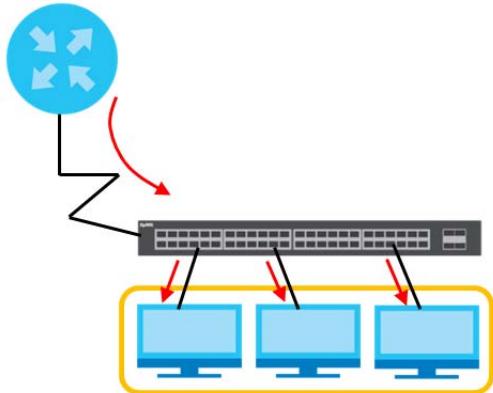
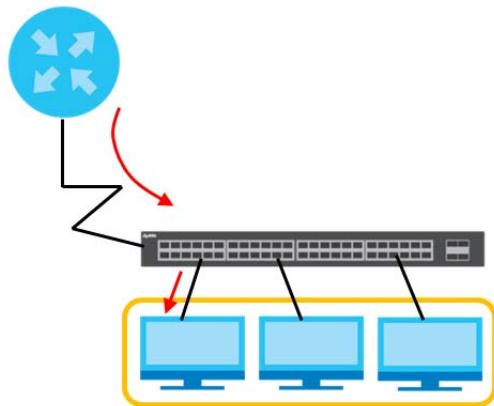
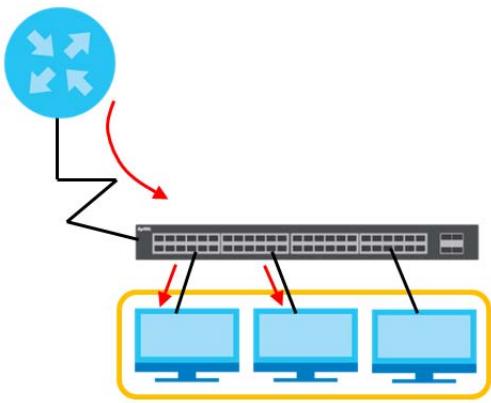


Figure 70 Static Multicast Forwarding to A Single Port**Figure 71** Static Multicast Forwarding to Multiple Ports

11.2 Configuring Static Multicast Forwarding

Use this screen to configure rules to forward specific multicast frames, such as streaming or control frames, to specific port(s).

Click **Advanced Application > Static Multicast Forwarding** to display the configuration screen as shown.

Figure 72 Advanced Application > Static Multicast Forwarding

Static Multicast Forwarding	
Active	<input type="checkbox"/>
Name	<input type="text"/>
MAC Address	<input type="text"/> : <input type="text"/>
VID	<input type="text"/>
Port	<input type="text"/>
<input type="button" value="Add"/> <input type="button" value="Cancel"/> <input type="button" value="Clear"/>	
<input type="button" value="Index"/> <input type="button" value="Active"/> <input type="button" value="Name"/> <input type="button" value="MAC Address"/> <input type="button" value="VID"/> <input type="button" value="Port"/> <input type="button" value="Delete"/>	
<input type="button" value="Delete"/> <input type="button" value="Cancel"/>	

The following table describes the labels in this screen.

Table 26 Advanced Application > Static Multicast Forwarding

LABEL	DESCRIPTION
Active	Select this check box to activate your rule. You may temporarily deactivate a rule without deleting it by clearing this check box.
Name	Type a descriptive name (up to 32 printable ASCII characters) for this static multicast MAC address forwarding rule. This is for identification only.
MAC Address	Enter a multicast MAC address which identifies the multicast group. The last binary bit of the first octet pair in a multicast MAC address must be 1. For example, the first octet pair 00000001 is 01 and 00000011 is 03 in hexadecimal, so 01:00:5e:00:00:0A and 03:00:5e:00:00:27 are valid multicast MAC addresses.
VID	You can forward frames with matching destination MAC address to port(s) within a VLAN group. Enter the ID that identifies the VLAN group here. If you don't have a specific target VLAN, enter 1.
Port	Enter the port(s) where frames with destination MAC address that matched the entry above are forwarded. You can enter multiple ports separated by (no space) comma (,) or hyphen (-). For example, enter "3-5" for ports 3, 4, and 5. Enter "3,5,7" for ports 3, 5, and 7.
Add	Click Add to save your rule to the OLT's run-time memory. The OLT loses this rule if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields to their last saved values.
Clear	Click Clear to begin configuring this screen afresh.
Index	Click an index number to modify a static multicast MAC address rule for port(s).
Active	This field displays whether a static multicast MAC address forwarding rule is active (Yes) or not (No). You may temporarily deactivate a rule without deleting it.
Name	This field displays the descriptive name for identification purposes for a static multicast MAC address-forwarding rule.
MAC Address	This field displays the multicast MAC address that identifies a multicast group.
VID	This field displays the ID number of a VLAN group to which frames containing the specified multicast MAC address will be forwarded.
Port	This field displays the port(s) within an identified VLAN group to which frames containing the specified multicast MAC address will be forwarded.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the check boxes.

CHAPTER 12

Filtering

12.1 Filtering Overview

This chapter discusses MAC address port filtering.

Filtering means sifting traffic going through the OLT based on the source and/or destination MAC addresses and VLAN group (ID).

12.1.1 What You Can Do

Use the **Filtering** screen ([Section 12.2 on page 114](#)) to create rules for traffic going through the OLT.

12.2 Configure a Filtering Rule

Use this screen to create rules for traffic going through the OLT. Click **Advanced Application > Filtering** in the navigation panel to display the screen as shown next.

Figure 73 Advanced Application > Filtering

The screenshot shows the 'Filtering' configuration interface. At the top, there is a header bar with tabs for 'Index', 'Active', 'Name', 'MAC Address', 'VID', 'Action', and 'Delete'. Below the header, there is a form for creating a new rule. The form fields include:

- Active:** A checkbox that is currently unchecked.
- Name:** An input field containing an empty string.
- Action:** Two checkboxes labeled 'Discard source' and 'Discard destination', both of which are unchecked.
- MAC:** An input field consisting of six colon-separated hex digits, all of which are empty.
- VID:** An input field consisting of two colon-separated hex digits, the first of which is empty and the second is also empty.

At the bottom of the form are three buttons: 'Add', 'Cancel', and 'Clear'. Below the form, there is a table with columns for 'Index', 'Active', 'Name', 'MAC Address', 'VID', 'Action', and 'Delete'. The table currently contains one row with the following values:

Index	Active	Name	MAC Address	VID	Action	Delete
						<input type="button" value="Delete"/>

Below the table are two more buttons: 'Delete' and 'Cancel'.

The following table describes the related labels in this screen.

Table 27 Advanced Application > Filtering

LABEL	DESCRIPTION
Active	Make sure to select this check box to activate your rule. You may temporarily deactivate a rule without deleting it by deselecting this check box.
Name	Type a descriptive name (up to 32 printable ASCII characters) for this rule. This is for identification only.
Action	Select Discard source to drop the frames from the source MAC address (specified in the MAC field). The OLT can still send frames to the MAC address. Select Discard destination to drop the frames to the destination MAC address (specified in the MAC address). The OLT can still receive frames originating from the MAC address. Select Discard source and Discard destination to block traffic to/from the MAC address specified in the MAC field.
MAC	Type a MAC address in valid MAC address format, that is, six hexadecimal character pairs.
VID	Type the VLAN group identification number.
Add	Click Add to save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields to your previous configuration.
Clear	Click Clear to clear the fields to the factory defaults.
Index	This field displays the index number of the rule. Click an index number to change the settings.
Active	This field displays Yes when the rule is activated and No when it is deactivated.
Name	This field displays the descriptive name for this rule. This is for identification purpose only.
MAC Address	This field displays the source/destination MAC address with the VLAN identification number to which the MAC address belongs.
VID	This field displays the VLAN group identification number.
Action	This field displays Discard source , Discard destination , or Discard both depending on what you configured above.
Delete	Check the rule(s) that you want to remove and then click the Delete button.
Cancel	Click Cancel to clear the selected checkbox(es).

CHAPTER 13

Spanning Tree Protocol

13.1 Spanning Tree Protocol Overview

The OLT supports Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP) as defined in the following standards.

- IEEE 802.1D Spanning Tree Protocol
- IEEE 802.1w Rapid Spanning Tree Protocol
- IEEE 802.1s Multiple Spanning Tree Protocol

The OLT also allows you to set up multiple STP configurations (or trees). Ports can then be assigned to the trees.

13.1.1 What You Can Do

- Use the **Spanning Tree Protocol Status** screen ([Section 13.2 on page 118](#)) to view the STP status in the different STP modes (RSTP or MSTP) you can configure on the OLT.
- Use the **Spanning Tree Configuration** screen ([Section 13.3 on page 119](#)) to activate one of the STP modes on the OLT.
- Use the **Rapid Spanning Tree Protocol** screen ([Section 13.4 on page 119](#)) to configure RSTP settings.
- Use the **Rapid Spanning Tree Protocol Status** screen ([Section 13.5 on page 121](#)) to view the RSTP status.
- Use the **Multiple Spanning Tree Protocol** screen ([Section 13.6 on page 122](#)) to configure MSTP.
- Use the **Multiple Spanning Tree Protocol Status** screen ([Section 13.7 on page 127](#)) to view the MSTP status.

13.1.2 What You Need to Know

Read on for concepts on STP that can help you configure the screens in this chapter.

(Rapid) Spanning Tree Protocol

(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a switch to interact with other (R)STP -compliant switches in your network to ensure that only one path exists between any two stations on the network.

The OLT uses IEEE 802.1w RSTP (Rapid Spanning Tree Protocol) that allows faster convergence of the spanning tree than STP (while also being backwards compatible with STP-only aware bridges). In RSTP, topology change information is directly propagated throughout the network from the device that generates the topology change. In STP, a longer delay is required as the device that causes a topology change first notifies the root bridge that then notifies the network. Both RSTP and STP flush unwanted

learned addresses from the filtering database. In RSTP, the port states are Discarding, Learning, and Forwarding.

Note: In this user's guide, "STP" refers to both STP and RSTP.

STP Terminology

The root bridge is the base of the spanning tree.

Path cost is the cost of transmitting a frame onto a LAN through that port. The recommended cost is assigned according to the speed of the link to which a port is attached. The slower the media, the higher the cost.

Table 28 STP Path Costs

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

How STP Works

After a bridge determines the lowest cost-spanning tree with STP, it enables the root port and the ports that are the designated ports for connected LANs, and disables all other ports that participate in STP. Network packets are therefore only forwarded between enabled ports, eliminating any possible network loops.

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

Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the root bridge. If a bridge does not get a Hello BPDU after a predefined interval (Max Age), the bridge assumes that the link to the root bridge is down. This bridge then initiates negotiations with other bridges to reconfigure the network to re-establish a valid network topology.

STP Port States

STP assigns five port states to eliminate packet looping. A bridge port is not allowed to go directly from blocking state to forwarding state so as to eliminate transient loops.

Table 29 STP Port States

PORT STATE	DESCRIPTION
Disabled	STP is disabled (default).
Blocking	Only configuration and management BPDUs are received and processed.
Listening	All BPDUs are received and processed. Note: The listening state does not exist in RSTP.
Learning	All BPDUs are received and processed. Information frames are submitted to the learning process but not forwarded.
Forwarding	All BPDUs are received and processed. All information frames are received and forwarded.

Multiple STP

Multiple Spanning Tree Protocol (IEEE 802.1s) is backward compatible with STP/RSTP and addresses the limitations of existing spanning tree protocols (STP and RSTP) in networks to include the following features:

- One Common and Internal Spanning Tree (CIST) that represents the entire network's connectivity.
- Grouping of multiple bridges (or switching devices) into regions that appear as one single bridge on the network.
- A VLAN can be mapped to a specific Multiple Spanning Tree Instance (MSTI). MSTI allows multiple VLANs to use the same spanning tree.
- Load-balancing is possible as traffic from different VLANs can use distinct paths in a region.

13.2 Spanning Tree Protocol Status Screen

The Spanning Tree Protocol status screen changes depending on what standard you choose to implement on your network. Click **Advanced Application > Spanning Tree Protocol** to see the screen as shown.

Figure 74 Advanced Application > Spanning Tree Protocol

Spanning Tree Protocol: RSTP		Configuration	RSTP	MSTP
Bridge	Root	Our Bridge		
Bridge ID	0000-000000000000	0000-000000000000		
Hello Time (second)	0	0		
Max Age (second)	0	0		
Forwarding Delay (second)	0	0		
Cost to Bridge	0			
Port ID	0X0000			
Topology Changed Times	0			
Time Since Last Change	0:00:00			

This screen differs depending on which STP mode (RSTP or MSTP) you configure on the OLT. This screen is described in detail in the section that follows the configuration section for each STP mode. Click **Configuration** to activate one of the STP standards on the OLT.

13.3 Spanning Tree Configuration

Use the **Spanning Tree Configuration** screen to activate one of the STP modes on the OLT. Click **Configuration** in the **Advanced Application > Spanning Tree Protocol**.

Figure 75 Advanced Application > Spanning Tree Protocol > Configuration



The following table describes the labels in this screen.

Table 30 Advanced Application > Spanning Tree Protocol > Configuration

LABEL	DESCRIPTION
Spanning Tree Mode	You can activate one of the STP modes on the OLT. Select Rapid Spanning Tree or Multiple Spanning Tree . See Section 13.1 on page 116 for background information on STP.
Apply	Click Apply to save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

13.4 Configure Rapid Spanning Tree Protocol

Use this screen to configure RSTP settings, see [Section 13.1 on page 116](#) for more information on RSTP. Click **RSTP** in the **Advanced Application > Spanning Tree Protocol** screen.

Figure 76 Advanced Application > Spanning Tree Protocol > RSTP

The screenshot shows the RSTP configuration interface. At the top, there is a header bar with the title "Rapid Spanning Tree Protocol" and a "Status" button. Below this is a table with four rows of configuration parameters:

Active	<input type="checkbox"/>
Bridge Priority	32768 ▾
Hello Time	2 Seconds
MAX Age	20 Seconds

Below the configuration table is a large table titled "Port" with columns: Port, Active, Edge, Priority, and Path Cost. The table lists 24 ports (1 through 24) and includes a topology diagram at the bottom. The "Active" column contains checkboxes, and the "Edge" column contains checkboxes. The "Priority" column shows values such as 128 or 4, and the "Path Cost" column shows values such as 4 or 2. The topology diagram shows connections between ports 8, 18, 19, 20, 21, 22, 23, and 24.

At the bottom of the screen are two buttons: "Apply" and "Cancel".

The following table describes the labels in this screen.

Table 31 Advanced Application > Spanning Tree Protocol > RSTP

LABEL	DESCRIPTION
Status	Click Status to display the RSTP Status screen (see Figure 77 on page 122).
Active	Select this check box to activate RSTP. Clear this checkbox to disable RSTP. Note: You must also activate Rapid Spanning Tree in the Advanced Application > Spanning Tree Protocol > Configuration screen to enable RSTP on the OLT.
Bridge Priority	Bridge priority is used in determining the root switch, root port and designated port. 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. Select a value from the drop-down list box. The lower the numeric value you assign, the higher the priority for this bridge. 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.
Max Age	This is the maximum time (in seconds) the OLT can wait without receiving a BPDU before attempting to reconfigure. All OLT 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 OLT ports attached to the network. The allowed range is 6 to 40 seconds.

Table 31 Advanced Application > Spanning Tree Protocol > RSTP (continued)

LABEL	DESCRIPTION
Forwarding Delay	This is the maximum time (in seconds) the OLT 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: Note: $2 * (\text{Forward Delay} - 1) \geq \text{Max Age} \geq 2 * (\text{Hello Time} + 1)$
Port	This field displays the port number. * means all ports.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to activate RSTP on this port.
Edge	Select this check box to configure a port as an edge port when it is directly attached to a computer. An edge port changes its initial STP port state from blocking state to forwarding state immediately without going through listening and learning states right after the port is configured as an edge port or when its link status changes. Note: An edge port becomes a non-edge port as soon as it receives a Bridge Protocol Data Unit (BPDU).
Priority	Configure the priority for each port here. Priority decides which port should be disabled when more than one port forms a loop in a switch. Ports with a higher priority numeric value are disabled first. The allowed range is between 0 and 255 and the default value is 128.
Path Cost	Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost - see Table 28 on page 117 for more information.
Apply	Click Apply to save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

13.5 Rapid Spanning Tree Protocol Status

Click **Advanced Application > Spanning Tree Protocol** in the navigation panel to display the status screen as shown next. See [Section 13.1 on page 116](#) for more information on RSTP.

Note: This screen is only available after you activate RSTP on the OLT.

Figure 77 Advanced Application > Spanning Tree Protocol > Status: RSTP

Spanning Tree Protocol: RSTP		Configuration	RSTP	MSTP
Bridge	Root	Our Bridge		
Bridge ID	0000-000000000000	0000-000000000000		
Hello Time (second)	0	0		
Max Age (second)	0	0		
Forwarding Delay (second)	0	0		
Cost to Bridge	0			
Port ID	0X0000			
Topology Changed Times	0			
Time Since Last Change	0:00:00			

The following table describes the labels in this screen.

Table 32 Advanced Application > Spanning Tree Protocol > Status: RSTP

LABEL	DESCRIPTION
Configuration	Click Configuration to specify which STP mode you want to activate. Click RSTP to edit RSTP settings on the OLT.
Bridge	Root refers to the base of the spanning tree (the root bridge). Our Bridge is this switch. This OLT may also be the root bridge.
Bridge ID	This is the unique identifier for this bridge, consisting of bridge priority plus MAC address. This ID is the same for Root and Our Bridge if the OLT is the root switch.
Hello Time (second)	This is the time interval (in seconds) at which the root switch transmits a configuration message. The root bridge determines Hello Time, Max Age and Forwarding Delay.
Max Age (second)	This is the maximum time (in seconds) the OLT can wait without receiving a configuration message before attempting to reconfigure.
Forwarding Delay (second)	This is the time (in seconds) the root switch will wait before changing states (that is, listening to learning to forwarding).
	Note: The listening state does not exist in RSTP.
Cost to Bridge	This is the path cost from the root port on this OLT to the root switch.
Port ID	This is the priority and number of the port on the OLT through which this OLT must communicate with the root of the Spanning Tree.
Topology Changed Times	This is the number of times the spanning tree has been reconfigured.
Time Since Last Change	This is the time since the spanning tree was last reconfigured.

13.6 Configure Multiple Spanning Tree Protocol

To configure MSTP, click **MSTP** in the **Advanced Application > Spanning Tree Protocol** screen. See [Multiple STP on page 118](#) for more information on MSTP.

Figure 78 Advanced Application > Spanning Tree Protocol > MSTP

Multiple Spanning Tree Protocol

		Port	Status																																																																				
Bridge:																																																																							
Active	<input type="checkbox"/>																																																																						
Hello Time	2	seconds																																																																					
MAX Age	20	seconds																																																																					
Forwarding Delay	15	seconds																																																																					
Maximum hops	20																																																																						
Configuration Name	5cf4ab9ce758																																																																						
Revision Number	0																																																																						
Apply Cancel																																																																							
Instance:																																																																							
Instance	<input type="text" value="32768"/>																																																																						
Bridge Priority	<input type="text" value="32768"/>																																																																						
VLAN Range	<input type="button" value="Start"/>	<input type="button" value="End"/>	<input type="button" value="Add"/> <input type="button" value="Remove"/> <input type="button" value="Clear"/>																																																																				
Enabled VLAN(s)																																																																							
<table border="1"> <thead> <tr> <th>Port</th> <th>Active</th> <th>Priority</th> <th>Path Cost</th> </tr> </thead> <tbody> <tr><td>*</td><td><input type="checkbox"/></td><td></td><td></td></tr> <tr><td>1</td><td><input type="checkbox"/></td><td>128</td><td>4</td></tr> <tr><td>2</td><td><input type="checkbox"/></td><td>128</td><td>4</td></tr> <tr><td>3</td><td><input type="checkbox"/></td><td>128</td><td>4</td></tr> <tr><td>4</td><td><input type="checkbox"/></td><td>128</td><td>4</td></tr> <tr><td>5</td><td><input type="checkbox"/></td><td>128</td><td>4</td></tr> <tr><td>6</td><td><input type="checkbox"/></td><td>128</td><td>4</td></tr> <tr><td>7</td><td><input type="checkbox"/></td><td>128</td><td>4</td></tr> <tr><td>17</td><td><input type="checkbox"/></td><td>128</td><td>4</td></tr> <tr><td>18</td><td><input type="checkbox"/></td><td>128</td><td>4</td></tr> <tr><td>19</td><td><input type="checkbox"/></td><td>128</td><td>4</td></tr> <tr><td>20</td><td><input type="checkbox"/></td><td>128</td><td>4</td></tr> <tr><td>21</td><td><input type="checkbox"/></td><td>128</td><td>2</td></tr> <tr><td>22</td><td><input type="checkbox"/></td><td>128</td><td>2</td></tr> <tr><td>23</td><td><input type="checkbox"/></td><td>128</td><td>2</td></tr> <tr><td>24</td><td><input type="checkbox"/></td><td>128</td><td>2</td></tr> </tbody> </table>				Port	Active	Priority	Path Cost	*	<input type="checkbox"/>			1	<input type="checkbox"/>	128	4	2	<input type="checkbox"/>	128	4	3	<input type="checkbox"/>	128	4	4	<input type="checkbox"/>	128	4	5	<input type="checkbox"/>	128	4	6	<input type="checkbox"/>	128	4	7	<input type="checkbox"/>	128	4	17	<input type="checkbox"/>	128	4	18	<input type="checkbox"/>	128	4	19	<input type="checkbox"/>	128	4	20	<input type="checkbox"/>	128	4	21	<input type="checkbox"/>	128	2	22	<input type="checkbox"/>	128	2	23	<input type="checkbox"/>	128	2	24	<input type="checkbox"/>	128	2
Port	Active	Priority	Path Cost																																																																				
*	<input type="checkbox"/>																																																																						
1	<input type="checkbox"/>	128	4																																																																				
2	<input type="checkbox"/>	128	4																																																																				
3	<input type="checkbox"/>	128	4																																																																				
4	<input type="checkbox"/>	128	4																																																																				
5	<input type="checkbox"/>	128	4																																																																				
6	<input type="checkbox"/>	128	4																																																																				
7	<input type="checkbox"/>	128	4																																																																				
17	<input type="checkbox"/>	128	4																																																																				
18	<input type="checkbox"/>	128	4																																																																				
19	<input type="checkbox"/>	128	4																																																																				
20	<input type="checkbox"/>	128	4																																																																				
21	<input type="checkbox"/>	128	2																																																																				
22	<input type="checkbox"/>	128	2																																																																				
23	<input type="checkbox"/>	128	2																																																																				
24	<input type="checkbox"/>	128	2																																																																				
Add Cancel																																																																							
Instance	VLAN	Active Port	Delete																																																																				
0	1-4094	-	<input type="button" value="Delete"/>																																																																				
Delete Cancel																																																																							

The following table describes the labels in this screen.

Table 33 Advanced Application > Spanning Tree Protocol > MSTP

LABEL	DESCRIPTION
Port	Click Port to display the MSTP Port screen (see Figure 79 on page 126).
Status	Click Status to display the MSTP Status screen (see Figure 80 on page 127).
Active	Select this to activate MSTP on the OLT. Clear this to disable MSTP on the OLT. Note: You must also activate Multiple Spanning Tree in the Advanced Application > Spanning Tree Protocol > Configuration screen to enable MSTP on the OLT.
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.
Max Age	This is the maximum time (in seconds) the OLT can wait without receiving a BPDU before attempting to reconfigure. All OLT 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 OLT ports attached to the network. The allowed range is 6 to 40 seconds.
Forwarding Delay	This is the maximum time (in seconds) the OLT 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: Note: $2 * (\text{Forward Delay} - 1) \geq \text{Max Age} \geq 2 * (\text{Hello Time} + 1)$
Maximum hops	Enter the number of hops (between 1 and 255) in an MSTP region before the BPDU is discarded and the port information is aged.
Configuration Name	Enter a descriptive name (up to 32 characters) of an MST region.
Revision Number	Enter a number to identify a region's configuration. Devices must have the same revision number to belong to the same region.
Apply	Click Apply to save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Instance	Use this section to configure MSTI (Multiple Spanning Tree Instance) settings.
Instance	Enter the number you want to use to identify this MST instance on the OLT. Note: The OLT supports instance numbers 0-16.
Bridge Priority	Set the priority of the OLT for the specific spanning tree instance. The lower the number, the more likely the OLT will be chosen as the root bridge within the spanning tree instance. Enter priority values between 0 and 61440 in increments of 4096 (thus valid values are 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344 and 61440).
VLAN Range	Enter the start of the VLAN ID range that you want to add or remove from the VLAN range edit area in the Start field. Enter the end of the VLAN ID range that you want to add or remove from the VLAN range edit area in the End field. Next click: <ul style="list-style-type: none">• Add - to add this range of VLAN(s) to be mapped to the MST instance.• Remove - to remove this range of VLAN(s) from being mapped to the MST instance.• Clear - to remove all VLAN(s) from being mapped to this MST instance.
Enabled VLAN(s)	This field displays which VLAN(s) are mapped to this MST instance.
Port	This field displays the port number. * means all ports.

Table 33 Advanced Application > Spanning Tree Protocol > MSTP (continued)

LABEL	DESCRIPTION
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to add this port to the MST instance.
Priority	Configure the priority for each port here. Priority decides which port should be disabled when more than one port forms a loop in a switch. Ports with a higher priority numeric value are disabled first. The allowed range is between 0 and 255 and the default value is 128.
Path Cost	Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost - see Table 28 on page 117 for more information.
Add	Click Add to save this MST instance to the OLT's run-time memory. The OLT loses this change if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Instance	This field displays the ID of an MST instance.
VLAN	This field displays the VID (or VID ranges) to which the MST instance is mapped.
Active Port	This field displays the ports configured to participate in the MST instance.
	Select an entry's check box to select a specific entry.
Delete	Check the rule(s) that you want to remove and then click the Delete button.
Cancel	Click Cancel to clear the selected checkbox(es).

13.6.1 Multiple Spanning Tree Protocol Port Configuration

Click **Advanced Application > Spanning Tree Protocol > MSTP > Port** in the navigation panel to display the status screen as shown next. See [Multiple STP on page 118](#) for more information on MSTP.

Figure 79 Advanced Application > Spanning Tree Protocol > MSTP > Port

Port	Edge
*	<input type="checkbox"/>
1	<input checked="" type="checkbox"/>
2	<input checked="" type="checkbox"/>
3	<input checked="" type="checkbox"/>
4	<input checked="" type="checkbox"/>
5	<input checked="" type="checkbox"/>
6	<input checked="" type="checkbox"/>
7	<input checked="" type="checkbox"/>
8	<input checked="" type="checkbox"/>
9	<input type="checkbox"/>
10	<input checked="" type="checkbox"/>
11	<input checked="" type="checkbox"/>
12	<input checked="" type="checkbox"/>
13	<input checked="" type="checkbox"/>
14	<input checked="" type="checkbox"/>
15	<input checked="" type="checkbox"/>
16	<input checked="" type="checkbox"/>
17	<input type="checkbox"/>
18	<input checked="" type="checkbox"/>
19	<input checked="" type="checkbox"/>
20	<input checked="" type="checkbox"/>
21	<input checked="" type="checkbox"/>
22	<input checked="" type="checkbox"/>
23	<input checked="" type="checkbox"/>
24	<input checked="" type="checkbox"/>

MSTP

Apply **Cancel**

The following table describes the labels in this screen.

Table 34 Advanced Application > Spanning Tree Protocol > MSTP > Port

LABEL	DESCRIPTION
MSTP	Click MSTP to edit MSTP settings on the OLT.
Port	This field displays the port number. * means all ports.
*	<p>Settings in this row apply to all ports.</p> <p>Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis.</p> <p>Note: Changes in this row are copied to all the ports as soon as you make them.</p>
Edge	<p>Select this check box to configure a port as an edge port when it is directly attached to a computer. An edge port changes its initial STP port state from blocking state to forwarding state immediately without going through listening and learning states right after the port is configured as an edge port or when its link status changes.</p> <p>Note: An edge port becomes a non-edge port as soon as it receives a Bridge Protocol Data Unit (BPDU).</p>
Apply	Click Apply to save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

13.7 Multiple Spanning Tree Protocol Status

Click **Advanced Application > Spanning Tree Protocol** in the navigation panel to display the status screen as shown next. See [Multiple STP on page 118](#) for more information on MSTP.

Note: This screen is only available after you activate MSTP on the OLT.

Figure 80 Advanced Application > Spanning Tree Protocol > Status: MSTP

Spanning Tree Protocol Status		Configuration RSTP MSTP																																				
Spanning Tree Protocol: MSTP																																						
CST																																						
<table><tr><td>Bridge</td><td>Root</td><td>Our Bridge</td></tr><tr><td>Bridge ID</td><td>0-000000000000</td><td>8000-000000000000</td></tr><tr><td>Hello Time (second)</td><td>0</td><td>2</td></tr><tr><td>Max Age (second)</td><td>0</td><td>20</td></tr><tr><td>Forwarding Delay (second)</td><td>0</td><td>15</td></tr><tr><td>Cost to Bridge</td><td>0</td><td>0</td></tr><tr><td>Port ID</td><td>0x0000</td><td>0x0000</td></tr><tr><td>Configuration Name</td><td colspan="2">5cf4ab9ce758</td></tr><tr><td>Revision Number</td><td colspan="2">0</td></tr><tr><td>Configuration Digest</td><td colspan="2">AC36177F50283CD4B83821D8AB26DE62</td></tr><tr><td>Topology Changed Times</td><td colspan="2">0</td></tr><tr><td>Time Since Last Change</td><td colspan="2" rowspan="3">0:00:00</td></tr></table>			Bridge	Root	Our Bridge	Bridge ID	0-000000000000	8000-000000000000	Hello Time (second)	0	2	Max Age (second)	0	20	Forwarding Delay (second)	0	15	Cost to Bridge	0	0	Port ID	0x0000	0x0000	Configuration Name	5cf4ab9ce758		Revision Number	0		Configuration Digest	AC36177F50283CD4B83821D8AB26DE62		Topology Changed Times	0		Time Since Last Change	0:00:00	
Bridge	Root	Our Bridge																																				
Bridge ID	0-000000000000	8000-000000000000																																				
Hello Time (second)	0	2																																				
Max Age (second)	0	20																																				
Forwarding Delay (second)	0	15																																				
Cost to Bridge	0	0																																				
Port ID	0x0000	0x0000																																				
Configuration Name	5cf4ab9ce758																																					
Revision Number	0																																					
Configuration Digest	AC36177F50283CD4B83821D8AB26DE62																																					
Topology Changed Times	0																																					
Time Since Last Change	0:00:00																																					
Instance:																																						
<table><tr><td>Instance</td><td>VLAN</td></tr><tr><td>0</td><td>1-4094</td></tr></table>			Instance	VLAN	0	1-4094																																
Instance	VLAN																																					
0	1-4094																																					
MSTI <input type="button" value="1"/> ▼																																						
<table><tr><td>Bridge</td><td>Regional Root</td><td>Our Bridge</td></tr><tr><td>Bridge ID</td><td>0000-000000000000</td><td>8001-000000000000</td></tr><tr><td>Internal Cost</td><td>0</td><td>0</td></tr><tr><td>Port ID</td><td>0x0000</td><td>0x0000</td></tr></table>			Bridge	Regional Root	Our Bridge	Bridge ID	0000-000000000000	8001-000000000000	Internal Cost	0	0	Port ID	0x0000	0x0000																								
Bridge	Regional Root	Our Bridge																																				
Bridge ID	0000-000000000000	8001-000000000000																																				
Internal Cost	0	0																																				
Port ID	0x0000	0x0000																																				

The following table describes the labels in this screen.

Table 35 Advanced Application > Spanning Tree Protocol > Status: MSTP

LABEL	DESCRIPTION
Configuration	Click Configuration to specify which STP mode you want to activate. Click MSTP to edit MSTP settings on the OLT.
CST	This section describes the Common Spanning Tree settings.
Bridge	Root refers to the base of the spanning tree (the root bridge). Our Bridge is this switch. This OLT may also be the root bridge.
Bridge ID	This is the unique identifier for this bridge, consisting of bridge priority plus MAC address. This ID is the same for Root and Our Bridge if the OLT is the root switch.
Hello Time (second)	This is the time interval (in seconds) at which the root switch transmits a configuration message. The root bridge determines Hello Time, Max Age and Forwarding Delay.
Max Age (second)	This is the maximum time (in seconds) the OLT can wait without receiving a configuration message before attempting to reconfigure.
Forwarding Delay (second)	This is the time (in seconds) the root switch will wait before changing states (that is, listening to learning to forwarding).
Cost to Bridge	This is the path cost from the root port on this OLT to the root switch.

Table 35 Advanced Application > Spanning Tree Protocol > Status: MSTP (continued)

LABEL	DESCRIPTION
Port ID	This is the priority and number of the port on the OLT through which this OLT must communicate with the root of the Spanning Tree.
Configuration Name	This field displays the configuration name for this MST region.
Revision Number	This field displays the revision number for this MST region.
Configuration Digest	A configuration digest is generated from the VLAN-MSTI mapping information. This field displays the 16-octet signature that is included in an MSTP BPDU. This field displays the digest when MSTP is activated on the system.
Topology Changed Times	This is the number of times the spanning tree has been reconfigured.
Time Since Last Change	This is the time since the spanning tree was last reconfigured.
Instance	These fields display the MSTI to VLAN mapping. In other words, which VLANs run on each spanning tree instance.
Instance	This field displays the MSTI ID.
VLAN	This field displays which VLANs are mapped to an MSTI.
MSTI	Select the MST instance settings you want to view.
Bridge	Root refers to the base of the MST instance. Our Bridge is this switch. This OLT may also be the root bridge.
Bridge ID	This is the unique identifier for this bridge, consisting of bridge priority plus MAC address. This ID is the same for Root and Our Bridge if the OLT is the root switch.
Internal Cost	This is the path cost from the root port in this MST instance to the regional root switch.
Port ID	This is the priority and number of the port on the OLT through which this OLT must communicate with the root of the MST instance.

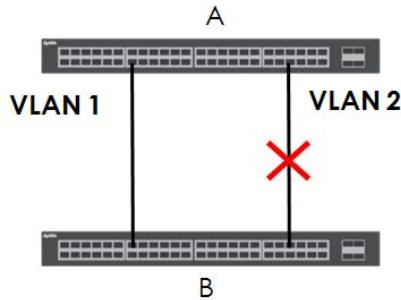
13.8 Technical Reference

This section provides technical background information on the topics discussed in this chapter.

13.8.1 MSTP Network Example

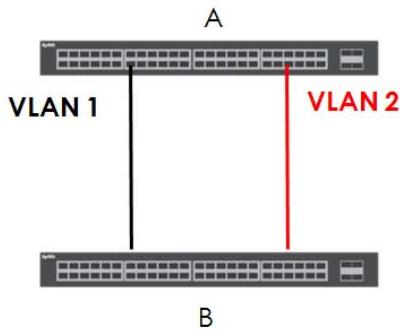
The following figure shows a network example where two VLANs are configured on the two switches. If the switches are using STP or RSTP, the link for VLAN 2 will be blocked as STP and RSTP allow only one link in the network and block the redundant link.

Figure 81 STP/RSTP Network Example



With MSTP, VLANs 1 and 2 are mapped to different spanning trees in the network. Thus traffic from the two VLANs travel on different paths. The following figure shows the network example using MSTP.

Figure 82 MSTP Network Example



13.8.2 MST Region

An MST region is a logical grouping of multiple network devices that appears as a single device to the rest of the network. Each MSTP-enabled device can only belong to one MST region. When BPDUs enter an MST region, external path cost (of paths outside this region) is increased by one. Internal path cost (of paths within this region) is increased by one when BPDUs traverse the region.

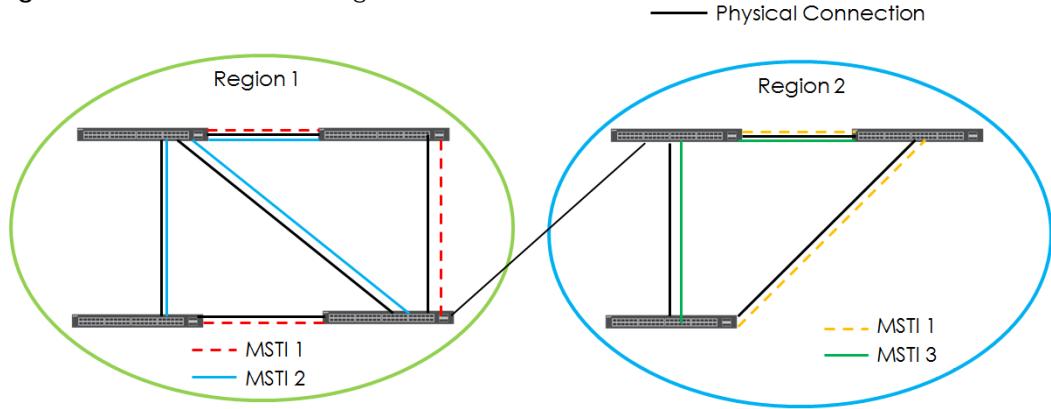
Devices that belong to the same MST region are configured to have the same MSTP configuration identification settings. These include the following parameters:

- Name of the MST region
- Revision level as the unique number for the MST region
- VLAN-to-MST Instance mapping

13.8.3 MST Instance

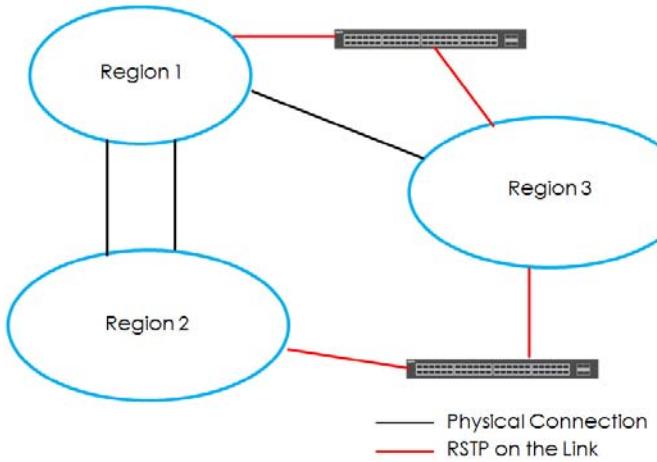
An MST Instance (MSTI) is a spanning tree instance. VLANs can be configured to run on a specific MSTI. Each created MSTI is identified by a unique number (known as an MST ID) known internally to a region. Thus an MSTI does not span across MST regions.

The following figure shows an example where there are two MST regions. Regions 1 and 2 have 2 spanning tree instances.

Figure 83 MSTIs in Different Regions

13.8.4 Common and Internal Spanning Tree (CIST)

A CIST represents the connectivity of the entire network and it is equivalent to a spanning tree in an STP/RSTP. The CIST is the default MST instance (MSTID 0). Any VLANs that are not members of an MST instance are members of the CIST. In an MSTP-enabled network, there is only one CIST that runs between MST regions and single spanning tree devices. A network may contain multiple MST regions and other network segments running RSTP.

Figure 84 MSTP and Legacy RSTP Network Example

CHAPTER 14

Bandwidth Control

14.1 Bandwidth Control Overview

This chapter shows you how you can cap the maximum bandwidth using the **Bandwidth Control** screen.

Bandwidth control means defining a maximum allowable bandwidth for incoming and/or out-going traffic flows on a port.

14.1.1 What You Can Do

Use the **Bandwidth Control** screen ([Section 14.2 on page 131](#)) to limit the bandwidth for traffic going through the OLT.

14.2 Bandwidth Control Setup

Click **Advanced Application > Bandwidth Control** in the navigation panel to bring up the screen as shown next.

Figure 85 Advanced Application > Bandwidth Control

Port	Ingress Rate		Egress Rate			
	Active	Commit Rate Kbps	Active	Peak Rate Kbps	Active	Kbps
*	<input checked="" type="checkbox"/>					
1	<input type="checkbox"/>	1	<input type="checkbox"/>	1	<input type="checkbox"/>	1
2	<input type="checkbox"/>	1	<input type="checkbox"/>	1	<input type="checkbox"/>	1
3	<input type="checkbox"/>	1	<input type="checkbox"/>	1	<input type="checkbox"/>	1
4	<input type="checkbox"/>	1	<input type="checkbox"/>	1	<input type="checkbox"/>	1
5	<input type="checkbox"/>	1	<input type="checkbox"/>	1	<input type="checkbox"/>	1
6	<input type="checkbox"/>	1	<input type="checkbox"/>	1	<input type="checkbox"/>	1
7	<input type="checkbox"/>	1	<input type="checkbox"/>	1	<input type="checkbox"/>	1
8	<input type="checkbox"/>	1	<input type="checkbox"/>	1	<input type="checkbox"/>	1
9	<input type="checkbox"/>	1	<input type="checkbox"/>	1	<input type="checkbox"/>	1
10	<input type="checkbox"/>	1	<input type="checkbox"/>	1	<input type="checkbox"/>	1
16	<input type="checkbox"/>	1	<input type="checkbox"/>	1	<input type="checkbox"/>	4
18	<input type="checkbox"/>	1	<input type="checkbox"/>	1	<input type="checkbox"/>	1
19	<input type="checkbox"/>	1	<input type="checkbox"/>	1	<input type="checkbox"/>	1
20	<input type="checkbox"/>	1	<input type="checkbox"/>	1	<input type="checkbox"/>	1
21	<input type="checkbox"/>	1	<input type="checkbox"/>	1	<input type="checkbox"/>	1
22	<input type="checkbox"/>	1	<input type="checkbox"/>	1	<input type="checkbox"/>	1
23	<input type="checkbox"/>	1	<input type="checkbox"/>	1	<input type="checkbox"/>	1
24	<input type="checkbox"/>	1	<input type="checkbox"/>	1	<input type="checkbox"/>	1

Apply **Cancel**

The following table describes the related labels in this screen.

Table 36 Advanced Application > Bandwidth Control

LABEL	DESCRIPTION
Active	Select this check box to enable bandwidth control on the OLT.
Port	This field displays the port number. * means all ports.
*	<p>Settings in this row apply to all ports.</p> <p>Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis.</p> <p>Note: Changes in this row are copied to all the ports as soon as you make them.</p>
Ingress Rate	<p>Specify the maximum bandwidth allowed in kilobits per second (Kbps) for the incoming traffic flow on a port.</p> <p>Note: Ingress rate bandwidth control applies to layer 2 traffic only.</p>
Active	Select this check box to activate commit rate limits on this port.
Commit Rate	Specify the guaranteed bandwidth allowed in kilobits per second (Kbps) for the incoming traffic flow on a port. The commit rate should be less than the peak rate. The sum of commit rates cannot be greater than or equal to the uplink bandwidth.
Active	Select this check box to activate peak rate limits on this port.

Table 36 Advanced Application > Bandwidth Control (continued)

LABEL	DESCRIPTION
Peak Rate	Specify the maximum bandwidth allowed in kilobits per second (Kbps) for the incoming traffic flow on a port.
Active	Select this check box to activate peak rate limits on this port.
Egress Rate	Specify the maximum bandwidth allowed in kilobits per second (Kbps) for the out-going traffic flow on a port.
Apply	Click Apply to save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields.

CHAPTER 15

Broadcast Storm Control

15.1 Broadcast Storm Control Overview

This chapter introduces and shows you how to configure the broadcast storm control feature.

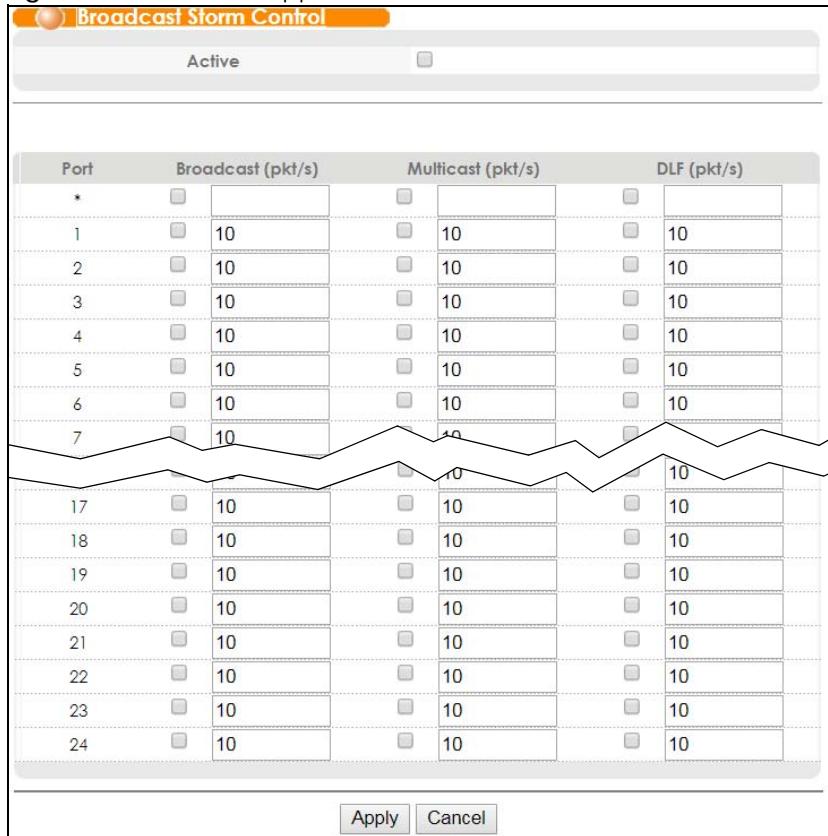
Broadcast storm control limits the number of broadcast, multicast and destination lookup failure (DLF) packets the OLT receives per second on the ports. When the maximum number of allowable broadcast, multicast and/or DLF packets is reached per second, the subsequent packets are discarded. Enable this feature to reduce broadcast, multicast and/or DLF packets in your network. You can specify limits for each packet type on each port.

15.1.1 What You Can Do

Use the **Broadcast Storm Control** screen ([Section 15.2 on page 134](#)) to limit the number of broadcast, multicast and destination lookup failure (DLF) packets the OLT receives per second on the ports.

15.2 Broadcast Storm Control Setup

Click **Advanced Application > Broadcast Storm Control** in the navigation panel to display the screen as shown next.

Figure 86 Advanced Application > Broadcast Storm Control

The following table describes the labels in this screen.

Table 37 Advanced Application > Broadcast Storm Control

LABEL	DESCRIPTION
Active	Select this check box to enable traffic storm control on the OLT. Clear this check box to disable this feature.
Port	This field displays the port number. * means all ports.
*	<p>Settings in this row apply to all ports.</p> <p>Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis.</p> <p>Note: Changes in this row are copied to all the ports as soon as you make them.</p>
Broadcast (pkt/s)	Select this option and specify how many broadcast packets the port receives per second.
Multicast (pkt/s)	Select this option and specify how many multicast packets the port receives per second.
DLF (pkt/s)	Select this option and specify how many destination lookup failure (DLF) packets the port receives per second.
Apply	Click Apply to save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields.

CHAPTER 16

Mirroring

16.1 Mirroring Overview

This chapter discusses port mirroring setup screens.

Port mirroring allows you to copy a traffic flow to a monitor port (the port you copy the traffic to) in order that you can examine the traffic from the monitor port without interference.

16.1.1 What You Can Do

Use the **Mirroring** screen ([Section 16.2 on page 136](#)) to select a monitor port and specify the traffic flow to be copied to the monitor port.

16.2 Port Mirroring Setup

Click **Advanced Application > Mirroring** in the navigation panel to display the **Mirroring** screen. Use this screen to select a monitor port and specify the traffic flow to be copied to the monitor port.

Figure 87 Advanced Application > Mirroring

Port	Mirrored	Direction
*	<input type="checkbox"/>	Ingress ▼
1	<input checked="" type="checkbox"/>	Ingress ▼
2	<input checked="" type="checkbox"/>	Ingress ▼
3	<input checked="" type="checkbox"/>	Ingress ▼
4	<input checked="" type="checkbox"/>	Ingress ▼
5	<input checked="" type="checkbox"/>	Ingress ▼
6	<input checked="" type="checkbox"/>	Ingress ▼
7	<input type="checkbox"/>	Ingress ▼
16	<input checked="" type="checkbox"/>	Ingress ▼
17	<input checked="" type="checkbox"/>	Ingress ▼
18	<input checked="" type="checkbox"/>	Ingress ▼
19	<input checked="" type="checkbox"/>	Ingress ▼
20	<input checked="" type="checkbox"/>	Ingress ▼
21	<input checked="" type="checkbox"/>	Ingress ▼
22	<input checked="" type="checkbox"/>	Ingress ▼
23	<input checked="" type="checkbox"/>	Ingress ▼
24	<input checked="" type="checkbox"/>	Ingress ▼

Apply **Cancel**

The following table describes the labels in this screen.

Table 38 Advanced Application > Mirroring

LABEL	DESCRIPTION
Active	Select this check box to activate port mirroring on the OLT. Clear this check box to disable the feature.
Monitor Port	The monitor port 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 port(s). Enter the port number of the monitor port.
Mirror Vlan	Select the mirror VLAN over which the mirrored traffic is forwarded.
Port	This field displays the port number. * means all ports.
*	<p>Settings in this row apply to all ports.</p> <p>Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis.</p> <p>Note: Changes in this row are copied to all the ports as soon as you make them.</p>
Mirrored	Select this option to mirror the traffic on a port.
Direction	Specify the direction of the traffic to mirror by selecting from the drop-down list box. Choices are Egress (outgoing), Ingress (incoming) and Both .
Apply	Click Apply to save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields.

CHAPTER 17

Link Aggregation

17.1 Link Aggregation Overview

This chapter shows you how to logically aggregate physical links to form one logical, higher-bandwidth link.

Link aggregation (trunking) is the grouping of physical ports into one logical higher-capacity link. You may want to trunk ports if for example, it is cheaper to use multiple lower-speed links than to under-utilize a high-speed, but more costly, single-port link. However, the more ports you aggregate then the fewer available ports you have. A trunk group is one logical link containing multiple ports.

The beginning port of each trunk group must be physically connected to form a trunk group.

17.1.1 What You Can Do

- Use the **Link Aggregation Status** screen ([Section 17.2 on page 139](#)) to view ports you have configured to be in the trunk group, ports that are currently transmitting data as one logical link in the trunk group and so on.
- Use the **Link Aggregation Setting** screen ([Section 17.3 on page 140](#)) to configure to enable static link aggregation.
- Use the **Link Aggregation Control Protocol** screen ([Section 17.3.1 on page 142](#)) to enable Link Aggregation Control Protocol (LACP).

17.1.2 What You Need to Know

The OLT supports both static and dynamic link aggregation.

Note: In a properly planned network, it is recommended to implement static link aggregation only. This ensures increased network stability and control over the trunk groups on your OLT.

See [Section 17.4.1 on page 144](#) for a static port trunking example.

Dynamic Link Aggregation

The OLT adheres to the IEEE 802.3ad standard for static and dynamic (LACP) port trunking.

The IEEE 802.3ad standard describes the Link Aggregation Control Protocol (LACP) for dynamically creating and managing trunk groups.

When you enable LACP link aggregation on a port, the port can automatically negotiate with the ports at the remote end of a link to establish trunk groups. LACP also allows port redundancy, that is, if an

operational port fails, then one of the “standby” ports become operational without user intervention. Please note that:

- You must connect all ports point-to-point to the same Ethernet switch and configure the ports for LACP trunking.
- LACP only works on full-duplex links.
- All ports in the same trunk group must have the same media type, speed, duplex mode and flow control settings.

Configure trunk groups or LACP before you connect the Ethernet switch to avoid causing network topology loops.

Link Aggregation ID

LACP aggregation ID consists of the following information¹:

Table 39 Link Aggregation ID: Local Switch

SYSTEM PRIORITY	MAC ADDRESS	KEY	PORT PRIORITY	PORT NUMBER
0000	00-00-00-00-00-00	0000	00	0000

Table 40 Link Aggregation ID: Peer Switch

SYSTEM PRIORITY	MAC ADDRESS	KEY	PORT PRIORITY	PORT NUMBER
0000	00-00-00-00-00-00	0000	00	0000

17.2 Link Aggregation Status

Click **Advanced Application > Link Aggregation** in the navigation panel. The **Link Aggregation Status** screen displays by default. See [Section 17.1 on page 138](#) for more information.

Figure 88 Advanced Application > Link Aggregation

The screenshot shows a table titled "Link Aggregation Status" with 12 rows, each representing a trunk group (T1 to T12). The columns are: Group ID, Enabled Ports, Synchronized Ports, Aggregator ID, Criteria, and Status. Most entries in the table are "-". Under "Criteria", all rows show "src-dst-mac". Under "Status", all rows show "-".

Link Aggregation Status		Link Aggregation Setting			
Group ID	Enabled Ports	Synchronized Ports	Aggregator ID	Criteria	Status
T1	-	-	-	src-dst-mac	-
T2	-	-	-	src-dst-mac	-
T3	-	-	-	src-dst-mac	-
T4	-	-	-	src-dst-mac	-
T5	-	-	-	src-dst-mac	-
T6	-	-	-	src-dst-mac	-
T7	-	-	-	src-dst-mac	-
T8	-	-	-	src-dst-mac	-
T9	-	-	-	src-dst-mac	-
T10	-	-	-	src-dst-mac	-
T11	-	-	-	src-dst-mac	-
T12	-	-	-	src-dst-mac	-

1. Port Priority and Port Number are 0 as it is the aggregator ID for the trunk group, not the individual port.

The following table describes the labels in this screen.

Table 41 Advanced Application > Link Aggregation

LABEL	DESCRIPTION
Group ID	This field displays the group ID to identify a trunk group, that is, one logical link containing multiple ports.
Enabled Ports	These are the ports you have configured in the Link Aggregation screen to be in the trunk group. The port number(s) displays only when this trunk group is activated and there is a port belonging to this group.
Synchronized Ports	These are the ports that are currently transmitting data as one logical link in this trunk group.
Aggregator ID	Link Aggregator ID consists of the following: system priority, MAC address, key, port priority and port number. Refer to Link Aggregation ID on page 139 for more information on this field. The ID displays only when there is a port belonging to this trunk group and LACP is also enabled for this group.
Criteria	This shows the outgoing traffic distribution algorithm used in this trunk group. Packets from the same source and/or to the same destination are sent over the same link within the trunk. src-mac means the OLT distributes traffic based on the packet's source MAC address. dst-mac means the OLT distributes traffic based on the packet's destination MAC address. src-dst-mac means the OLT distributes traffic based on a combination of the packet's source and destination MAC addresses. src-ip means the OLT distributes traffic based on the packet's source IP address. dst-ip means the OLT distributes traffic based on the packet's destination IP address. src-dst-ip means the OLT distributes traffic based on a combination of the packet's source and destination IP addresses.
Status	This field displays how these ports were added to the trunk group. It displays: <ul style="list-style-type: none"> • Static - if the ports are configured as static members of a trunk group. • LACP - if the ports are configured to join a trunk group via LACP.

17.3 Link Aggregation Setting

Click **Advanced Application > Link Aggregation > Link Aggregation Setting** to display the screen shown next. See [Section 17.1 on page 138](#) for more information on link aggregation.

Figure 89 Advanced Application > Link Aggregation > Link Aggregation Setting

Link Aggregation Setting		Status	LACP
Group ID	Active	Criteria	
T1	<input type="checkbox"/>	src-dst-mac ▼	
T2	<input type="checkbox"/>	src-dst-mac ▼	
T3	<input type="checkbox"/>	src-dst-mac ▼	
T4	<input type="checkbox"/>	src-dst-mac ▼	
T5	<input type="checkbox"/>	src-dst-mac ▼	
T6	<input type="checkbox"/>	src-dst-mac ▼	
T7	<input type="checkbox"/>	src-dst-mac ▼	
T8	<input type="checkbox"/>	src-dst-mac ▼	
T9	<input type="checkbox"/>	src-dst-mac ▼	
T10	<input type="checkbox"/>	src-dst-mac ▼	
T11	<input type="checkbox"/>	src-dst-mac ▼	
T12	<input type="checkbox"/>	src-dst-mac ▼	

Port	Group
eth-1	None ▼
eth-2	None ▼
eth-3	None ▼
eth-4	None ▼
eth-5	None ▼
eth-6	None ▼
eth-7	None ▼
eth-8	None ▼
eth-9	None ▼
eth-10	None ▼
eth-11	None ▼
eth-12	None ▼
eth-13	None ▼
eth-14	None ▼
eth-15	None ▼
eth-16	None ▼
eth-17	None ▼
eth-18	None ▼
eth-19	None ▼
eth-20	None ▼

The following table describes the labels in this screen.

Table 42 Advanced Application > Link Aggregation > Link Aggregation Setting

LABEL	DESCRIPTION
Link Aggregation Setting	This is the only screen you need to configure to enable static link aggregation.
Group ID	The field identifies the link aggregation group, that is, one logical link containing multiple ports.
Active	Select this option to activate a trunk group.

Table 42 Advanced Application > Link Aggregation > Link Aggregation Setting (continued)

LABEL	DESCRIPTION
Criteria	Select the outgoing traffic distribution type. Packets from the same source and/or to the same destination are sent over the same link within the trunk. By default, the OLT uses the src-dst-mac distribution type. If the OLT is behind a router, the packet's destination or source MAC address will be changed. In this case, set the OLT to distribute traffic based on its IP address to make sure port trunking can work properly. Select src-mac to distribute traffic based on the packet's source MAC address. Select dst-mac to distribute traffic based on the packet's destination MAC address. Select src-dst-mac to distribute traffic based on a combination of the packet's source and destination MAC addresses. Select src-ip to distribute traffic based on the packet's source IP address. Select dst-ip to distribute traffic based on the packet's destination IP address. Select src-dst-ip to distribute traffic based on a combination of the packet's source and destination IP addresses.
Port	This field displays the port number.
Group	Select the trunk group to which a port belongs. Note: When you enable the port security feature on the OLT and configure port security settings for a port, you cannot include the port in an active trunk group.
Apply	Click Apply to save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

17.3.1 Link Aggregation Control Protocol

Click **Advanced Application > Link Aggregation > Link Aggregation Setting > LACP** to display the screen shown next. See [Dynamic Link Aggregation on page 138](#) for more information on dynamic link aggregation.

Figure 90 Advanced Application > Link Aggregation > Link Aggregation Setting > LACP

Link Aggregation Control Protocol [Link Aggregation Setting](#)

Active	<input type="checkbox"/>
System Priority	65535

Group ID	LACP Active
T1	<input type="checkbox"/>
T2	<input type="checkbox"/>
T3	<input type="checkbox"/>
T4	<input type="checkbox"/>
T5	<input type="checkbox"/>
T6	<input type="checkbox"/>
T7	<input type="checkbox"/>
T8	<input type="checkbox"/>
T9	<input type="checkbox"/>
T10	<input type="checkbox"/>
T11	<input type="checkbox"/>
T12	<input type="checkbox"/>

Port	LACP Timeout
*	30 ▼ seconds
eth-1	30 ▼ seconds
eth-2	30 ▼ seconds
eth-3	30 ▼ seconds
eth-4	30 ▼ seconds
eth-5	30 ▼ seconds
eth-6	30 ▼ seconds
eth-7	30 ▼ seconds
eth-8	30 ▼ seconds
eth-9	30 ▼ seconds
eth-10	30 ▼ seconds
eth-11	30 ▼ seconds
eth-12	30 ▼ seconds
eth-13	30 ▼ seconds
eth-14	30 ▼ seconds
eth-15	30 ▼ seconds
eth-16	30 ▼ seconds
eth-17	30 ▼ seconds
eth-18	30 ▼ seconds
eth-19	30 ▼ seconds
eth-20	30 ▼ seconds

The following table describes the labels in this screen.

Table 43 Advanced Application > Link Aggregation > Link Aggregation Setting > LACP

LABEL	DESCRIPTION
Link Aggregation Control Protocol	Note: Do not configure this screen unless you want to enable dynamic link aggregation.
Active	Select this checkbox to enable Link Aggregation Control Protocol (LACP).
System Priority	LACP system priority is a number between 1 and 65,535. 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 Aggregation Control Protocol (LACP). The smaller the number, the higher the priority level.
Group ID	The field identifies the link aggregation group, that is, one logical link containing multiple ports.
LACP Active	Select this option to enable LACP for a trunk.
Port	This field displays the port number. * means all ports.
*	<p>Settings in this row apply to all ports.</p> <p>Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis.</p> <p>Note: Changes in this row are copied to all the ports as soon as you make them.</p>
LACP Timeout	<p>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.</p> <p>Select either 1 second or 30 seconds.</p>
Apply	Click Apply to save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

17.4 Technical Reference

This section provides technical background information on the topics discussed in this chapter.

17.4.1 Static Trunking Example

This example shows you how to create a static port trunk group for ports 2-5.

- 1 **Configure static trunking** - Click **Advanced Application > Link Aggregation > Link Aggregation Setting**. In this screen activate trunk group **T1**, select the traffic distribution algorithm used by this group and select the ports that should belong to this group as shown in the figure below. Click **Apply** when you are done.

Figure 91 Trunking Example - Configuration Screen

The screenshot shows two tables in a network configuration interface:

Group ID	Active	Criteria
T1	<input checked="" type="checkbox"/>	src-dst-mac ▾
T2	<input type="checkbox"/>	src-dst-mac ▾
T3	<input type="checkbox"/>	src-dst-mac ▾
T4	<input type="checkbox"/>	src-dst-mac ▾
T5	<input type="checkbox"/>	src-dst-mac ▾
T6	<input type="checkbox"/>	src-dst-mac ▾
T7	<input type="checkbox"/>	src-dst-mac ▾
T8	<input type="checkbox"/>	src-dst-mac ▾
T9	<input type="checkbox"/>	src-dst-mac ▾
T10	<input type="checkbox"/>	src-dst-mac ▾
T11	<input type="checkbox"/>	src-dst-mac ▾
T12	<input type="checkbox"/>	src-dst-mac ▾

Port	Group
eth-1	None ▾
eth-2	T1 ▾
eth-3	T1 ▾
eth-4	T1 ▾
eth-5	T1 ▾
eth-6	None ▾
eth-7	None ▾
eth-8	None ▾
eth-9	None ▾
eth-10	None ▾
eth-11	None ▾
eth-12	None ▾
eth-13	None ▾
eth-14	None ▾
eth-15	None ▾
eth-16	None ▾
eth-17	None ▾
eth-18	None ▾
eth-19	None ▾
eth-20	None ▾

Apply **Cancel**

- 2 Make your physical connections** - make sure that the ports that you want to belong to the trunk group are connected to the same destination. The following figure shows ports 2-5 on switch A connected to switch B.

Figure 92 Trunking Example - Physical Connections

Your trunk group 1 (T1) configuration is now complete.

Port Security

17.5 Port Security Overview

This chapter shows you how to set up port security.

Port security allows only packets with dynamically learned MAC addresses and/or configured static MAC addresses to pass through a port on the OLT. The OLT can learn up to 16K MAC addresses in total with no limit on individual ports other than the sum cannot exceed 16K.

For maximum port security, enable this feature, disable MAC address learning and configure static MAC address(es) for a port. It is not recommended you disable port security together with MAC address learning as this will result in many broadcasts. By default, MAC address learning is still enabled even though the port security is not activated.

17.5.1 What You Can Do

Use the **Port Security** screen ([Section 17.6 on page 146](#)) to enable port security and disable MAC address learning. You can also enable the port security feature on a port.

17.6 Port Security Setup

Click **Advanced Application > Port Security** in the navigation panel to display the screen as shown.

Figure 93 Advanced Application > Port Security

MAC Freeze :

Port List	<input type="text"/>	<input type="button" value="MAC freeze"/>
-----------	----------------------	---

Port Security :

Active	<input type="checkbox"/>
--------	--------------------------

Anti-Mac-Spoof :

Active	<input type="checkbox"/>
--------	--------------------------

Port	Active	Anti-Mac-Spoof	Address Learning	Limited Number of Learned MAC Address
*	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
1	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0
2	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0
3	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0
4	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0
5	<input type="checkbox"/>		<input checked="" type="checkbox"/>	0
6	<input type="checkbox"/>		<input checked="" type="checkbox"/>	0
7	<input type="checkbox"/>		<input checked="" type="checkbox"/>	0
17	<input type="checkbox"/>		<input checked="" type="checkbox"/>	0
18	<input type="checkbox"/>		<input checked="" type="checkbox"/>	0
19	<input type="checkbox"/>		<input checked="" type="checkbox"/>	0
20	<input type="checkbox"/>		<input checked="" type="checkbox"/>	0
21	<input type="checkbox"/>		<input checked="" type="checkbox"/>	0
22	<input type="checkbox"/>		<input checked="" type="checkbox"/>	0
23	<input type="checkbox"/>		<input checked="" type="checkbox"/>	0
24	<input type="checkbox"/>		<input checked="" type="checkbox"/>	0

The following table describes the labels in this screen.

Table 44 Advanced Application > Port Security

LABEL	DESCRIPTION
MAC Freeze	
Port List	Enter the number of the port(s) (separated by a comma) on which you want to enable port security and disable MAC address learning. After you click MAC freeze , all previously learned MAC addresses on the specified port(s) will become static MAC addresses and display in the Static MAC Forwarding screen.
MAC freeze	Click MAC freeze to have the OLT automatically select the Active check boxes and clear the Address Learning check boxes only for the ports specified in the Port list .
Port Security	
Active	Select this option to enable port security on the OLT.
Anti-Mac-Spoof	
Active	Select this check box to enable MAC spoofing protection on the OLT.
Port	This field displays the port number. * means all ports.

Table 44 Advanced Application > Port Security (continued)

LABEL	DESCRIPTION
*	<p>Settings in this row apply to all ports.</p> <p>Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis.</p> <p>Note: Changes in this row are copied to all the ports as soon as you make them.</p>
Active	<p>Select this check box to enable the port security feature on this port. The OLT forwards packets whose MAC address(es) is in the MAC address table on this port. Packets with no matching MAC address(es) are dropped.</p> <p>Clear this check box to disable the port security feature. The OLT forwards all packets on this port.</p>
Anti-Mac-Spoof	Turn on MAC spoofing protection to have the system check for hosts with fake or duplicated MAC addresses which attempt to access the system.
Address Learning	MAC address learning reduces outgoing broadcast traffic. For MAC address learning to occur on a port, the port itself must be active with address learning enabled.
Limited Number of Learned MAC Address	Use this field to limit the number of (dynamic) MAC addresses that may be learned on a port. For example, if you set this field to "5" on port 2, then only the devices with these five learned MAC addresses may access port 2 at any one time. A sixth device would have to wait until one of the five learned MAC addresses aged out. MAC address aging out time can be set in the Switch Setup screen. The valid range is from "0" to "16K". "0" means this feature is disabled.
Apply	Click Apply to save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

Classifier

17.7 Classifier Overview

This chapter introduces and shows you how to configure the packet classifier on the OLT. It also discusses Quality of Service (QoS) and classifier concepts as employed by the OLT.

17.7.1 What You Can Do

- Use the **Classifier** screen ([Section 17.8 on page 149](#)) to define the classifiers and view a summary of the classifier configuration. After you define the classifier, you can specify actions (or policy) to act upon the traffic that matches the rules.

17.7.2 What You Need to Know

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 time-critical application such as video-on-demand.

A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming port number. For example, you can configure a classifier to select traffic from the same protocol port (such as Telnet) to form a flow.

Configure QoS on the OLT to group and prioritize application traffic and fine-tune network performance. Setting up QoS involves two separate steps:

- 1 Configure classifiers to sort traffic into different flows.
- 2 Configure policy rules to define actions to be performed on a classified traffic flow (refer to [Chapter 18 on page 155](#) to configure policy rules).

17.8 Classifier

Use the **Classifier** screen to define the classifiers. After you define the classifier, you can specify actions (or policy) to act upon the traffic that matches the rules. To configure policy rules, refer to [Chapter 18 on page 155](#).

Click **Advanced Application > Classifier** in the navigation panel to display the configuration screen as shown.

Figure 94 Advanced Application > Classifier

The screenshot displays the 'Classifier' configuration interface. At the top, there are fields for 'Active' (unchecked), 'Name' (empty), and 'Packet Format' (set to 'All'). Below these are sections for 'VLAN' (radio button 'Any' selected), 'Priority' (radio button 'Any' selected, dropdown '0'), 'Ethernet Type' (radio button 'All' selected, dropdown 'All'), and 'Layer 2' classification for 'Source' and 'Destination' (both MAC Address and Port fields). The 'DSCP' and 'IP Protocol' sections follow, with 'IP Protocol' showing 'All' selected and 'Establish Only' checked. Below this are 'Layer 3' classification sections for 'Source' and 'Destination' (IP Address / Address Prefix and Socket Number fields). At the bottom, there are 'Add', 'Cancel', and 'Clear' buttons, followed by a table for managing classifier rules.

Index	Active	Name	Rule	Delete
				<input type="button" value="Delete"/> <input type="button" value="Cancel"/>

The following table describes the labels in this screen.

Table 45 Advanced Application > Classifier

LABEL	DESCRIPTION
Active	Select this option to enable this rule.
Name	Enter a descriptive name for this rule for identifying purposes.
Packet Format	Specify the format of the packet. Choices are All , Ethernet II tagged and Ethernet II untagged . A value of Ethernet II indicates that the packets are formatted according to RFC 894, Ethernet II encapsulation.
Layer 2	Specify the fields below to configure a layer 2 classifier.

Table 45 Advanced Application > Classifier (continued)

LABEL	DESCRIPTION
VLAN	Select Any to classify traffic from any VLAN or select the second option and specify the source VLAN ID in the field provided.
Priority	Select Any to classify traffic from any priority level or select the second option and specify a priority level in the field provided.
Ethernet Type	Select an Ethernet type or select Others and enter the Ethernet type number in hexadecimal value. Refer to Table 47 on page 152 for information.
Source	
MAC Address	Select Any to apply the rule to all MAC addresses. To specify a source, select MAC to enter the source MAC address of the packet in valid MAC address format (six hexadecimal character pairs).
Port	Type the port number to which the rule should be applied. You may choose one port only or all ports (Any).
Destination	
MAC Address	Select Any to apply the rule to all MAC addresses. To specify a destination, select MAC to enter the destination MAC address of the packet in valid MAC address format (six hexadecimal character pairs).
Port	Type the port number to which the rule should be applied. You may choose one port only or all ports (Any).
Layer 3	
Specify the fields below to configure a layer 3 classifier.	
DSCP	Select Any to classify traffic from any DSCP or select the second option and specify a DSCP (DiffServ Code Point) number between 0 and 63 in the field provided.
IP Protocol	Select an IPv4 protocol type or select Others and enter the protocol number in decimal value. Refer to Table 48 on page 153 for more information. You may select Establish Only for TCP protocol type. This means that the OLT will pick out the packets that are sent to establish TCP connections.
Source	
IP Address/Address Prefix	Enter a source IP address in dotted decimal notation. Specify the address prefix by entering the number of ones in the subnet mask. A subnet mask can be represented in a 32-bit notation. For example, the subnet mask "255.255.255.0" can be represented as "11111111.11111111.11111111.00000000", and counting up the number of ones in this case results in 24.
Socket Number	Note: You must select either UDP or TCP in the IP Protocol field before you configure the socket numbers. Select Any to apply the rule to all TCP/UDP protocol port numbers or select the second option and enter a TCP/UDP protocol port number. Refer to Table 49 on page 153 for more information.
Destination	
IP Address/Address Prefix	Enter a destination IP address in dotted decimal notation. Specify the address prefix by entering the number of ones in the subnet mask.

Table 45 Advanced Application > Classifier (continued)

LABEL	DESCRIPTION
Socket Number	Note: You must select either UDP or TCP in the IP Protocol field before you configure the socket numbers. Select Any to apply the rule to all TCP/UDP protocol port numbers or select the second option and enter a TCP/UDP protocol port number. Refer to Table 49 on page 153 for more information.
Add	Click Add to insert the entry in the summary table below and save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields back to your previous configuration.
Clear	Click Clear to set the above fields back to the factory defaults.

17.8.1 Viewing and Editing Classifier Configuration Summary

To view a summary of the classifier configuration, scroll down to the summary table at the bottom of the **Classifier** screen. To change the settings of a rule, click a number in the **Index** field.

Note: When two rules conflict with each other, a higher layer rule has priority over lower layer rule.

Figure 95 Advanced Application > Classifier > Classifier Configuration: Summary Table

The screenshot shows a summary table with the following data:

Index	Active	Name	Rule	Delete
1	No	Class1	PktFormat = Ethernet II untagged;	<input checked="" type="checkbox"/>

At the bottom of the table are two buttons: **Delete** and **Cancel**.

The following table describes the labels in this screen.

Table 46 Advanced Application > Classifier > Classifier Configuration: Summary Table

LABEL	DESCRIPTION
Index	This field displays the index number of the rule. Click an index number to edit the rule.
Active	This field displays Yes when the rule is activated and No when it is deactivated.
Name	This field displays the descriptive name for this rule. This is for identification purpose only.
Rule	This field displays a summary of the classifier rule's settings.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the check boxes.

The following table shows some other common Ethernet types and the corresponding protocol number.

Table 47 Common Ethernet Types and Protocol Numbers

ETHERNET TYPE	PROTOCOL NUMBER
IP ETHII	0800
X.75 Internet	0801
NBS Internet	0802
ECMA Internet	0803
Chaosnet	0804

Table 47 Common Ethernet Types and Protocol Numbers

ETHERNET TYPE	PROTOCOL NUMBER
X.25 Level 3	0805
XNS Compat	0807
Banyan Systems	0BAD
BBN Simnet	5208
IBM SNA	80D5
AppleTalk AARP	80F3

In the Internet Protocol there is a field, called “Protocol”, to identify the next level protocol. The following table shows some common protocol types and the corresponding protocol number. Refer to <http://www.iana.org/assignments/protocol-numbers> for a complete list.

Table 48 Common IP Protocol Types and Protocol Numbers

PROTOCOL TYPE	PROTOCOL NUMBER
ICMP	1
TCP	6
UDP	17
EGP	8
L2TP	115

Some of the most common TCP and UDP port numbers are:

Table 49 Common TCP and UDP Port Numbers

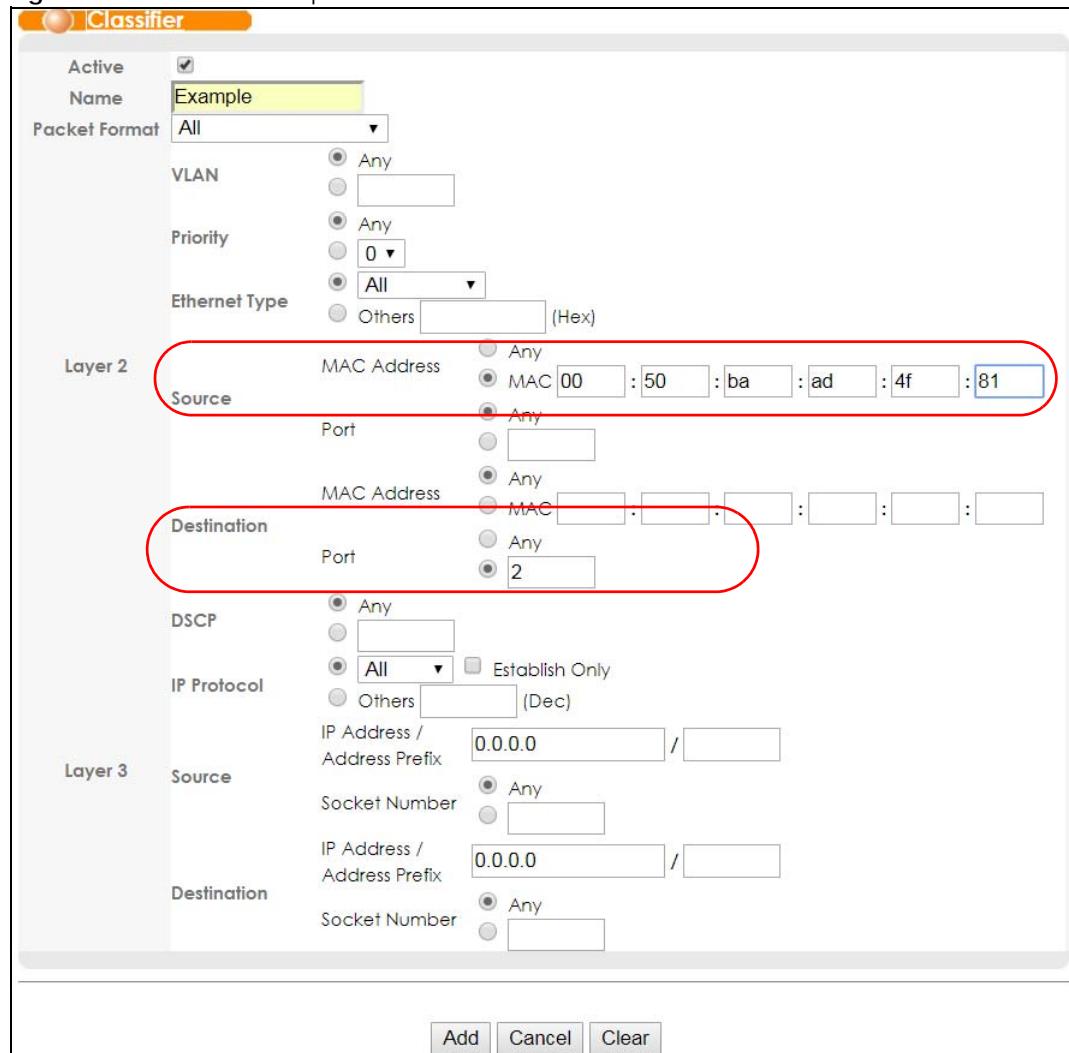
PROTOCOL NAME	TCP/UDP PORT NUMBER
FTP	21
Telnet	23
SMTP	25
DNS	53
HTTP	80
POP3	110

See [Appendix B on page 636](#) for information on commonly used port numbers.

17.9 Classifier Example

The following screen shows an example where you configure a classifier that identifies all traffic from MAC address 00:50:ba:ad:4f:81 on port 2.

After you have configured a classifier, you can configure a policy (in the **Policy** screen) to define action(s) on the classified traffic flow.

Figure 96 Classifier: Example

CHAPTER 18

Policy Rule

18.1 Policy Rules Overview

This chapter shows you how to configure policy rules.

A classifier distinguishes traffic into flows based on the configured criteria (refer to [Chapter 17 on page 148](#) for more information). A policy rule ensures that a traffic flow gets the requested treatment in the network.

18.1.1 What You Need to Know

Read on for concepts that can help you configure the screens in this chapter.

DiffServ

DiffServ (Differentiated Services) 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 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

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.

DSCP (6 bits)	Unused (2 bits)
---------------	-----------------

The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different kinds of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

Two Rate Three Color Marker Traffic Policing

Traffic policing is the limiting of the input or output transmission rate of a class of traffic on the basis of user-defined criteria. Traffic policing methods measure traffic flows against user-defined criteria and identify it as either conforming, exceeding or violating the criteria.

Two Rate Three Color Marker (TRTCM, defined in RFC 2698) is a type of traffic policing that identifies packets by comparing them to two user-defined rates: the Committed Information Rate (CIR) and the Peak Information Rate (PIR). The CIR specifies the average rate at which packets are admitted to the network. The PIR is greater than or equal to the CIR. CIR and PIR values are based on the guaranteed and maximum bandwidth respectively as negotiated between a service provider and client.

Two Rate Three Color Marker evaluates incoming packets and marks them with one of three colors which refer to packet loss priority levels. High packet loss priority level is referred to as red, medium is referred to as yellow and low is referred to as green. After TRTCM is configured and DiffServ is enabled the following actions are performed on the colored packets:

- Red (high loss priority level) packets are dropped.
- Yellow (medium loss priority level) packets are dropped if there is congestion on the network.
- Green (low loss priority level) packets are forwarded.

TRTCM operates in one of two modes: color-blind or color-aware. In color-blind mode, packets are marked based on evaluating against the PIR and CIR regardless of if they have previously been marked or not. In the color-aware mode, packets are marked based on both existing color and evaluation against the PIR and CIR. If the packets do not match any of colors, then the packets proceed unchanged.

18.1.2 What You Can Do

Use the **Policy Rule** screen ([Section 18.2 on page 156](#)) to enable the policy and display the active classifier(s) you configure in the **Classifier** screen.

18.2 Configuring Policy Rules

You must first configure a classifier in the **Classifier** screen. Refer to [Section 17.8 on page 149](#) for more information.

Click **Advanced Applications > Policy Rule** in the navigation panel to display the screen as shown.

Figure 97 Advanced Application > Policy Rule

Policy					
Active	<input type="checkbox"/>				
Name					
Classifier(s)					
Parameters	VLAN ID	<input type="text"/>	General	Metering	
	Cir	<input type="text"/> Kbps			
	Pir	<input type="text"/> Kbps			
	Egress Port	<input type="text"/> 1	Out-of-Profile	<input type="text"/>	
	Mirror Port	<input type="text"/> 1	DSCP	<input type="text"/>	
	Outgoing packet format for Egress port	<input checked="" type="radio"/> Tag <input type="radio"/> Untag			
	Priority	<input type="text"/> 0 ▼			
DSCP	<input type="text"/>				
TOS	<input type="text"/> 0 ▼				
Forwarding					
<input checked="" type="radio"/> No change <input type="radio"/> Discard the packet <input type="radio"/> Do not drop the matching frame previously marked for dropping					
Priority <input checked="" type="radio"/> No change <input type="radio"/> Set the packet's 802.1p priority <input type="radio"/> Send the packet to priority queue <input type="radio"/> Replace the 802.1p priority field with the IP TOS value					
Diffserv <input checked="" type="radio"/> No change <input type="radio"/> Set the packet's TOS field <input type="radio"/> Replace the IP TOS field with the 802.1p priority value <input type="radio"/> Set the Diffserv Codepoint field in the frame					
Action	Outgoing				
	<input type="checkbox"/> Send the packet to the mirror port <input type="checkbox"/> Send the packet to the egress port <input type="checkbox"/> Send the matching frames(broadcast or DLF, multicast, marked for dropping or to be sent to the CPU) to the egress port <input type="checkbox"/> Set the packet's VLAN ID				
	Metering				
	<input type="checkbox"/> Enable <div style="border: 1px solid #ccc; padding: 2px;"> <input type="checkbox"/> Drop the packet <input type="checkbox"/> Change the DSCP value <input type="checkbox"/> Set Out-Drop Precedence <input type="checkbox"/> Do not drop the matching frame previously marked for dropping </div>				
	Set-green-to-cosq				
	<input type="checkbox"/> Enable <input type="text"/> 0 ▼				
<input type="button" value="Add"/> <input type="button" value="Cancel"/> <input type="button" value="Clear"/>					
Index	Active	Name	Classifier(s)	Delete	
			<input type="button" value="Delete"/> <input type="button" value="Cancel"/>		

The following table describes the labels in this screen.

Table 50 Advanced Application > Policy Rule

LABEL	DESCRIPTION
Active	Select this option to enable the policy.
Name	Enter a descriptive name for identification purposes.
Classifier(s)	This field displays the active classifier(s) you configure in the Classifier screen. Select the classifier(s) to which this policy rule applies. To select more than one classifier, press [SHIFT] and select the choices at the same time. You can add up to 256 classifiers for a policy rule.
Parameters	Set the fields below for this policy. You only have to set the field(s) that is related to the action(s) you configure in the Action field.
General	
VLAN ID	Specify a VLAN ID.
Egress Port	Type the number of an outgoing port.
Mirror Port	Type the number of a mirror port. The mirror port 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 port(s).
Outgoing packet format for Egress port	At the time of writing, the OLT doesn't support this feature.
Priority	Specify a priority level between 0 and 7.
DSCP	Specify a DSCP (DiffServ Code Point) number between 0 and 63.
TOS	Specify the type of service (TOS) priority level between 0 and 7.
Metering	You can configure the desired bandwidth available to a traffic flow. Traffic that exceeds the maximum bandwidth allocated in the Cir , Pir , and Out-of-Profile DSCP fields (in cases where the network is congested) is called out-of-profile traffic.
Cir	Specify the Commit Information Rate (CIR). See Section on page 156 for more information about TRTCM (Two Rate Three Color Marker) and CIR.
Pir	Specify the Peak Information Rate (PIR). See Section on page 156 for more information about TRTCM (Two Rate Three Color Marker) and PIR.
Out-of-Profile DSCP	Specify a new DSCP number (between 0 and 63) if you want to replace or remark the DSCP number for out-of-profile traffic.

Table 50 Advanced Application > Policy Rule (continued)

LABEL	DESCRIPTION
Action	<p>Specify the action(s) the OLT takes on the associated classified traffic flow.</p> <p>Note: You can specify only one action (pair) in a policy rule. To have the OLT take multiple actions on the same traffic flow, you need to define multiple classifiers with the same criteria and apply different policy rules.</p> <p>Say you have several classifiers that identify the same traffic flow and you specify a different policy rule for each. If their policy actions conflict (Discard the packet, Send the packet to the egress port and Metering), the OLT only applies the policy rules depending on the classifier names. The longer the classifier name, the higher the classifier priority. If two classifier names are the same length, the bigger the character, the higher the classifier priority. The lowercase letters (such as a and b) have higher priority than the capitals (such as A and B) in the classifier name. For example, the classifier with the name of class 2, class a or class B takes priority over the classifier with the name of class 1 or class A.</p> <p>Let's say you set two classifiers (Class 1 and Class 2) and both identify all traffic from MAC address 11:22:33:44:55:66 on port 3.</p> <p>If Policy 1 applies to Class 1 and the action is to drop the packets, Policy 2 applies to Class 2 and the action is to forward the packets to the egress port, the OLT will forward the packets.</p> <p>If Policy 1 applies to Class 1 and the action is to drop the packets, Policy 2 applies to Class 2 and the action is to enable bandwidth limitation, the OLT will follow the bandwidth limitation settings.</p> <p>If Policy 1 applies to Class 1 and the action is to forward the packets to the egress port, Policy 2 applies to Class 2 and the action is to enable bandwidth limitation, the OLT will follow the bandwidth limitation settings.</p>
Forwarding	<p>Select No change to forward the packets.</p> <p>Select Discard the packet to drop the packets.</p> <p>Select Do not drop the matching frame previously marked for dropping to retain the frames that were marked to be dropped before. For example, the traffic that exceeds the maximum bandwidth allocated in the Advanced Application > Bandwidth Control screen won't be dropped if Do not drop the matching frame previously marked for dropping is selected.</p>
Priority	<p>Select No change to keep the priority setting of the frames.</p> <p>Select Set the packet's 802.1p priority to replace the packet's 802.1p priority field with the value you set in the Priority field.</p> <p>Select Send the packet to priority queue to replace the packet's 802.1p priority field with the value you set in the Priority field and put the packets in the designated queue.</p> <p>Select Replace the 802.1p priority field with the IP TOS value to replace the packet's 802.1p priority field with the value you set in the TOS field and put the packets in the designated queue.</p>
Diffserv	<p>Select No change to keep the TOS and/or DSCP fields in the packets.</p> <p>Select Set the Diffserv Codepoint field in the frame to set the DSCP field with the value you configure in the DSCP field.</p> <p>At the time of writing, The OLT doesn't support Set the packet's TOS field and Replace the IP TOS with the 802.1p priority value.</p>
Outgoing	<p>Select Send the packet to the mirror port to send the packet to the mirror port.</p> <p>Select Send the packet to the egress port to send the packet to the egress port.</p> <p>Select Set the packet's VLAN ID to set the packet's VLAN ID.</p> <p>At the time of writing, The OLT doesn't support Send the matching frames(broadcast or DLF, multicast, marked for dropping or to be sent to the CPU) to the egress port.</p>

Table 50 Advanced Application > Policy Rule (continued)

LABEL	DESCRIPTION
Metering	Select Enable to activate bandwidth limitation on the traffic flow(s) then set the actions to be taken on out-of-profile packets. Also, enable Metering to use Two Rate Three Color Marker (TRTCM) to identify packets by comparing them to the Committed Information Rate (CIR) and the Peak Information Rate (PIR). These two rates are defined in the Parameter field.
Out-of-profile action	Select the action(s) to be performed for out-of-profile traffic. See the description of the Metering field for the out-of-profile traffic definition. Select Drop the packet to discard the out-of-profile traffic. Select Change the DSCP value to replace the DSCP field with the value specified in the Out-of-profile-DSCP field. Select Set Out-Drop Precedence to mark out-of-profile traffic and drop it when network is congested. Select Do not drop the matching frame previously marked for dropping to queue the frames that are marked to be dropped.
Set-green-to-cosq	
Enable	Select this to assign the incoming packets marked as green via TRTCM (Two Rate Three Color Marker) to a CoS (Class of Service) queue. See Section on page 156 for more information about how packets are marked as red, yellow, and green via TRTCM. To use TRTCM, enable Metering in the Advanced Application > Policy Rule screen. <ul style="list-style-type: none"> • The incoming packets from 1/10 G ports are marked as yellow by default. • The incoming packets from an ONT are marked as green by default.
Green-to-cosq	Select the CoS queue priority level for the incoming packets marked as green for transmission. 7 has the highest priority and 0 the lowest. It's recommended to assign the incoming packets marked as green via TRTCM to the highest CoS queue priority level.
Add	Click Add to inset the entry to the summary table below and save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields back to your previous configuration.
Clear	Click Clear to set the above fields back to the factory defaults.
Index	This field displays the policy index number. Click an index number to edit the policy.
Active	This field displays Yes when policy is activated and No when it deactivated.
Name	This field displays the name you have assigned to this policy.
Classifier(s)	This field displays the name(s) of the classifier to which this policy applies.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the check boxes.

18.3 Policy Example

The figure below shows an example **Policy** screen where you configure a policy to limit bandwidth on a traffic flow classified using the **Example** classifier (refer to [Section 17.9 on page 153](#)).

Figure 98 Policy Example

The screenshot shows a policy configuration window with the following details:

- General Information:**
 - Name:** Test
 - Classifier(s):** Example
 - Active:** Checked
- Metering:**
 - Cir: 300 Kbps
 - Pir: 500 Kbps
- Parameters:**
 - VLAN ID: [Empty]
 - Egress Port: 1
 - Mirror Port: 1
 - Outgoing packet format for Egress port: Tag (radio button selected)
 - Priority: 0
 - DSCP: [Empty]
 - TOS: 0
- Action Configuration:**
 - Forwarding:**
 - No change (radio button selected)
 - Discard the packet
 - Do not drop the matching frame previously marked for dropping
 - Priority:**
 - No change (radio button selected)
 - Set the packet's 802.1p priority
 - Send the packet to priority queue
 - Replace the 802.1p priority field with the IP TOS value
 - Diffserv:**
 - No change (radio button selected)
 - Set the packet's TOS field
 - Replace the IP TOS field with the 802.1p priority value
 - Set the Diffserv Codepoint field in the frame
 - Outgoing:**
 - Send the packet to the mirror port
 - Send the packet to the egress port
 - Send the matching frames(broadcast or DLF, multicast, marked for dropping or to be sent to the CPU) to the egress port
 - Set the packet's VLAN ID
 - Metering:**
 - Enable
 - Drop the packet
 - Change the DSCP value
 - Set Out-Drop Precedence
 - Do not drop the matching frame previously marked for dropping
 - Set-green-to-cosq:**
 - Enable
 - Green-to-cosq: 0
- Buttons at the bottom:**
 - Add (highlighted with a red circle)
 - Cancel
 - Clear

CHAPTER 19

Queuing Method

19.1 Queuing Method Overview

This chapter introduces the queuing methods supported.

Queuing is used to help solve performance degradation when there is network congestion. Use the **Queuing Method** screen to configure queuing algorithms for outgoing traffic. See also **Priority Queue Assignment in Switch Setup** and **802.1p Priority in Port Setup** for related information.

19.1.1 What You Can Do

Use the **Queuing Method** screen ([Section 19.2 on page 163](#)) set priorities for the queues of the OLT. This distributes bandwidth across the different traffic queues.

19.1.2 What You Need to Know

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

Strictly Priority Queuing (SPQ) services queues based on priority only. As traffic comes into the OLT, 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. SPQ does not automatically adapt to changing network requirements.

Weighted Fair Queuing

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. By default, the weight for Q0 is 1, for Q1 is 2, for Q2 is 3, and so on.

19.2 Configuring Queuing

Use this screen to set priorities for the queues of the OLT. This distributes bandwidth across the different traffic queues.

Click **Advanced Application > Queuing Method** in the navigation panel.

Figure 99 Advanced Application > Queuing Method

Port	Method	Weight								Hybrid-SPQ Lowest-Queue
		Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	
*	SPQ								None	
1	SPQ	1	2	3	4	5	6	7	8	None
2	WFQ	1	2	3	4	5	6	7	8	None
3	SPQ	1	2	3	4	5	6	7	8	None
4	WFQ	1	2	3	4	5	6	7	8	None
5	SPQ	1	2	3	4	5	6	7	8	None
16	WFQ	1	2	3	4	5	6	7	8	None
17	SPQ	1	2	3	4	5	6	7	8	None
18	WFQ	1	2	3	4	5	6	7	8	None
19	SPQ	1	2	3	4	5	6	7	8	None
20	WFQ	1	2	3	4	5	6	7	8	None
21	SPQ	1	2	3	4	5	6	7	8	None
22	WFQ	1	2	3	4	5	6	7	8	None
23	SPQ	1	2	3	4	5	6	7	8	None
24	WFQ	1	2	3	4	5	6	7	8	None
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>										

The following table describes the labels in this screen.

Advanced Application > Queuing Method

LABEL	DESCRIPTION
Port	This label shows the port you are configuring. * means all ports.
*	<p>Settings in this row apply to all ports.</p> <p>Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis.</p> <p>Note: Changes in this row are copied to all the ports as soon as you make them.</p>

Advanced Application > Queuing Method (continued)

LABEL	DESCRIPTION
Method	Select SPQ (Strictly Priority Queuing) or WFQ (Weighted Fair Queuing). Strictly Priority Queuing services queues based on priority only. When the highest priority queue empties, traffic on the next highest-priority queue begins. Q7 has the highest priority and Q0 the lowest. Weighted Fair Queuing is used to guarantee each queue's minimum bandwidth based on their bandwidth portion (weight) (the number you configure in the Weight field). Queues with larger weights get more guaranteed bandwidth than queues with smaller weights.
Weight	When you select WFQ enter the queue weight here. Bandwidth is divided across the different traffic queues according to their weights.
Hybrid-SPQ Lowest-Queue	This field is applicable only when you select WFQ . Select a queue (Q0 to Q7) to have the OLT use SPQ to service the subsequent queue(s) after and including the specified queue for the port. For example, if you select Q5 , the OLT services traffic on Q5 , Q6 and Q7 using SPQ . Select None to always use WFQ for the port.
Apply	Click Apply to save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

CHAPTER 20

VLAN Stacking

This chapter shows you how to configure VLAN stacking on your OLT. See the chapter on VLANs for more background information on Virtual LAN.

See [Section 6.4 on page 71](#) for tutorials on how to use VLAN stacking on PON ports.

20.1 VLAN Stacking Overview

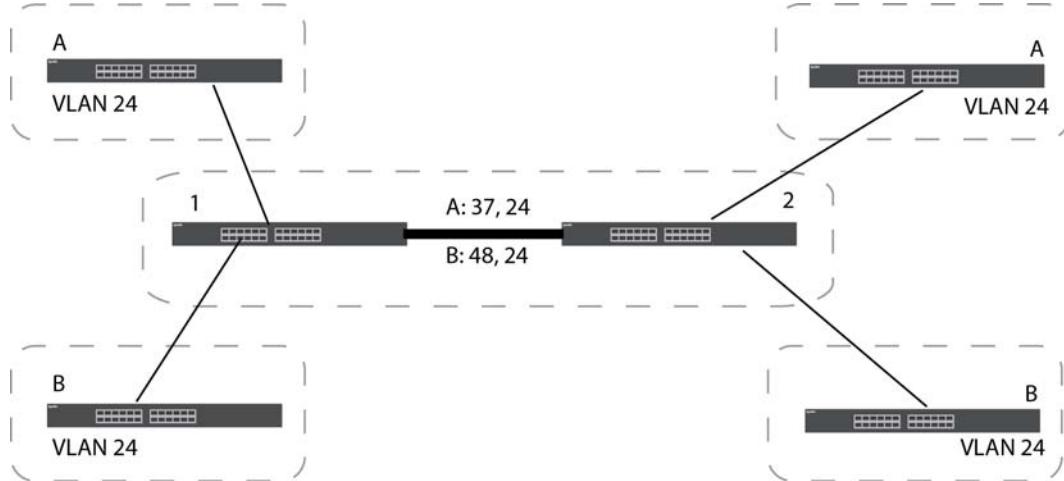
A service provider can use VLAN stacking to allow it to distinguish multiple customers VLANs, even those with the same (customer-assigned) VLAN ID, within its network.

Use VLAN stacking 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 4,094 VLAN groups with each group containing up to 4,094 customer VLANs. This allows a service provider to provide different service, 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 on ports for these applications. 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.

20.1.1 VLAN Stacking Example

In the following example figure, both **A** and **B** are Service Provider's Network (SPN) customers with VPN tunnels between their head offices and branch offices respectively. Both have an identical VLAN tag for their VLAN group. The service provider can separate these two VLANs within its network by adding tag 37 to distinguish customer **A** and tag 48 to distinguish customer **B** at edge device **1** and then stripping those tags at edge device **2** as the data frames leave the network.

Figure 100 VLAN Stacking Example

20.2 VLAN Stacking Port Roles

Each port can have three VLAN stacking “roles”, **Normal**, **Access Port** and **Tunnel Port** (the latter is for Gigabit ports only).

- Select **Normal** for “regular” (non-VLAN stacking) IEEE 802.1Q frame switching.
- Select **Access Port** for ingress ports on the service provider’s edge devices (**1** and **2** in the VLAN stacking example figure). The incoming frame is treated as “untagged”, so a second VLAN tag (outer VLAN tag) can be added.

Note: Static VLAN Tx Tagging MUST be disabled on a port where you choose **Normal** or **Access Port**.

- Select **Tunnel Port** (available for Gigabit ports only) for egress ports at the edge of the service provider’s network. All VLANs belonging to a customer can be aggregated into a single service provider’s VLAN (using the outer VLAN tag defined by the Service Provider’s (SP) VLAN ID (VID)).

Note: Static VLAN Tx Tagging MUST be enabled on a port where you choose **Tunnel Port**.

20.3 VLAN Tag Format

A VLAN tag (service provider VLAN stacking or customer IEEE 802.1Q) consists of the following three fields.

Table 51 VLAN Tag Format

Type	Priority	VID

Type is a standard Ethernet type code identifying the frame and indicates that whether the frame carries IEEE 802.1Q tag information. **SP TPID** (Service Provider Tag Protocol Identifier) is the service provider VLAN stacking tag type. Many vendors use 0x8100 or 0x9100.

TPID (Tag Protocol Identifier) is the customer IEEE 802.1Q tag.

- If the VLAN stacking port role is **Access Port**, then the OLT adds the **SP TPID** tag to all incoming frames on the service provider's edge devices (1 and 2 in the VLAN stacking example figure).
- If the VLAN stacking port role is **Tunnel Port**, then the OLT only adds the **SP TPID** tag to all incoming frames on the service provider's edge devices (1 and 2 in the VLAN stacking example figure) that have an **SP TPID** different to the one configured on the OLT. (If an incoming frame's **SP TPID** is the same as the one configured on the OLT, then the OLT will not add the tag.)

Priority refers to the IEEE 802.1p standard that allows the service provider to prioritize traffic based on the class of service (CoS) the customer has paid for.

- On the OLT, configure priority level of the inner IEEE 802.1Q tag in the **Port Setup** screen.
- "0" is the lowest priority level and "7" is the highest.

VID is the VLAN ID. **SP VID** is the VID for the second (service provider's) VLAN tag.

20.3.1 Frame Format

The frame format for an untagged Ethernet frame, a single-tagged 802.1Q frame (customer) and a "double-tagged" 802.1Q frame (service provider) is shown next.

Configure the fields as highlighted in the OLT **VLAN Stacking** screen.

Table 52 Single and Double Tagged 802.1Q Frame Format

						DA	SA	Len/Etype	Data	FCS	Untagged Ethernet frame
			DA	SA	TPID	Priority	VID	Len/Etype	Data	FCS	IEEE 802.1Q customer tagged frame
DA	SA	SPTPID	Priority	VID	TPID	Priority	VID	Len/Etype	Data	FCS	Double-tagged frame

Table 53 802.1Q Frame

DA	Destination Address	Priority	802.1p Priority
SA	Source Address	Len/Etype	Length and type of Ethernet frame
(SP)TPID	(Service Provider) Tag Protocol IDentifier	Data	Frame data
VID	VLAN ID	FCS	Frame Check Sequence

20.4 Configuring VLAN Stacking

Click **Advanced Application > VLAN Stacking** to display the screen as shown.

You can also use VLAN stacking on UNI ports. See [Section 33.2.3 on page 271](#) for more information.

Figure 101 Advanced Application > VLAN Stacking

Port	Role	Tunnel TPID
*	Normal	
pon-1	Normal	88a8
pon-2	Normal	88a8
pon-3	Normal	88a8
pon-4	Normal	88a8
eth-1	Normal	88a8
eth-2	Normal	88a8
eth-3	Normal	88a8
eth-4	Normal	88a8
eth-5	Normal	88a8
eth-6	Normal	88a8
eth-7	Normal	88a8
eth-8	Normal	88a8
eth-9	Normal	88a8
eth-10	Normal	88a8
eth-11	Normal	88a8
eth-12	Normal	88a8
eth-13	Normal	88a8
eth-14	Normal	88a8
eth-15	Normal	88a8
eth-16	Normal	88a8
eth-17	Normal	88a8
eth-18	Normal	88a8
eth-19	Normal	88a8
eth-20	Normal	88a8

Apply **Cancel**

The following table describes the labels in this screen.

Table 54 Advanced Application > VLAN Stacking

LABEL	DESCRIPTION
Port	This field displays the port number.
*	<p>Settings in this row apply to all ports.</p> <p>Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis.</p> <p>Note: Changes in this row are copied to all the ports as soon as you make them.</p>
Role	<p>Select Normal to have the OLT ignore frames received (or transmitted) on this port with VLAN stacking tags. Anything you configure in SPVID of the Port-based QinQ is ignored.</p> <p>Select Access Port to have the OLT add the SP TPID tag to all incoming frames received on this port. Select Access Port for ingress ports at the edge of the service provider's network.</p> <p>Select Tunnel Port (available for Gigabit ports only) for egress ports at the edge of the service provider's network. Select Tunnel Port to have the OLT add the Tunnel TPID tag to all outgoing frames sent on this port.</p> <p>In order to support VLAN stacking on a port, the port must be able to allow frames of 1526 Bytes (1522 Bytes + 4 Bytes for the second tag) to pass through it.</p>

Table 54 Advanced Application > VLAN Stacking (continued)

LABEL	DESCRIPTION
Tunnel TPID	TPID is a standard Ethernet type code identifying the frame and indicates whether the frame carries IEEE 802.1Q tag information. Enter a four-digit hexadecimal number from 0000 to FFFF that the OLT adds in the outer VLAN tag of the frames sent on the tunnel port(s). The OLT also uses this to check if the received frames are double-tagged. The default value of this field is 0x88a8 defined in IEEE 802.1ad. It's used to identify the service tag of an incoming frame. The value of this field is 0x8100 as defined in IEEE 802.1Q. It's used to identify the customer tag of an incoming frame. If the OLT needs to communicate with other vendors' devices, they should use the same TPID. Note: You can define up to four different tunnel TPIDs (including 8100) in this screen at a time.
Apply	Click Apply to save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

20.4.1 Port-based Q-in-Q

Port-based Q-in-Q lets the OLT treat all frames received on the same port as the same VLAN flows and add the same outer VLAN tag to them, even they have different customer VLAN IDs.

Click **Port-based QinQ** in the **Advanced Application > VLAN Stacking** screen to display the screen as shown.

Figure 102 Advanced Application > VLAN Stacking > Port-based QinQ

Port	SPVID	Priority
*		0 ▼
pon-1	1	0 ▼
pon-2	1	0 ▼
pon-3	1	0 ▼
pon-4	1	0 ▼
eth-1	1	0 ▼
eth-2	1	0 ▼
eth-3	1	0 ▼
eth-4	1	0 ▼
eth-5	1	0 ▼
eth-6	1	0 ▼
eth-7	1	0 ▼
eth-8	1	0 ▼
eth-9	1	0 ▼
eth-10	1	0 ▼
eth-11	1	0 ▼
eth-12	1	0 ▼
eth-13	1	0 ▼
eth-14	1	0 ▼
eth-15	1	0 ▼
eth-16	1	0 ▼
eth-17	1	0 ▼
eth-18	1	0 ▼
eth-19	1	0 ▼
eth-20	1	0 ▼

Apply **Cancel**

The following table describes the labels in this screen.

Table 55 Advanced Application > VLAN Stacking > Port-based QinQ

LABEL	DESCRIPTION
Port	This field displays the port number. * means all ports (on the same OLT).
SPVID	SPVID is the service provider's VLAN ID (the outer VLAN tag). Enter the service provider ID (from 1 to 4094) for frames received on this port. See Chapter 9 on page 95 for more background information on VLAN ID.
Priority	Select a priority level (from 0 to 7). This is the service provider's priority level that adds to the frames received on this port. "0" is the lowest priority level and "7" is the highest.
Apply	Click Apply to save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

CHAPTER 21

Multicast

21.1 Multicast Overview

This chapter shows you how to configure various multicast features.

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 RFC 1112, RFC 2236 and RFC 3376 for information on IGMP versions 1, 2 and 3 respectively.

21.1.1 What You Can Do

- Use the **Multicast Status** screen ([Section 21.2 on page 173](#)) to view multicast group information.
- Use the **Multicast Setting** screen ([Section 21.3 on page 176](#)) to configure multicast settings on the OLT.
- Use the **IGMP Snooping VLAN** screen ([Section 21.3.1 on page 178](#)) to perform IGMP snooping on up to 16 VLANs.
- Use the **Mcast Channel** screen ([Section 21.3.2 on page 180](#)) to configures a GPON client multicast channel.

21.1.2 What You Need to Know

Read on for concepts on Multicasting that can help you configure the screens in this chapter.

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 subnetwork. 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 website for more information).

IGMP Snooping

A OLT can passively snoop on IGMP 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 OLT to learn multicast groups without you having to manually configure them.

The OLT 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. IGMP snooping generates no additional network traffic, allowing you to significantly reduce multicast traffic passing through your OLT.

IGMP Snooping and VLANs

The OLT can perform IGMP snooping on up to 16 VLANs. You can configure the OLT to automatically learn multicast group membership of any VLANs. The OLT then performs IGMP snooping on the first 16 VLANs that send IGMP packets. This is referred to as auto mode. Alternatively, you can specify the VLANs that IGMP snooping should be performed on. This is referred to as fixed mode. In fixed mode the OLT does not learn multicast group membership of any VLANs other than those explicitly added as an IGMP snooping VLAN.

IGMP Proxy

IGMP proxy maintains a joined member list for each IGMP group on the OLT. This OLT automatically and periodically sends queries to the subscriber ports to get the subscribing information and response the upper layer router's query for the member list. In addition, it enables the OLT not to report the leave request sent from one subscriber to upper layer router if there are still other subscriber(s) in the same IGMP group. It also allows the OLT not to report the join request sent from one subscriber to upper layer router if any subscriber is still in the same IGMP group. In other words, an IGMP proxy OLT only forward the first join request and the last leave request in an IGMP network to its upper layer router. It can reduce multicast traffic significantly.

Note: You must set one of Gigabit Ethernet ports to "Fixed mode" before enabling IGMP proxy.

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.

MLD Messages

A multicast router or switch periodically sends general queries to MLD hosts to update the multicast forwarding table. When an MLD host wants to join a multicast group, it sends an MLD Report message for that address.

An MLD Done message is equivalent to an IGMP Leave message. When an MLD host wants to leave a multicast group, it can send a Done message to the router or switch. If the leave mode is not set to immediate, the router or switch sends a group-specific query to the port on which the Done message is received to determine if other devices connected to this port should remain in the group.

21.2 Multicast Status

Click **Advanced Application > Multicast** to display the screen as shown. This screen shows the multicast group information. See [Section 21.1.2 on page 171](#) for more information on multicasting.

Figure 103 Advanced Application > Multicast

Multicast Status			Multicast Setting								
Port	Total	VID	Multicast Group (Filter Mode)	Client IP	Up Time						
Multicast Group Member											
VID	Total		Multicast Group	Number	Member						
Clear IGMP Counter											
<input checked="" type="radio"/> Any	Port	<input type="button" value="Clear Counter"/>									
<input type="radio"/> Port	1										
IGMP Per Port Receive Counter											
Port	V1	V2	Report In	Query In	Dropped By						
	Leave	V3	V1	V2	V3						
1	0	0	0	0	0						
2	0	0	0	0	0						
3	0	0	0	0	0						
4	0	0	0	0	0						
5	0	0	0	0	0						
6	0	0	0	0	0						
7	0	0	0	0	0						
8	0	0	0	0	0						
9	0	0	0	0	0						
20	0	0	0	0	0						
21	0	0	0	0	0						
22	0	0	0	0	0						
23	0	0	0	0	0						
24	0	0	0	0	0						
IGMP Per Port Specific Counter											
Port	Total	GroupNum	Join	Leave	Dropped By						
				MaxGroup	Filter MVR Others						
1	0	0	0	0	0 0 0						
2	0	0	0	0	0 0 0						
3	0	0	0	0	0 0 0						
4	0	0	0	0	0 0 0						
5	0	0	0	0	0 0 0						
6	0	0	0	0	0 0 0						
7	0	0	0	0	0 0 0						
8	0	0	0	0	0 0 0						
19	0	0	0	0	0 0 0						
20	0	0	0	0	0 0 0						
21	0	0	0	0	0 0 0						
22	0	0	0	0	0 0 0						
23	0	0	0	0	0 0 0						
24	0	0	0	0	0 0 0						
IGMP Per Port Transmit Counter											
Port	V1	V2	Report Out	Leave	V3	V1	V2	V3			
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			
16	0	0	0	0	0	0	0	0			
17	0	0	0	0	0	0	0	0			
18	0	0	0	0	0	0	0	0			
19	0	0	0	0	0	0	0	0			
20	0	0	0	0	0	0	0	0			
21	0	0	0	0	0	0	0	0			
22	0	0	0	0	0	0	0	0			
23	0	0	0	0	0	0	0	0			
24	0	0	0	0	0	0	0	0			
IGMP Per VLAN Receive Counter						IGMP Per VLAN Specific Counter					
VID	V1	V2	Report In	Leave	V3	V1	V2	V3	Dropped By		
						Total	GroupNum	Join	Leave	MaxGroup	Filter MVR Others
IGMP Per VLAN Specific Counter						IGMP Per VLAN Transmit Counter			IGMP Per Port Querier Source IP		
VID	V1	V2	Report Out	Leave	V3	V1	V2	V3	Querier Source IP		

The following table describes the labels in this screen.

Table 56 Advanced Application > Multicast

LABEL	DESCRIPTION
Multicast Status	
Port	This column displays the numbers of the ports belonging to a multicast group and the port's bonding group ID if it is a member of one. A star (*) displays if the port is the main port in the bonding group.
Total	This field displays to how many multicast groups this port belongs. In the IPTV application, a multicast group represents a TV channel. This field shows how many TV channels have been subscribed to on this port.
VID	This field displays the multicast VLAN ID.

Table 56 Advanced Application > Multicast

LABEL	DESCRIPTION
Multicast Group (Filter Mode) Source Address	<p>This field displays the multicast group source address and source filtering mode. In IPTV, the multicast group source address means the address of a media server which provides media content.</p> <p>IGMPv3 and MLdv2 supports multicast source filtering.</p> <p>In INCLUDE mode, the client listens to the specified sources only.</p> <p>In EXCLUDE mode, the client listens to all sources other than the specified address.</p> <p>When the OLT receives a multicast packet destined to a configured multicast group and the packet's source address is in the INCLUDE list or not in the EXCLUDE list, the OLT forwards the packets to the clients that join this group.</p>
Client IP	This field displays an IP address which is a member in this multicast group. In IPTV, this means the IP address of a set-top box connected to this port.
Up Time	This field displays how long (in hh:mm:ss format) this port has been a member of the multicast group since the last time it joined. In IPTV, this means how long a user has been watching this channel.
Multicast Group Member	
VID	This field displays the multicast VLAN ID.
Total	This field displays how many ports in this VLAN.
Multicast Group	This field displays the IP multicast group addresses in this VLAN.
Number	This field displays how many ports belong to this multicast group.
Member	This field displays the port number(s) that belong to the multicast group. The port's bonding group ID also displays in brackets if the port has joined one.
Clear IGMP Counter	
Any	Select this, select Port or Vlan from the drop-down list box and then click Clear Counter to have the OLT clear IGMP counters for all ports or for all VLANs.
Port	Select this, select a port number from the drop-down list box and then click Clear Counter to have the OLT clear IGMP counters for the port.
IGMP Per Port Receive Counter	
This section displays incoming multicast traffic statistics per port.	
Port	This field displays a port number and the port's bonding group ID if it has joined one. A star (*) displays if the port is the main port in the bonding group.
Report In	This column displays how many V1 , V2 , and V3 multicast join messages and multicast Leave messages the port has received since the last start up or clearing of the IGMP counters. V1 , V2 , and V3 means IGMP versions 1, 2 and 3.
Query In	This column displays how many V1 , V2 , and V3 multicast queries the port has received.
Dropped By	<p>This column displays the number of multicast queries this port has dropped due to the following reasons:</p> <p>Rate: the receiving rate exceeds the configured rate limit setting. You can configure the limit setting for the port in the Basic Setting > Port Setup screen.</p> <p>Others: packets are dropped due to reasons other than the previous one.</p>
IGMP Per Port Specific Counter	
This section displays multicast traffic statistics per port.	
Port	This field displays a port number and the port's bonding group ID if it has joined one. A star (*) displays if the port is the main port in the bonding group.
Total GroupNum	This field displays the total number of multicast groups this port has learned since the last start up or clearing of the IGMP counters.
Join	This field displays the number of multicast groups in Join messages this port has received.

Table 56 Advanced Application > Multicast

LABEL	DESCRIPTION								
Leave	This field displays the number of multicast groups in Leave messages this port has received.								
Dropped By	<p>This column displays the number of multicast queries this port has dropped due to the following reasons:</p> <p>MaxGroup: the number of multicast groups the port has joined exceeds the per-port Max Group Limit configured in the Advanced Application > Multicast > Multicast Setting screen.</p> <p>Filter: the port is not allowed to join a multicast group in a multicast join message this port received. You can configure the filtering list in the Advanced Application > Multicast > Multicast Setting screen.</p> <p>MVR: this port is not configured as a receiver port in the MVR multicast VLAN. You can configure the MVR settings in the Advanced Application > Multicast > Multicast Setting > MVR screen.</p> <p>Others: reasons other than the ones described above, such as the OLT has insufficient memory.</p>								
IGMP Per Port Transmit Counter	<p>This section displays outgoing multicast traffic statistics per port.</p> <table border="1"> <tr> <td>Port</td><td>This field displays a port number and the port's bonding group ID if it has joined one. A star (*) displays if the port is the main port in the bonding group.</td></tr> <tr> <td>Report Out</td><td>This column displays how many V1, V2, and V3 multicast join messages and multicast Leave messages the port has transmitted. V1, V2, and V3 means IGMP versions 1, 2 and 3.</td></tr> <tr> <td>Query Out</td><td>This column displays how many valid V1, V2, and V3 multicast queries the port has transmitted.</td></tr> </table>	Port	This field displays a port number and the port's bonding group ID if it has joined one. A star (*) displays if the port is the main port in the bonding group.	Report Out	This column displays how many V1 , V2 , and V3 multicast join messages and multicast Leave messages the port has transmitted. V1 , V2 , and V3 means IGMP versions 1, 2 and 3.	Query Out	This column displays how many valid V1 , V2 , and V3 multicast queries the port has transmitted.		
Port	This field displays a port number and the port's bonding group ID if it has joined one. A star (*) displays if the port is the main port in the bonding group.								
Report Out	This column displays how many V1 , V2 , and V3 multicast join messages and multicast Leave messages the port has transmitted. V1 , V2 , and V3 means IGMP versions 1, 2 and 3.								
Query Out	This column displays how many valid V1 , V2 , and V3 multicast queries the port has transmitted.								
IGMP Per VLAN Receive Counter	<p>This section displays incoming multicast traffic statistics per VLAN network.</p> <table border="1"> <tr> <td>VID</td><td>This field displays the multicast VLAN ID.</td></tr> <tr> <td>Report In</td><td>This column displays how many V1, V2, and V3 multicast join messages and multicast Leave messages this VLAN network has received. V1, V2, and V3 means IGMP versions 1, 2 and 3.</td></tr> <tr> <td>Query In</td><td>This column displays how many valid V1, V2, and V3 multicast queries this VLAN network has received.</td></tr> <tr> <td>Dropped By</td><td> <p>This column displays how many multicast queries that have been dropped in this VLAN due to the following reasons:</p> <p>Rate: the receiving rate of the ports in this VLAN exceeds the configured rate limits. You can configure the limit settings in the Basic Setting > Port Setup screen.</p> <p>Others: reasons other than the previous one.</p> </td></tr> </table>	VID	This field displays the multicast VLAN ID.	Report In	This column displays how many V1 , V2 , and V3 multicast join messages and multicast Leave messages this VLAN network has received. V1 , V2 , and V3 means IGMP versions 1, 2 and 3.	Query In	This column displays how many valid V1 , V2 , and V3 multicast queries this VLAN network has received.	Dropped By	<p>This column displays how many multicast queries that have been dropped in this VLAN due to the following reasons:</p> <p>Rate: the receiving rate of the ports in this VLAN exceeds the configured rate limits. You can configure the limit settings in the Basic Setting > Port Setup screen.</p> <p>Others: reasons other than the previous one.</p>
VID	This field displays the multicast VLAN ID.								
Report In	This column displays how many V1 , V2 , and V3 multicast join messages and multicast Leave messages this VLAN network has received. V1 , V2 , and V3 means IGMP versions 1, 2 and 3.								
Query In	This column displays how many valid V1 , V2 , and V3 multicast queries this VLAN network has received.								
Dropped By	<p>This column displays how many multicast queries that have been dropped in this VLAN due to the following reasons:</p> <p>Rate: the receiving rate of the ports in this VLAN exceeds the configured rate limits. You can configure the limit settings in the Basic Setting > Port Setup screen.</p> <p>Others: reasons other than the previous one.</p>								
IGMP Per VLAN Specific Counter	<p>This section displays multicast traffic statistics per VLAN network.</p> <table border="1"> <tr> <td>VID</td><td>This field displays the multicast VLAN ID.</td></tr> <tr> <td>Total GroupNum</td><td>This field displays the total number of multicast groups this VLAN network has learned since the last start up or clearing of the IGMP counters.</td></tr> <tr> <td>Join</td><td>This field displays the number of multicast groups in Join messages this port has received.</td></tr> <tr> <td>Leave</td><td>This field displays the number of multicast groups in Leave messages this port has received.</td></tr> </table>	VID	This field displays the multicast VLAN ID.	Total GroupNum	This field displays the total number of multicast groups this VLAN network has learned since the last start up or clearing of the IGMP counters.	Join	This field displays the number of multicast groups in Join messages this port has received.	Leave	This field displays the number of multicast groups in Leave messages this port has received.
VID	This field displays the multicast VLAN ID.								
Total GroupNum	This field displays the total number of multicast groups this VLAN network has learned since the last start up or clearing of the IGMP counters.								
Join	This field displays the number of multicast groups in Join messages this port has received.								
Leave	This field displays the number of multicast groups in Leave messages this port has received.								

Table 56 Advanced Application > Multicast

LABEL	DESCRIPTION
Dropped By	<p>This column displays how many multicast queries that have been dropped in this VLAN due to the following reasons:</p> <p>MaxGroup: the number of multicast groups the ports in this VLAN have joined exceeds the per-port Max Group Limit configured in the Advanced Application > Multicast > Multicast Setting screen.</p> <p>Filter: the VLAN is not allowed to join a multicast group in a multicast join message the ports in this VLAN received. You can configure the filtering list in the Advanced Application > Multicast > Multicast Setting screen.</p> <p>MVR: the receiving ports in this VLAN are not the receiver ports in the MVR multicast VLANs. You can configure the MVR settings in the Advanced Application > Multicast > Multicast Setting > MVR screen.</p> <p>Others: reasons other than the ones described above, such as the OLT has insufficient memory.</p>
IGMP Per VLAN Transmit Counter	
This section displays outgoing multicast traffic statistics per VLAN network.	
Report Out	This column displays how many V1 , V2 , and V3 multicast join messages and multicast Leave messages sent on a VLAN network. V1 , V2 , and V3 means IGMP versions 1, 2 and 3.
VID	This field displays the multicast VLAN ID.
Query Out	This column displays how many valid V1 , V2 , and V3 multicast queries sent on a VLAN network.
IGMP Per Port Querier Source IP	
Index	This is the index number of the entry.
Port	The number of a port which has received multicast queries.
VID	The VLAN ID to which the received multicast queries belong.
Querier Source IP	The IP address of the device which sent the multicast queries.

21.3 Multicast Setting

Click **Advanced Application > Multicast > Multicast Setting** link to display the screen as shown. See [Section 21.1.2 on page 171](#) for more information on multicasting.

Figure 104 Advanced Application > Multicast > Multicast Setting

Port	Immed. Leave	IGMP Querier Mode
*	<input type="checkbox"/>	Auto ▾
1	<input checked="" type="checkbox"/>	Edge ▾
2	<input checked="" type="checkbox"/>	Edge ▾
3	<input checked="" type="checkbox"/>	Edge ▾
4	<input checked="" type="checkbox"/>	Edge ▾
5	<input checked="" type="checkbox"/>	Auto ▾
6	<input checked="" type="checkbox"/>	Auto ▾
15	<input checked="" type="checkbox"/>	Auto ▾
16	<input checked="" type="checkbox"/>	Auto ▾
17	<input checked="" type="checkbox"/>	Auto ▾
18	<input checked="" type="checkbox"/>	Auto ▾
19	<input checked="" type="checkbox"/>	Auto ▾
20	<input checked="" type="checkbox"/>	Auto ▾
21	<input checked="" type="checkbox"/>	Auto ▾
22	<input checked="" type="checkbox"/>	Auto ▾
23	<input checked="" type="checkbox"/>	Auto ▾
24	<input checked="" type="checkbox"/>	Auto ▾

The following table describes the labels in this screen.

Table 57 Advanced Application > Multicast > Multicast Setting

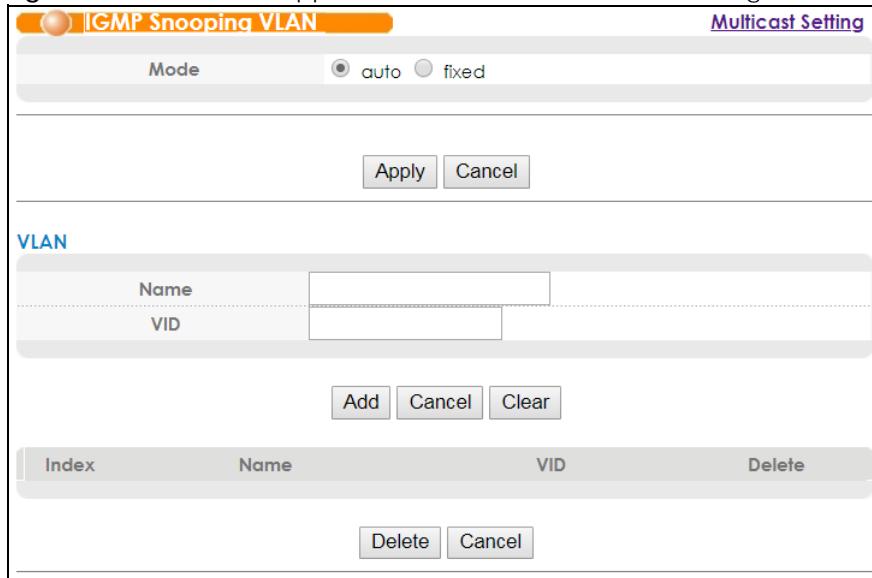
LABEL	DESCRIPTION
IGMP Action	Use these settings to configure multicast group membership discovery.
Enable MLD	Enables Multicast Listener Discovery version one (MLD v1) and version two (MLD v2) on the OLT. See Section 21.1.2 on page 171 for information about MLD.
Host Timeout	Specify the time (from 1 to 16,711,450) in seconds that elapses before the OLT removes an IGMP group membership entry if it does not receive report messages from the port.
Leave Timeout	Enter an IGMP leave timeout value (from 1 to 16,711,450) in seconds. This defines how many seconds the OLT waits for an IGMP report before removing an IGMP snooping membership entry when an IGMP leave message is received from a host.
802.1p Priority	Select a priority level (0-7) to which the OLT changes the priority in outgoing IGMP control packets. Otherwise, select No-Change to not replace the priority.
Proxy	Select MGMDv3 Mode to enable Multicast Group Membership Discovery version three (MGMDv3) and have the OLT send IGMPv3 or MLDv2 queries instead of IGMPv2 or MLDv1 queries. MGMDv2 indicates IGMPv2 in IPv4 networks and MLDv1 in IPv6 networks. MGMDv3 indicates IGMPv3 in IPv4 networks and MLDv2 in IPv6 networks. Note: MGMDv3 only applies in IGMP proxy mode.

Table 57 Advanced Application > Multicast > Multicast Setting

LABEL	DESCRIPTION
Unknown Multicast Frame	Specify the action to perform when the OLT receives an unknown multicast frame. Select Drop to discard the frame(s). Select Flooding to send the frame(s) to all ports.
Reserved Multicast Group	Multicast addresses (224.0.0.0 to 224.0.0.255) are reserved for the local scope. For examples, 224.0.0.1 is for all hosts in this subnet, 224.0.0.2 is for all multicast routers in this subnet, etc. A router will not forward a packet with the destination IP address within this range. See the IANA web site for more information. Specify the action to perform when the OLT receives a frame with a reserved multicast address. Select Drop to discard the frame(s). Select Flooding to send the frame(s) to all ports.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Immed. Leave	Select this option to set the OLT to remove this port from the multicast tree when an IGMP version 2 leave message is received on this port. Select this option if there is only one host connected to this port.
IGMP Querier Mode	The OLT treats an IGMP query port as being connected to an IGMP multicast router (or server). The OLT forwards IGMP join or leave packets to an IGMP query port. Select Auto to have the OLT use the port as an IGMP query port if the port receives IGMP query packets. Select Fixed to have the OLT always use the port as an IGMP query port. Select this when you connect an IGMP multicast server to the port. Select Edge to stop the OLT from using the port as an IGMP query port. The OLT will not keep any record of an IGMP router being connected to this port. The OLT does not forward IGMP join or leave packets to this port.
Apply	Click Apply to save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

21.3.1 IGMP Snooping VLAN

Click **Advanced Application > Multicast > Multicast Setting** in the navigation panel. Click the **IGMP Snooping VLAN** link to display the screen as shown. See [IGMP Snooping and VLANs on page 172](#) for more information on IGMP Snooping VLAN.

Figure 105 Advanced Application > Multicast > Multicast Setting > IGMP Snooping VLAN

The following table describes the labels in this screen.

Table 58 Advanced Application > Multicast > Multicast Setting > IGMP Snooping VLAN

LABEL	DESCRIPTION
Mode	Select auto to have the OLT learn multicast group membership information of any VLANs automatically. Select fixed to have the OLT only learn multicast group membership information of the VLAN(s) that you specify below. In either auto or fixed mode, the OLT can learn up to 16 VLANs. The OLT drops any IGMP control messages which do not belong to these 16 VLANs.
Apply	Click Apply to save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
VLAN	Use this section of the screen to add VLANs upon which the OLT is to perform IGMP snooping.
Name	Enter the descriptive name of the VLAN for identification purposes.
VID	Enter the ID of a static VLAN; the valid range is between 1 and 4094.
Add	Click this to create a new entry or to update an existing one. This saves your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields to your previous configuration.
Clear	Click Clear to reset the fields to the factory defaults.
Index	This is the index number of the IGMP snooping VLAN entry in the table. Click on an index number to view more details or change the settings.
Name	This field displays the descriptive name for this VLAN group.
VID	This field displays the ID number of the VLAN group.
Delete	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.

Table 58 Advanced Application > Multicast > Multicast Setting > IGMP Snooping VLAN (continued)

LABEL	DESCRIPTION
Delete	Check the entry(ies) that you want to remove, then click the Delete button.
Cancel	Click Cancel to clear the check boxes.

21.3.2 Mcast Channel

Use this screen to configure a GPON client multicast channel. Click **Advanced Application > Multicast > Multicast Setting** in the navigation panel. Click the **Mcast Channel** link to display the screen as shown.

Figure 106 Advanced Application > Multicast > Multicast Setting > Mcast Channel

Index	Name	Rule	Delete
*			<input type="checkbox"/>

The following table describes the labels in this screen.

Table 59 Advanced Application > Multicast > Multicast Setting > Mcast Channel

LABEL	DESCRIPTION
Mcast-Channel	
Active	Select this to have the settings configured here take effect.
Name	Enter a descriptive name for the entry.
start-group-ip	Specify the beginning IP address of the multicast IP address range. The range of addresses must be between 224.0.0.0 and 239.255.255.255.
end-group-ip	Specify the ending IP address of the multicast IP address range. The range of addresses must be between 224.0.0.0 and 239.255.255.255.
vlan	Enter the VLAN ID; the valid range is between 1 and 4094.
pbit	Select the IEEE 802.1p priority level to add to the untagged frames of this multicast channel.
src-ip	Specify the source IP of the IGMP server supplying this range of groups.
package-member	Assigns an ID number to this multicast channel. The valid range is between 1 and 32. Subscribers will be able to order package members according to this identifier.
Cac Profile	Select a QoS CAC profile. If you haven't created one, click Cac Profile Setting to do so.
preview-duration	Specify the duration in seconds (1-6000) that a subscriber can join to a group. This field is meaningful only when this multicast channel is ordered by subscribers with preview privilege.
preview-count	Specify the maximum number of times (1-100) a subscriber can preview this multicast channel's content. This field is meaningful only when this multicast channel is ordered by subscribers with preview privilege.

Table 59 Advanced Application > Multicast > Multicast Setting > Mcast Channel

LABEL	DESCRIPTION
preview-blackout	Specify the duration in seconds (0-7200) that a subscriber has to wait between 2 times of previewing a group. This field is meaningful only when this multicast channel is ordered by subscribers with preview privilege.
Add	Click this to create a new entry or to update an existing one. This saves your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields to your previous configuration.
Clear	Click Clear to reset the fields to the factory defaults.
Index	This is the index number of the entry.
*	Use this row to select all of the profiles for deletion.
Name	This displays the name of the entry.
Rule	This displays the multicast channel settings of this entry.
Delete	Select this for one or more profiles and click Delete to remove them.
Delete	Click Delete to remove the profiles with the Delete option selected.
Cancel	Click Cancel to begin configuring the screen again.

CHAPTER 22

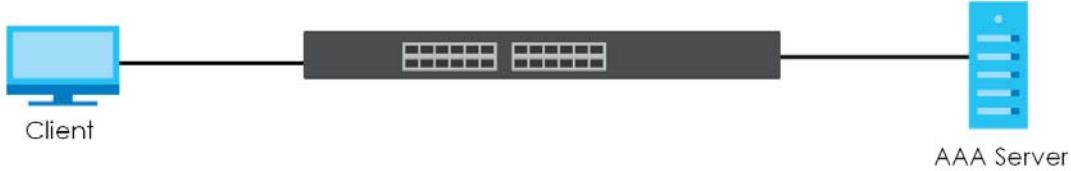
AAA

22.1 AAA Overview

This chapter describes how to configure authentication, authorization and accounting settings on the OLT.

The external servers that perform authentication, authorization and accounting functions are known as AAA servers. The OLT supports RADIUS (Remote Authentication Dial-In User Service, see [RADIUS and TACACS+ on page 183](#)) as the external authentication and authorization server.

Figure 107 AAA Server



22.1.1 What You Can Do

- Use the **AAA** screen ([Section 22.2 on page 183](#)) to display the links to the screens where you can enable authentication and authorization or both of them on the OLT.
- use the **RADIUS Server Setup** screen ([Section 22.3 on page 183](#)) to configure your RADIUS server settings.
- Use the **TACACS+ Server Setup** screen ([Section 22.4 on page 185](#)) to configure your TACACS+ authentication settings.
- Use the **AAA Setup** screen ([Section 22.5 on page 186](#)) to configure authentication, authorization and accounting settings, such as the methods used to authenticate users accessing the OLT and which database the OLT should use first.

22.1.2 What You Need to Know

Authentication is the process of determining who a user is and validating access to the OLT. The OLT can authenticate users who try to log in based on user accounts configured on the OLT itself. The OLT 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 OLT but user B cannot. The OLT can authorize users based on user accounts configured on the OLT 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 OLT can use an external server to track when users log in, log out, and so on. Accounting can also record system related actions such as boot up and shut down times of the OLT.

Local User Accounts

By storing user profiles locally on the OLT, your OLT is able to authenticate and authorize users without interacting with a network AAA server. However, there is a limit on the number of users you may authenticate in this way (See [Section 38.4 on page 313](#)).

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 60 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 OLT) and the TACACS server is encrypted.

22.2 AAA Screens

The **AAA** screens allow you to enable authentication and authorization or both of them on the OLT. First, configure your authentication server settings (RADIUS) and then set up the authentication priority, activate authorization.

Click **Advanced Application > AAA** in the navigation panel to display the screen as shown.

Figure 108 Advanced Application > AAA



22.3 RADIUS Server Setup

Use this screen to configure your RADIUS server settings. See [RADIUS and TACACS+ on page 183](#) for more information on RADIUS servers and [Section 22.6.2 on page 190](#) for RADIUS attributes utilized by the authentication features on the OLT. Click on the **RADIUS Server Setup** link in the **AAA** screen to view the screen as shown.

Figure 109 Advanced Application > AAA > RADIUS Server Setup

The screenshot shows the RADIUS Server Setup interface under the AAA section. It is divided into two main sections: **Authentication Server** and **Accounting Server**.

Authentication Server:

- Mode:** index-priority
- Timeout:** 30 seconds
- Table:**

Index	IP Address	UDP Port	Shared Secret	Delete
1	0.0.0.0	1812		<input type="checkbox"/>
2	0.0.0.0	1812		<input type="checkbox"/>
- Buttons:** Apply, Cancel

Accounting Server:

- Timeout:** 30 seconds
- Table:**

Index	IP Address	UDP Port	Shared Secret	Delete
1	0.0.0.0	1813		<input type="checkbox"/>
2	0.0.0.0	1813		<input type="checkbox"/>
- Buttons:** Apply, Cancel

The following table describes the labels in this screen.

Table 61 Advanced Application > AAA > RADIUS Server Setup

LABEL	DESCRIPTION
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 OLT tries to authenticate with the first configured RADIUS server, if the RADIUS server does not respond then the OLT 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 OLT waits for an authentication 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 OLT waits for a response from the first RADIUS server for 15 seconds and then tries the second RADIUS server.
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.
UDP 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 OLT. This key is not sent over the network. This key must be the same on the external RADIUS server and the OLT.

Table 61 Advanced Application > AAA > RADIUS Server Setup (continued)

LABEL	DESCRIPTION
Delete	Check this box if you want to remove an existing RADIUS server entry from the OLT. This entry is deleted when you click Apply .
Accounting Server	Use this section to configure your RADIUS accounting server settings.
Timeout	Specify the amount of time in seconds that the OLT waits for an accounting request response from the RADIUS accounting server.
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.
UDP Port	The default port of a RADIUS accounting server for accounting is 1813 . 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 accounting server and the OLT. This key is not sent over the network. This key must be the same on the external RADIUS accounting server and the OLT.
Delete	Check this box if you want to remove an existing RADIUS accounting server entry from the OLT. This entry is deleted when you click Apply .
Apply	Click Apply to save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

22.4 TACACS+ Server Setup

Use this screen to configure your TACACS+ server settings. See [RADIUS and TACACS+ on page 183](#) for more information on TACACS+ servers. Click on the **TACACS+ Server Setup** link in the **AAA** screen to view the screen as shown.

Figure 110 Advanced Application > AAA > TACACS+ Server Setup

The screenshot shows the TACACS+ Server Setup interface divided into two main sections: **Authentication Server** and **Accounting Server**.

Authentication Server:

- Mode:** index-priority
- Timeout:** 30 seconds
- Table:**

Index	IP Address	TCP Port	Shared Secret	Delete
1	0.0.0.0	49		<input type="checkbox"/>
2	0.0.0.0	49		<input type="checkbox"/>
- Buttons:** Apply, Cancel

Accounting Server:

- Timeout:** 30 seconds
- Table:**

Index	IP Address	TCP Port	Shared Secret	Delete
1	0.0.0.0	49		<input type="checkbox"/>
2	0.0.0.0	49		<input type="checkbox"/>
- Buttons:** Apply, Cancel

The following table describes the labels in this screen.

Table 62 Advanced Application > AAA > TACACS+ Server Setup

LABEL	DESCRIPTION
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 OLT tries to authenticate with the first configured TACACS+ server, if the TACACS+ server does not respond then the OLT 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 (between 1 to 1000) that the OLT 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 OLT waits for a response from the first TACACS+ server for 15 seconds and then tries the second TACACS+ server.
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.
TCP 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 OLT. This key is not sent over the network. This key must be the same on the external TACACS+ server and the OLT.
Delete	Check this box if you want to remove an existing TACACS+ server entry from the OLT. This entry is deleted when you click Apply .
Accounting Server	Use this section to configure your TACACS+ accounting settings.
Timeout	Specify the amount of time in seconds (between 1 to 1000) that the OLT waits for an accounting request response from the TACACS+ server.
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.
TCP Port	The default port of a TACACS+ accounting server 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 OLT. This key is not sent over the network. This key must be the same on the external TACACS+ accounting server and the OLT.
Delete	Check this box if you want to remove an existing TACACS+ accounting server entry from the OLT. This entry is deleted when you click Apply .
Apply	Click Apply to save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

22.5 AAA Setup

Use this screen to configure authentication, authorization and accounting settings on the OLT. Click on the **AAA Setup** link in the **AAA** screen to view the screen as shown.

Figure 111 Advanced Application > AAA > AAA Setup

AAA Setup

Authentication

Type	Method 1	Method 2	Method 3
Privilege Enable	local	-	-
Login	local	-	-

Authorization

Type	Active	Method
Exec	<input checked="" type="checkbox"/>	radius
Dot1x	<input checked="" type="checkbox"/>	radius

Accounting

Update Period		0 minutes			
Type	Active	Broadcast	Mode	Method	Privilege
System	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	-	radius	-
Exec	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	start-stop	radius	-
Dot1x	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	start-stop	radius	-
Commands	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	stop-only	tacacs+	0

Buttons: Apply, Cancel

The following table describes the labels in this screen.

Table 63 Advanced Application > AAA > AAA Setup

LABEL	DESCRIPTION
Authentication	Use this section to specify the methods used to authenticate users accessing the OLT.
Privilege Enable	<p>These fields specify which database the OLT should use (first, second and third) to authenticate access privilege level for administrator accounts (users for OLT management).</p> <p>Configure the access privilege of accounts via commands (See the CLI Reference Guide) for local authentication. The TACACS+ and RADIUS are external servers. Before you specify the priority, make sure you have set up the corresponding database correctly first.</p> <p>You can specify up to three methods for the OLT to authenticate the access privilege level of administrators. The OLT checks the methods in the order you configure them (first Method 1, then Method 2 and finally Method 3). You must configure the settings in the Method 1 field. If you want the OLT to check other sources for access privilege level specify them in Method 2 and Method 3 fields.</p> <p>Select local to have the OLT check the access privilege configured for local authentication.</p> <p>Select radius or tacacs+ to have the OLT check the access privilege via the external servers.</p>

Table 63 Advanced Application > AAA > AAA Setup (continued)

LABEL	DESCRIPTION
Login	<p>These fields specify which database the OLT should use (first, second and third) to authenticate administrator accounts (users for OLT management).</p> <p>Configure the local user accounts in the Access Control > Logins screen. The RADIUS is a external server. Before you specify the priority, make sure you have set up the corresponding database correctly first.</p> <p>You can specify up to three methods for the OLT to authenticate administrator accounts. The OLT checks the methods in the order you configure them (first Method 1, and finally Method 2). You must configure the settings in the Method 1 field. If you want the OLT to check other sources for administrator accounts, specify them in the Method 2 field.</p> <p>Select local to have the OLT check the administrator accounts configured in the Access Control > Logins screen.</p> <p>Select radius to have the OLT check the administrator accounts configured via your RADIUS server.</p>
Authorization	Use this section to configure authorization settings on the OLT.
Type	<p>Set whether the OLT provides the following services to a user.</p> <ul style="list-style-type: none"> • Exec: Allow an administrator which logs into the OLT through Telnet or SSH to have a different access privilege level assigned via the external server. • Dot1x: Allow an IEEE 802.1x client to have different bandwidth limit or VLAN ID assigned via the external server.
Active	Select this to activate authorization for a specified event types.
Method	<p>Select whether you want to use RADIUS for authorization of specific types of events.</p> <p>RADIUS is the only method for IEEE 802.1x authorization.</p>
Accounting	Use this section to configure accounting settings on the OLT.
Update Period	This is the amount of time in minutes before the OLT sends an update to the accounting server. This is only valid if you select the start-stop option for the Exec or Dot1x entries.
Type	<p>The OLT supports the following types of events to be sent to the accounting server(s):</p> <ul style="list-style-type: none"> • System - Configure the OLT to send information when the following system events occur: system boots up, system shuts down, system accounting is enabled, system accounting is disabled • Dot1x - Configure the OLT to send information when an IEEE 802.1x client begins a session (authenticates via the OLT), ends a session as well as interim updates of a session.
Active	Select this to activate accounting for a specified event types.
Broadcast	<p>Select this to have the OLT send accounting information to all configured accounting servers at the same time.</p> <p>If you don't select this and you have two accounting servers set up, then the OLT sends information to the first accounting server and if it doesn't get a response from the accounting server then it tries the second accounting server.</p>
Mode	<p>The OLT supports two modes of recording login events. Select:</p> <ul style="list-style-type: none"> • start-stop - to have the OLT 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 OLT send information to the accounting server only when a user ends a session.
Method	Select whether you want to use RADIUS for accounting of specific types of events.

Table 63 Advanced Application > AAA > AAA Setup (continued)

LABEL	DESCRIPTION
Apply	Click Apply to save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

22.6 Technical Reference

This section provides technical background information on the topics discussed in this chapter.

22.6.1 Vendor Specific Attribute

RFC 2865 standard specifies a method for sending vendor-specific information between a RADIUS server and a network access device (for example, the OLT). A company can create Vendor Specific Attributes (VSAs) to expand the functionality of a RADIUS server.

The OLT supports VSAs that allow you to perform the following actions based on user authentication:

- Limit bandwidth on incoming or outgoing traffic for the port the user connects to.
- Assign account privilege levels (See the CLI Reference Guide for more information on account privilege levels) for the authenticated user.

The VSAs are composed of the following:

- **Vendor-ID:** An identification number assigned to the company by the IANA (Internet Assigned Numbers Authority). Zyxel's vendor ID is 890.
- **Vendor-Type:** A vendor specified attribute, identifying the setting you want to modify.
- **Vendor-data:** A value you want to assign to the setting.

Note: Refer to the documentation that comes with your RADIUS server on how to configure VSAs for users authenticating via the RADIUS server.

The following table describes the VSAs supported on the OLT.

Table 64 Supported VSAs

FUNCTION	ATTRIBUTE
Ingress Bandwidth Assignment	Vendor-Id = 890 Vendor-Type = 1 Vendor-data = ingress rate (Kbps in decimal format)

Table 64 Supported VSAs

FUNCTION	ATTRIBUTE
Egress Bandwidth Assignment	Vendor-Id = 890 Vendor-Type = 2 Vendor-data = egress rate (Kbps in decimal format)
Privilege Assignment	Vendor-ID = 890 Vendor-Type = 3 Vendor-Data = " shell:priv-lvl=N " or Vendor-ID = 9 (CISCO) Vendor-Type = 1 (CISCO-AVPAIR) Vendor-Data = " shell:priv-lvl=N " where N is a privilege level (from 0 to 14). Note: If you set the privilege level of a login account differently on the RADIUS server(s) and the OLT, the user is assigned a privilege level from the database (RADIUS or local) the OLT uses first for user authentication.

22.6.1.1 Tunnel Protocol Attribute

You can configure tunnel protocol attributes on the RADIUS server (refer to your RADIUS server documentation) to assign a port on the OLT to a VLAN based on IEEE 802.1x authentication. The port VLAN settings are fixed and untagged. This will also set the port's VID. The following table describes the values you need to configure. Note that the bolded values in the table are fixed values as defined in RFC 3580.

Table 65 Supported Tunnel Protocol Attribute

FUNCTION	ATTRIBUTE
VLAN Assignment	Tunnel-Type = VLAN(13) Tunnel-Medium-Type = 802(6) Tunnel-Private-Group-ID = VLAN ID Note: You must also create a VLAN with the specified VID on the OLT.

22.6.2 Supported RADIUS Attributes

Remote Authentication Dial-In User Service (RADIUS) attributes are data used to define specific authentication elements in a user profile, which is stored on the RADIUS server. This appendix lists the RADIUS attributes supported by the OLT.

Refer to RFC 2865 for more information about RADIUS attributes used for authentication.

This section lists the attributes used by authentication functions on the OLT. In cases where the attribute has a specific format associated with it, the format is specified.

22.6.3 Attributes Used for Authentication

The following sections list the attributes sent from the OLT to the RADIUS server when performing authentication.

22.6.3.1 Attributes Used for Authenticating Privilege Access

User-Name

- The format of the User-Name attribute is \$enab#\$, where # is the privilege level (1-14).

User-Password

NAS-Identifier

NAS-IP-Address

22.6.3.2 Attributes Used to Login Users

User-Name

User-Password

NAS-Identifier

NAS-IP-Address

22.6.3.3 Attributes Used by the IEEE 802.1x Authentication

User-Name

NAS-Identifier

NAS-IP-Address

NAS-Port

NAS-Port-Type

- This value is set to **Ethernet(15)** on the OLT.

Calling-Station-Id

Frame-MTU

EAP-Message

State

Message-Authenticator

CHAPTER 23

IP Source Guard

23.1 IP Source Guard Overview

Use IP source guard to filter unauthorized DHCP and ARP packets in your network.

IP source guard uses a binding table to distinguish between authorized and unauthorized DHCP and ARP packets in your network. A binding contains these key attributes:

- MAC address
- VLAN ID
- IP address
- Port number

When the OLT receives a DHCP or ARP packet, it looks up the appropriate MAC address, VLAN ID, IP address, and port number in the binding table. If there is a binding, the OLT forwards the packet. If there is not a binding, the OLT discards the packet.

23.1.1 What You Can Do

- Use the **IP Source Guard Setup** screen ([Section 23.2 on page 193](#)) to look at the current bindings for DHCP snooping and ARP inspection.
- Use the **IP Source Guard Static Binding** screen ([Section 23.3 on page 194](#)) to manage static bindings for DHCP snooping and ARP inspection.
- Use the **DHCP Snooping** screen ([Section 23.4 on page 195](#)) to look at various statistics about the DHCP snooping database.
- Use this **DHCP Snooping Configure** screen ([Section 23.5 on page 198](#)) to enable DHCP snooping on the OLT (not on specific VLAN), specify the VLAN where the default DHCP server is located, and configure the DHCP snooping database.
- Use the **DHCP Snooping Port Configure** screen ([Section 23.5.1 on page 200](#)) to specify whether ports are trusted or untrusted ports for DHCP snooping.
- Use the **DHCP Snooping VLAN Configure** screen ([Section 23.5.2 on page 201](#)) to enable DHCP snooping on each VLAN and to specify whether or not the OLT adds DHCP relay agent option 82 information to DHCP requests that the OLT relays to a DHCP server for each VLAN.
- Use the **ARP Inspection Status** screen ([Section 23.6 on page 202](#)) to look at the current list of MAC address filters that were created because the OLT identified an unauthorized ARP packet.
- Use the **ARP Inspection VLAN Status** screen ([Section 23.7 on page 203](#)) to look at various statistics about ARP packets in each VLAN.
- Use the **ARP Inspection Log Status** screen ([Section 23.8 on page 204](#)) to look at log messages that were generated by ARP packets and that have not been sent to the syslog server yet.

- Use the **ARP Inspection Configure** screen ([Section 23.9 on page 205](#)) to enable ARP inspection on the OLT. You can also configure the length of time the OLT stores records of discarded ARP packets and global settings for the ARP inspection log.
- Use the **ARP Inspection Port Configure** screen ([Section 23.9.1 on page 207](#)) to specify whether ports are trusted or untrusted ports for ARP inspection.
- Use the **ARP Inspection VLAN Configure** screen ([Section 23.9.2 on page 208](#)) to enable ARP inspection on each VLAN and to specify when the OLT generates log messages for receiving ARP packets from each VLAN.

23.1.2 What You Need to Know

The OLT builds the binding table by snooping DHCP packets (dynamic bindings) and from information provided manually by administrators (static bindings).

IP source guard consists of the following features:

- Static bindings. Use this to create static bindings in the binding table.
- DHCP snooping. Use this to filter unauthorized DHCP packets on the network and to build the binding table dynamically.
- ARP inspection. Use this to filter unauthorized ARP packets on the network.

If you want to use dynamic bindings to filter unauthorized ARP packets (typical implementation), you have to enable DHCP snooping before you enable ARP inspection.

23.2 IP Source Guard Setup

Use this screen to look at the current bindings for DHCP snooping and ARP inspection. Bindings are used by DHCP snooping and ARP inspection to distinguish between authorized and unauthorized packets in the network. The OLT learns the bindings by snooping DHCP packets (dynamic bindings) and from information provided manually by administrators (static bindings). To open this screen, click **Advanced Application > IP Source Guard > IP Source Guard Setup**.

Figure 112 Advanced Application > IP Source Guard



The following table describes the labels in this screen.

Table 66 Advanced Application > IP Source Guard

LABEL	DESCRIPTION
Index	This field displays a sequential number for each binding.
MAC Address	This field displays the source MAC address in the binding.
IP Address	This field displays the IP address assigned to the MAC address in the binding.
Lease	This field displays how many days, hours, minutes, and seconds the binding is valid; for example, 2d3h4m5s means the binding is still valid for 2 days, 3 hours, 4 minutes, and 5 seconds. This field displays infinity if the binding is always valid (for example, a static binding).

Table 66 Advanced Application > IP Source Guard

LABEL	DESCRIPTION
Type	This field displays how the OLT learned the binding. static: This binding was learned from information provided manually by an administrator. dhcp-snooping: This binding was learned by snooping DHCP packets.
VID	This field displays the source VLAN ID in the binding.
Port	This field displays the port number in the binding. If this field is blank, the binding applies to all ports.

23.3 IP Source Guard Static Binding

Use this screen to manage static bindings for DHCP snooping and ARP inspection. Static bindings are uniquely identified by the MAC address and VLAN ID. Each MAC address and VLAN ID can only be in one static binding. If you try to create a static binding with the same MAC address and VLAN ID as an existing static binding, the new static binding replaces the original one. To open this screen, click **Advanced Application > IP Source Guard > Static Binding**.

Figure 113 Advanced Application > IP Source Guard > Static Binding

The screenshot shows a configuration interface for static bindings. At the top, there's a header bar with tabs for 'IPSG' and 'IPSG'. Below the header, there are four input fields: 'MAC Address' (with a colon-separated hex input field), 'IP Address' (with a dotted decimal input field), 'VLAN' (with a dropdown menu), and 'Port' (with two radio button options: '1' and 'Any'). Below these fields are three buttons: 'Add', 'Cancel', and 'Clear'. At the bottom of the main area, there's a row of buttons labeled 'Index', 'MAC Address', 'IP Address', 'Lease', 'Type', 'VLAN', 'Port', and 'Delete'. In the footer, there are two more buttons: 'Delete' and 'Cancel'.

The following table describes the labels in this screen.

Table 67 Advanced Application > IP Source Guard > Static Binding

LABEL	DESCRIPTION
MAC Address	Enter the source MAC address in the binding.
IP Address	Enter the IP address assigned to the MAC address in the binding.
VLAN	Enter the source VLAN ID in the binding.
Port	Specify the port(s) in the binding. If this binding has one port, select the first radio button and enter the port number in the field to the right. If this binding applies to all ports, select Any .
Add	Click this to create the specified static binding or to update an existing one.
Cancel	Click this to reset the values above based on the last selected static binding or, if not applicable, to clear the fields above.
Clear	Click this to clear the fields above.
Index	This field displays a sequential number for each binding.
MAC Address	This field displays the source MAC address in the binding.

Table 67 Advanced Application > IP Source Guard > Static Binding (continued)

LABEL	DESCRIPTION
IP Address	This field displays the IP address assigned to the MAC address in the binding.
Lease	This field displays how long the binding is valid.
Type	This field displays how the OLT learned the binding. static: This binding was learned from information provided manually by an administrator.
VLAN	This field displays the source VLAN ID in the binding.
Port	This field displays the port number in the binding. If this field is blank, the binding applies to all ports.
Delete	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Check the entry(ies) that you want to remove and then click Delete to remove the selected entry(ies) from the summary table.
Cancel	Click Cancel to clear the check boxes.

23.4 DHCP Snooping

Use this screen to look at various statistics about the DHCP snooping database. To open this screen, click **Advanced Application > IP Source Guard > DHCP Snooping**.

Figure 114 Advanced Application > IP Source Guard > DHCP Snooping

DHCP Snooping		Configure	IPSG																																																																																																																																		
Database Status																																																																																																																																					
<table border="1"> <thead> <tr> <th>Description</th><th colspan="3">Status</th></tr> </thead> <tbody> <tr> <td>Agent URL</td><td colspan="3"></td></tr> <tr> <td>Write delay timer</td><td>300</td><td colspan="2">seconds</td></tr> <tr> <td>Abort timer</td><td>300</td><td colspan="2" rowspan="10">seconds</td></tr> <tr> <td colspan="4"> </td></tr> <tr> <td>Agent running</td><td colspan="3">None</td></tr> <tr> <td>Delay timer expiry</td><td colspan="3">Not Running</td></tr> <tr> <td>Abort timer expiry</td><td colspan="3" rowspan="2">Not Running</td></tr> <tr> <td colspan="4"> </td></tr> <tr> <td>Last succeeded time</td><td colspan="3">None</td></tr> <tr> <td>Last failed time</td><td colspan="3">None</td></tr> <tr> <td>Last failed reason</td><td colspan="3" rowspan="2">No failure recorded</td></tr> <tr> <td colspan="4"> <table border="1"> <thead> <tr> <th>Times</th></tr> </thead> <tbody> <tr> <td>Total attempts</td><td>0</td></tr> <tr> <td>Startup failures</td><td>0</td></tr> <tr> <td>Successful transfers</td><td>0</td></tr> <tr> <td>Failed transfers</td><td>0</td></tr> <tr> <td>Successful reads</td><td>0</td></tr> <tr> <td>Failed reads</td><td>0</td></tr> <tr> <td>Successful writes</td><td>0</td></tr> <tr> <td>Failed writes</td><td>0</td></tr> </tbody> </table> </td></tr> <tr> <td colspan="4"> </td></tr> <tr> <td colspan="4">Database detail</td></tr> <tr> <td> <table border="1"> <thead> <tr> <th>Description</th><th colspan="3">Status</th></tr> </thead> <tbody> <tr> <td>First successful access</td><td colspan="3" rowspan="2">None</td></tr> <tr> <td colspan="4">Last ignored bindings counters</td></tr> <tr> <td>Binding collisions</td><td colspan="3">0</td></tr> <tr> <td>Invalid interfaces</td><td colspan="3">0</td></tr> <tr> <td>Parse failures</td><td colspan="3">0</td></tr> <tr> <td>Expired leases</td><td colspan="3">0</td></tr> <tr> <td>Unsupported vlans</td><td colspan="3">0</td></tr> <tr> <td>Last ignored time</td><td colspan="3" rowspan="2">None</td></tr> <tr> <td colspan="4"> <table border="1"> <thead> <tr> <th>Total ignored bindings counters</th></tr> </thead> <tbody> <tr> <td>Binding collisions</td><td>0</td></tr> <tr> <td>Invalid interfaces</td><td>0</td></tr> <tr> <td>Parse failures</td><td>0</td></tr> <tr> <td>Expired leases</td><td>0</td></tr> <tr> <td>Unsupported vlans</td><td>0</td></tr> </tbody> </table> </td></tr> <tr> <td colspan="4"> </td></tr> </tbody> </table> </td></tr></tbody></table>	Description	Status			Agent URL				Write delay timer	300	seconds		Abort timer	300	seconds						Agent running	None			Delay timer expiry	Not Running			Abort timer expiry	Not Running							Last succeeded time	None			Last failed time	None			Last failed reason	No failure recorded			<table border="1"> <thead> <tr> <th>Times</th></tr> </thead> <tbody> <tr> <td>Total attempts</td><td>0</td></tr> <tr> <td>Startup failures</td><td>0</td></tr> <tr> <td>Successful transfers</td><td>0</td></tr> <tr> <td>Failed transfers</td><td>0</td></tr> <tr> <td>Successful reads</td><td>0</td></tr> <tr> <td>Failed reads</td><td>0</td></tr> <tr> <td>Successful writes</td><td>0</td></tr> <tr> <td>Failed writes</td><td>0</td></tr> </tbody> </table>				Times	Total attempts	0	Startup failures	0	Successful transfers	0	Failed transfers	0	Successful reads	0	Failed reads	0	Successful writes	0	Failed writes	0					Database detail				<table border="1"> <thead> <tr> <th>Description</th><th colspan="3">Status</th></tr> </thead> <tbody> <tr> <td>First successful access</td><td colspan="3" rowspan="2">None</td></tr> <tr> <td colspan="4">Last ignored bindings counters</td></tr> <tr> <td>Binding collisions</td><td colspan="3">0</td></tr> <tr> <td>Invalid interfaces</td><td colspan="3">0</td></tr> <tr> <td>Parse failures</td><td colspan="3">0</td></tr> <tr> <td>Expired leases</td><td colspan="3">0</td></tr> <tr> <td>Unsupported vlans</td><td colspan="3">0</td></tr> <tr> <td>Last ignored time</td><td colspan="3" rowspan="2">None</td></tr> <tr> <td colspan="4"> <table border="1"> <thead> <tr> <th>Total ignored bindings counters</th></tr> </thead> <tbody> <tr> <td>Binding collisions</td><td>0</td></tr> <tr> <td>Invalid interfaces</td><td>0</td></tr> <tr> <td>Parse failures</td><td>0</td></tr> <tr> <td>Expired leases</td><td>0</td></tr> <tr> <td>Unsupported vlans</td><td>0</td></tr> </tbody> </table> </td></tr> <tr> <td colspan="4"> </td></tr> </tbody> </table>	Description	Status			First successful access	None			Last ignored bindings counters				Binding collisions	0			Invalid interfaces	0			Parse failures	0			Expired leases	0			Unsupported vlans	0			Last ignored time	None			<table border="1"> <thead> <tr> <th>Total ignored bindings counters</th></tr> </thead> <tbody> <tr> <td>Binding collisions</td><td>0</td></tr> <tr> <td>Invalid interfaces</td><td>0</td></tr> <tr> <td>Parse failures</td><td>0</td></tr> <tr> <td>Expired leases</td><td>0</td></tr> <tr> <td>Unsupported vlans</td><td>0</td></tr> </tbody> </table>				Total ignored bindings counters	Binding collisions	0	Invalid interfaces	0	Parse failures	0	Expired leases	0	Unsupported vlans	0				
Description	Status																																																																																																																																				
Agent URL																																																																																																																																					
Write delay timer	300	seconds																																																																																																																																			
Abort timer	300	seconds																																																																																																																																			
Agent running	None																																																																																																																																				
Delay timer expiry	Not Running																																																																																																																																				
Abort timer expiry	Not Running																																																																																																																																				
Last succeeded time	None																																																																																																																																				
Last failed time	None																																																																																																																																				
Last failed reason	No failure recorded																																																																																																																																				
<table border="1"> <thead> <tr> <th>Times</th></tr> </thead> <tbody> <tr> <td>Total attempts</td><td>0</td></tr> <tr> <td>Startup failures</td><td>0</td></tr> <tr> <td>Successful transfers</td><td>0</td></tr> <tr> <td>Failed transfers</td><td>0</td></tr> <tr> <td>Successful reads</td><td>0</td></tr> <tr> <td>Failed reads</td><td>0</td></tr> <tr> <td>Successful writes</td><td>0</td></tr> <tr> <td>Failed writes</td><td>0</td></tr> </tbody> </table>				Times	Total attempts	0	Startup failures	0	Successful transfers	0	Failed transfers	0	Successful reads	0	Failed reads	0	Successful writes	0	Failed writes	0																																																																																																																	
Times																																																																																																																																					
Total attempts	0																																																																																																																																				
Startup failures	0																																																																																																																																				
Successful transfers	0																																																																																																																																				
Failed transfers	0																																																																																																																																				
Successful reads	0																																																																																																																																				
Failed reads	0																																																																																																																																				
Successful writes	0																																																																																																																																				
Failed writes	0																																																																																																																																				
Database detail																																																																																																																																					
<table border="1"> <thead> <tr> <th>Description</th><th colspan="3">Status</th></tr> </thead> <tbody> <tr> <td>First successful access</td><td colspan="3" rowspan="2">None</td></tr> <tr> <td colspan="4">Last ignored bindings counters</td></tr> <tr> <td>Binding collisions</td><td colspan="3">0</td></tr> <tr> <td>Invalid interfaces</td><td colspan="3">0</td></tr> <tr> <td>Parse failures</td><td colspan="3">0</td></tr> <tr> <td>Expired leases</td><td colspan="3">0</td></tr> <tr> <td>Unsupported vlans</td><td colspan="3">0</td></tr> <tr> <td>Last ignored time</td><td colspan="3" rowspan="2">None</td></tr> <tr> <td colspan="4"> <table border="1"> <thead> <tr> <th>Total ignored bindings counters</th></tr> </thead> <tbody> <tr> <td>Binding collisions</td><td>0</td></tr> <tr> <td>Invalid interfaces</td><td>0</td></tr> <tr> <td>Parse failures</td><td>0</td></tr> <tr> <td>Expired leases</td><td>0</td></tr> <tr> <td>Unsupported vlans</td><td>0</td></tr> </tbody> </table> </td></tr> <tr> <td colspan="4"> </td></tr> </tbody> </table>	Description	Status			First successful access	None			Last ignored bindings counters				Binding collisions	0			Invalid interfaces	0			Parse failures	0			Expired leases	0			Unsupported vlans	0			Last ignored time	None			<table border="1"> <thead> <tr> <th>Total ignored bindings counters</th></tr> </thead> <tbody> <tr> <td>Binding collisions</td><td>0</td></tr> <tr> <td>Invalid interfaces</td><td>0</td></tr> <tr> <td>Parse failures</td><td>0</td></tr> <tr> <td>Expired leases</td><td>0</td></tr> <tr> <td>Unsupported vlans</td><td>0</td></tr> </tbody> </table>				Total ignored bindings counters	Binding collisions	0	Invalid interfaces	0	Parse failures	0	Expired leases	0	Unsupported vlans	0																																																																																		
Description	Status																																																																																																																																				
First successful access	None																																																																																																																																				
Last ignored bindings counters																																																																																																																																					
Binding collisions	0																																																																																																																																				
Invalid interfaces	0																																																																																																																																				
Parse failures	0																																																																																																																																				
Expired leases	0																																																																																																																																				
Unsupported vlans	0																																																																																																																																				
Last ignored time	None																																																																																																																																				
<table border="1"> <thead> <tr> <th>Total ignored bindings counters</th></tr> </thead> <tbody> <tr> <td>Binding collisions</td><td>0</td></tr> <tr> <td>Invalid interfaces</td><td>0</td></tr> <tr> <td>Parse failures</td><td>0</td></tr> <tr> <td>Expired leases</td><td>0</td></tr> <tr> <td>Unsupported vlans</td><td>0</td></tr> </tbody> </table>				Total ignored bindings counters	Binding collisions	0	Invalid interfaces	0	Parse failures	0	Expired leases	0	Unsupported vlans	0																																																																																																																							
Total ignored bindings counters																																																																																																																																					
Binding collisions	0																																																																																																																																				
Invalid interfaces	0																																																																																																																																				
Parse failures	0																																																																																																																																				
Expired leases	0																																																																																																																																				
Unsupported vlans	0																																																																																																																																				

The following table describes the labels in this screen.

Table 68 Advanced Application > IP Source Guard > DHCP Snooping

LABEL	DESCRIPTION
Database Status	This section displays the current settings for the DHCP snooping database. You can configure them in the DHCP Snooping Configure screen. See Section 23.5 on page 198 .
Agent URL	This field displays the location of the DHCP snooping database.
Write delay timer	This field displays how long (in seconds) the OLT tries to complete a specific update in the DHCP snooping database before it gives up.

Table 68 Advanced Application > IP Source Guard > DHCP Snooping (continued)

LABEL	DESCRIPTION
Abort timer	This field displays how long (in seconds) the OLT waits to update the DHCP snooping database after the current bindings change.
	This section displays information about the current update and the next update of the DHCP snooping database.
Agent running	This field displays the status of the current update or access of the DHCP snooping database. none : The OLT is not accessing the DHCP snooping database. read : The OLT is loading dynamic bindings from the DHCP snooping database. write : The OLT is updating the DHCP snooping database.
Delay timer expiry	This field displays how much longer (in seconds) the OLT tries to complete the current update before it gives up. It displays Not Running if the OLT is not updating the DHCP snooping database right now.
Abort timer expiry	This field displays when (in seconds) the OLT is going to update the DHCP snooping database again. It displays Not Running if the current bindings have not changed since the last update.
	This section displays information about the last time the OLT updated the DHCP snooping database.
Last succeeded time	This field displays the last time the OLT updated the DHCP snooping database successfully.
Last failed time	This field displays the last time the OLT updated the DHCP snooping database unsuccessfully.
Last failed reason	This field displays the reason the OLT updated the DHCP snooping database unsuccessfully.
	This section displays historical information about the number of times the OLT successfully or unsuccessfully read or updated the DHCP snooping database.
Total attempts	This field displays the number of times the OLT has tried to access the DHCP snooping database for any reason.
Startup failures	This field displays the number of times the OLT could not create or read the DHCP snooping database when the OLT started up or a new URL is configured for the DHCP snooping database.
Successful transfers	This field displays the number of times the OLT read bindings from or updated the bindings in the DHCP snooping database successfully.
Failed transfers	This field displays the number of times the OLT was unable to read bindings from or update the bindings in the DHCP snooping database.
Successful reads	This field displays the number of times the OLT read bindings from the DHCP snooping database successfully.
Failed reads	This field displays the number of times the OLT was unable to read bindings from the DHCP snooping database.
Successful writes	This field displays the number of times the OLT updated the bindings in the DHCP snooping database successfully.
Failed writes	This field displays the number of times the OLT was unable to update the bindings in the DHCP snooping database.
Database detail	
First successful access	This field displays the first time the OLT accessed the DHCP snooping database for any reason.
Last ignored bindings counters	This section displays the number of times and the reasons the OLT ignored bindings the last time it read bindings from the DHCP binding database. You can clear these counters by restarting the OLT or using CLI commands. See the CLI Reference Guide.

Table 68 Advanced Application > IP Source Guard > DHCP Snooping (continued)

LABEL	DESCRIPTION
Binding collisions	This field displays the number of bindings the OLT ignored because the OLT already had a binding with the same MAC address and VLAN ID.
Invalid interfaces	This field displays the number of bindings the OLT ignored because the port number was a trusted interface or does not exist anymore.
Parse failures	This field displays the number of bindings the OLT ignored because the OLT was unable to understand the binding in the DHCP binding database.
Expired leases	This field displays the number of bindings the OLT ignored because the lease time had already expired.
Unsupported vlans	This field displays the number of bindings the OLT ignored because the VLAN ID does not exist anymore.
Last ignored time	This field displays the last time the OLT ignored any bindings for any reason from the DHCP binding database.
Total Ignored bindings counters	This section displays the reasons the OLT has ignored bindings any time it read bindings from the DHCP binding database. You can clear these counters by restarting the OLT or using CLI commands. See the CLI Reference Guide.
Binding collisions	This field displays the number of bindings the OLT has ignored because the OLT already had a binding with the same MAC address and VLAN ID.
Invalid interfaces	This field displays the number of bindings the OLT has ignored because the port number was a trusted interface or does not exist anymore.
Parse failures	This field displays the number of bindings the OLT has ignored because the OLT was unable to understand the binding in the DHCP binding database.
Expired leases	This field displays the number of bindings the OLT has ignored because the lease time had already expired.
Unsupported vlans	This field displays the number of bindings the OLT has ignored because the VLAN ID does not exist anymore.

23.5 DHCP Snooping Configure

Use this screen to enable DHCP snooping on the OLT (not on specific VLAN), specify the VLAN where the default DHCP server is located, and configure the DHCP snooping database. The DHCP snooping database stores the current bindings on a secure, external TFTP server so that they are still available after a restart. To open this screen, click **Advanced Application > IP Source Guard > DHCP Snooping > Configure**.

Figure 115 Advanced Application > IP Source Guard > DHCP Snooping > Configure

The screenshot shows the 'DHCP Snooping Configure' screen. At the top, there are tabs for Port, VLAN, and DHCP Snooping, with 'DHCP Snooping' being the active tab. Under the 'Active' section, the 'Active' checkbox is checked. In the 'DHCP Vlan' section, the '100' radio button is selected. The 'Database' section contains fields for 'Agent URL' (empty), 'Timeout interval' (300 seconds), and 'Write delay interval' (300 seconds). Below this is a 'Renew DHCP Snooping URL' button. At the bottom are 'Apply' and 'Cancel' buttons.

The following table describes the labels in this screen.

Table 69 Advanced Application > IP Source Guard > DHCP Snooping > Configure

LABEL	DESCRIPTION
Active	Select this to enable DHCP snooping on the OLT. You still have to enable DHCP snooping on specific VLAN and specify trusted ports. Note: If DHCP is enabled and there are no trusted ports, DHCP requests will not succeed.
DHCP Vlan	Select a VLAN ID if you want the OLT to forward DHCP packets to DHCP servers on a specific VLAN. Note: You have to enable DHCP snooping on the DHCP VLAN too. You can enable Option82 in the DHCP Snooping VLAN Configure screen (Section 23.5.2 on page 201) to help the DHCP servers distinguish between DHCP requests from different VLAN. Select Disable if you do not want the OLT to forward DHCP packets to a specific VLAN.
Database	If Timeout interval is greater than Write delay interval , it is possible that the next update is scheduled to occur before the current update has finished successfully or timed out. In this case, the OLT waits to start the next update until it completes the current one.
Agent URL	Enter the location of the DHCP snooping database. The location should be expressed like this: <code>ftp://(domain name or IP address)/directory, if applicable/file name</code> ; for example, <code>ftp://192.168.10.1/database.txt</code> .
Timeout interval	Enter how long (10-65535 seconds) the OLT tries to complete a specific update in the DHCP snooping database before it gives up.
Write delay interval	Enter how long (10-65535 seconds) the OLT waits to update the DHCP snooping database the first time the current bindings change after an update. Once the next update is scheduled, additional changes in current bindings are automatically included in the next update.

Table 69 Advanced Application > IP Source Guard > DHCP Snooping > Configure (continued)

LABEL	DESCRIPTION
Renew DHCP Snooping URL	Enter the location of a DHCP snooping database, and click Renew if you want the OLT to load it. You can use this to load dynamic bindings from a different DHCP snooping database than the one specified in Agent URL . When the OLT loads dynamic bindings from a DHCP snooping database, it does not discard the current dynamic bindings first. If there is a conflict, the OLT keeps the dynamic binding in volatile memory and updates the Binding collisions counter in the DHCP Snooping screen (Section 23.4 on page 195).
Apply	Click Apply to save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values in this screen to their last-saved values.

23.5.1 DHCP Snooping Port Configure

Use this screen to specify whether ports are trusted or untrusted ports for DHCP snooping.

Note: If DHCP snooping is enabled but there are no trusted ports, DHCP requests cannot reach the DHCP server.

You can also specify the maximum number for DHCP packets that each port (trusted or untrusted) can receive each second. To open this screen, click **Advanced Application > IP Source Guard > DHCP Snooping > Configure > Port**.

Figure 116 Advanced Application > IP Source Guard > DHCP Snooping > Configure > Port

The screenshot shows a configuration interface titled "DHCP Snooping Port Configure". At the top right is a "Configure" button. The main area is a table with columns: "Port", "Server Trusted state", and "Rate (pps)". The "Port" column lists ports 1 through 24. The "Server Trusted state" column contains dropdown menus for each port, with most set to "Untrusted" and port 5 set to "Trusted". The "Rate (pps)" column shows a series of small graphs for each port, all currently at 0. At the bottom are "Apply" and "Cancel" buttons.

Port	Server Trusted state	Rate (pps)
*	Untrusted ▾	
1	Untrusted ▾	0
2	Untrusted ▾	0
3	Untrusted ▾	0
4	Untrusted ▾	0
5	Trusted ▾	0
6	Untrusted ▾	0
7	Untrusted ▾	0
19	Untrusted ▾	0
20	Untrusted ▾	0
21	Untrusted ▾	0
22	Untrusted ▾	0
23	Untrusted ▾	0
24	Untrusted ▾	0

Apply **Cancel**

The following table describes the labels in this screen.

Table 70 Advanced Application > IP Source Guard > IPv4 Source Guard Setup > DHCP Snooping > Configure > Port

LABEL	DESCRIPTION
Port	This field displays the port number. If you configure the * port, the settings are applied to all of the ports.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Server Trusted state	Select whether this port is a trusted port (Trusted) or an untrusted port (Untrusted). Trusted ports are connected to DHCP servers or other switches, and the OLT discards DHCP packets from trusted ports only if the rate at which DHCP packets arrive is too high. Untrusted ports are connected to subscribers, and the OLT discards DHCP packets from untrusted ports in the following situations: <ul style="list-style-type: none"> • The packet is a DHCP server packet (for example, OFFER, ACK, or NACK). • The source MAC address and source IP address in the packet do not match any of the current bindings. • The packet is a RELEASE or DECLINE packet, and the source MAC address and source port do not match any of the current bindings. • The rate at which DHCP packets arrive is too high.
Rate (pps)	Specify the maximum number for DHCP packets (1-2048) that the OLT receives from each port each second. The OLT discards any additional DHCP packets. Enter 0 to disable this limit, which is recommended for trusted ports.
Apply	Click Apply to save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values in this screen to their last-saved values.

23.5.2 DHCP Snooping VLAN Configure

Use this screen to enable DHCP snooping on each VLAN and to specify whether or not the OLT adds DHCP relay agent option 82 information ([Chapter 36 on page 288](#)) to DHCP requests that the OLT relays to a DHCP server for each VLAN. To open this screen, click **Advanced Application > IP Source Guard > DHCP Snooping > Configure > VLAN**.

See [Section 23.10.1.4 on page 210](#) for more information about the configuration order for DHCP option 82 settings in different screens.

Figure 117 Advanced Application > IP Source Guard > DHCP Snooping > Configure > VLAN

VID	Enabled	Option82	Information
*	No	<input type="checkbox"/>	<input type="checkbox"/>

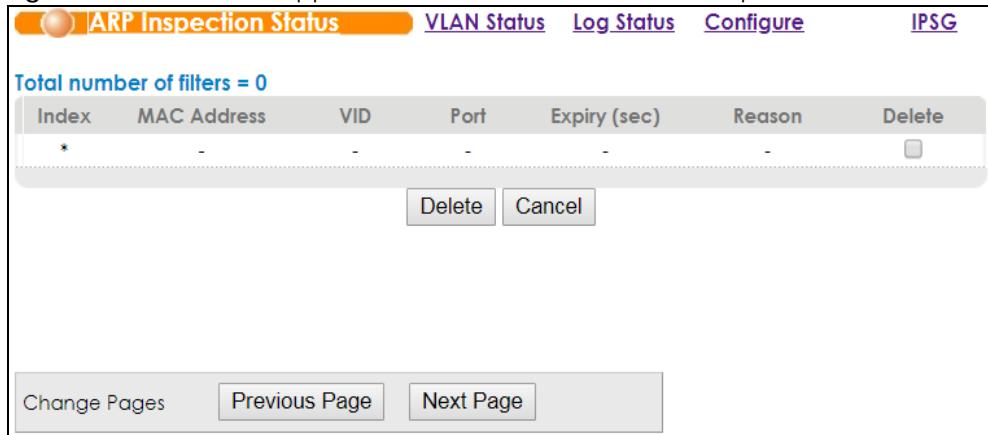
The following table describes the labels in this screen.

Table 71 Advanced Application > IP Source Guard > DHCP Snooping > Configure > VLAN

LABEL	DESCRIPTION
Show VLAN	Use this section to specify the VLANs you want to manage in the section below.
Start VID	Enter the lowest VLAN ID you want to manage in the section below.
End VID	Enter the highest VLAN ID you want to manage in the section below.
Apply	Click this to display the specified range of VLANs in the section below.
VID	This field displays the VLAN ID of each VLAN in the range specified above. If you configure the * VLAN, the settings are applied to all VLANs.
Enabled	Select Yes to enable DHCP snooping on the VLAN. You still have to enable DHCP snooping on the OLT and specify trusted ports. Note: The OLT will drop all DHCP requests if you enable DHCP snooping and there are no trusted ports.
Option 82	Select this to apply the DHCP option 82 profile to the specified port(s) in this VLAN.
Information	Select this so the OLT will add the information (such as slot number, port number, VLAN ID and/or system name) specified in the profile to DHCP requests that it broadcasts to the DHCP VLAN, if specified, or VLAN.
Apply	Click Apply to save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values in this screen to their last-saved values.

23.6 ARP Inspection Status

Use this screen to look at the current list of MAC address filters that were created because the OLT identified an unauthorized ARP packet. When the OLT identifies an unauthorized ARP packet, it automatically creates a MAC address filter to show the source MAC address and source VLAN ID of the unauthorized ARP packet currently. To open this screen, click **Advanced Application > IP Source Guard > ARP Inspection**.

Figure 118 Advanced Application > IP Source Guard > ARP Inspection

The following table describes the labels in this screen.

Table 72 Advanced Application > IP Source Guard > ARP Inspection

LABEL	DESCRIPTION
Total number of filters	This field displays the current number of MAC address filters that were created because the OLT identified unauthorized ARP packets.
Index	This field displays a sequential number for each MAC address filter.
MAC Address	This field displays the source MAC address in the MAC address filter.
VID	This field displays the source VLAN ID in the MAC address filter.
Port	This field displays the source port of the discarded ARP packet.
Expiry (sec)	This field displays how long (in seconds) the MAC address filter remains in the OLT. You can also delete the record manually (Delete).
Reason	This field displays the reason the ARP packet was discarded. MAC+VLAN: The MAC address and VLAN ID were not in the binding table. IP: The MAC address and VLAN ID were in the binding table, but the IP address was not valid. Port: The MAC address, VLAN ID, and IP address were in the binding table, but the port number was not valid.
Delete	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Check the entry(ies) that you want to remove and then click Delete to remove the selected entry(ies) from the summary table.
Cancel	Click Cancel to clear the check boxes.
Change Pages	Click Previous Page or Next Page to show the previous/next screen if all status information cannot be seen in one screen.

23.7 ARP Inspection VLAN Status

Use this screen to look at various statistics about ARP packets in each VLAN. To open this screen, click **Advanced Application > IP Source Guard > ARP Inspection > VLAN Status**.

Figure 119 Advanced Application > IP Source Guard > ARP Inspection > VLAN Status

VID	Received	Request	Reply	Forwarded	Dropped

The following table describes the labels in this screen.

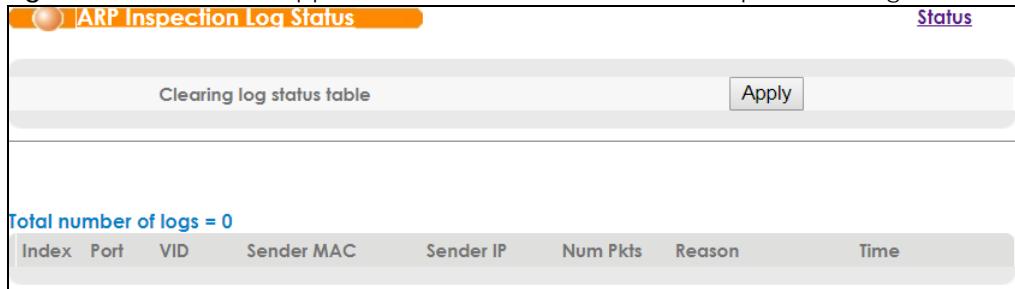
Table 73 Advanced Application > IP Source Guard > ARP Inspection > VLAN Status

LABEL	DESCRIPTION
Show VLAN range	Use this section to specify the VLANs you want to look at in the section below.
Enabled VLAN	Select this to look at all the VLANs on which ARP inspection is enabled in the section below.
Selected VLAN	Select this to look at all the VLANs in a specific range in the section below. Then, enter the lowest VLAN ID (Start VID) and the highest VLAN ID (End VID) you want to look at.
Apply	Click this to display the specified range of VLANs in the section below.
VID	This field displays the VLAN ID of each VLAN in the range specified above.
Received	This field displays the total number of ARP packets received from the VLAN since the OLT last restarted.
Request	This field displays the total number of ARP Request packets received from the VLAN since the OLT last restarted.
Reply	This field displays the total number of ARP Reply packets received from the VLAN since the OLT last restarted.
Forwarded	This field displays the total number of ARP packets the OLT forwarded for the VLAN since the OLT last restarted.
Dropped	This field displays the total number of ARP packets the OLT discarded for the VLAN since the OLT last restarted.

23.8 ARP Inspection Log Status

Use this screen to look at log messages that were generated by ARP packets and that have not been sent to the syslog server yet. To open this screen, click **Advanced Application > IP Source Guard > ARP Inspection > Log Status**.

Figure 120 Advanced Application > IP Source Guard > ARP Inspection > Log Status



The following table describes the labels in this screen.

Table 74 Advanced Application > IP Source Guard > ARP Inspection > Log Status

LABEL	DESCRIPTION
Clearing log status table	Click Apply to remove all the log messages that were generated by ARP packets and that have not been sent to the syslog server yet.
Total number of logs	This field displays the number of log messages that were generated by ARP packets and that have not been sent to the syslog server yet. If one or more log messages are dropped due to unavailable buffer, there is an entry called overflow with the current number of dropped log messages.
Index	This field displays a sequential number for each log message.
Port	This field displays the source port of the ARP packet.
VID	This field displays the source VLAN ID of the ARP packet.
Sender MAC	This field displays the source MAC address of the ARP packet.
Sender IP	This field displays the source IP address of the ARP packet.
Num Pkts	This field displays the number of ARP packets that were consolidated into this log message. The OLT consolidates identical log messages generated by ARP packets in the log consolidation interval into one log message. You can configure this interval in the ARP Inspection Configure screen. See Section 23.9 on page 205 .
Reason	<p>This field displays the reason the log message was generated.</p> <p>dhcp deny: An ARP packet was discarded because it violated a dynamic binding with the same MAC address and VLAN ID.</p> <p>static deny: An ARP packet was discarded because it violated a static binding with the same MAC address and VLAN ID.</p> <p>deny: An ARP packet was discarded because there were no bindings with the same MAC address and VLAN ID.</p> <p>dhcp permit: An ARP packet was forwarded because it matched a dynamic binding.</p> <p>static permit: An ARP packet was forwarded because it matched a static binding.</p> <p>In the ARP Inspection VLAN Configure screen, you can configure the OLT to generate log messages when ARP packets are discarded or forwarded based on the VLAN ID of the ARP packet. See Section 23.9.2 on page 208.</p>
Time	This field displays when the log message was generated.

23.9 ARP Inspection Configure

Use this screen to enable ARP inspection on the OLT. You can also configure the length of time the OLT stores records of discarded ARP packets and global settings for the ARP inspection log. To open this screen, click **Advanced Application > IP Source Guard > ARP Inspection > Configure**.

Figure 121 Advanced Application > IP Source Guard > ARP Inspection > Configure

The screenshot shows the 'ARP Inspection Configure' screen. At the top, there are three tabs: 'Port', 'VLAN', and 'ARP Inspection'. The 'ARP Inspection' tab is active. Below the tabs, there is a section titled 'Filter Aging Time' with a 'Filter aging time' input field containing '300' and a unit of 'seconds'. Underneath this is a 'Log Profile' section with three rows: 'Log buffer size' (32 entries), 'Syslog rate' (5 entries), and 'Log interval' (1 seconds). At the bottom of the screen are two buttons: 'Apply' and 'Cancel'.

The following table describes the labels in this screen.

Table 75 Advanced Application > IP Source Guard > ARP Inspection > Configure

LABEL	DESCRIPTION
Active	Select this to enable ARP inspection on the OLT. You still have to enable ARP inspection on specific VLAN and specify trusted ports.
Filter Aging Time	
Filter aging time	This setting has no effect on existing MAC address filters. Enter how long (1-2147483647 seconds) the MAC address filter remains in the OLT after the OLT identifies an unauthorized ARP packet. The OLT automatically deletes the MAC address filter afterwards. Enter 0 if you want the MAC address filter to be permanent.
Log Profile	
Log buffer size	Enter the maximum number (1-1024) of log messages that were generated by ARP packets and have not been sent to the syslog server yet. Make sure this number is appropriate for the specified Syslog rate and Log interval . If the number of log messages in the OLT exceeds this number, the OLT stops recording log messages and simply starts counting the number of entries that were dropped due to unavailable buffer. Click Clearing log status table in the ARP Inspection Log Status screen to clear the log and reset this counter. See Section 23.8 on page 204 .
Syslog rate	Enter the maximum number of syslog messages the OLT can send to the syslog server in one batch. This number is expressed as a rate because the batch frequency is determined by the Log Interval . You must configure the syslog server (Chapter 48 on page 464) to use this. Enter 0 if you do not want the OLT to send log messages generated by ARP packets to the syslog server. The relationship between Syslog rate and Log interval is illustrated in the following examples: <ul style="list-style-type: none"> • 4 invalid ARP packets per second, Syslog rate is 5, Log interval is 1: the OLT sends 4 syslog messages every second. • 6 invalid ARP packets per second, Syslog rate is 5, Log interval is 2: the OLT sends 5 syslog messages every 2 seconds.
Log interval	Enter how often (1-86400 seconds) the OLT sends a batch of syslog messages to the syslog server. Enter 0 if you want the OLT to send syslog messages immediately. See Syslog rate for an example of the relationship between Syslog rate and Log interval .

Table 75 Advanced Application > IP Source Guard > ARP Inspection > Configure (continued)

LABEL	DESCRIPTION
Apply	Click Apply to save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values in this screen to their last-saved values.

23.9.1 ARP Inspection Port Configure

Use this screen to specify whether ports are trusted or untrusted ports for ARP inspection. You can also specify the maximum rate at which the OLT receives ARP packets on each untrusted port. To open this screen, click **Advanced Application > IP Source Guard > ARP Inspection > Configure > Port**.

Figure 122 Advanced Application > IP Source Guard > ARP Inspection > Configure > Port

Port	Trusted State	Limit	
		Rate (pps)	Burst interval (seconds)
*	Untrusted ▾	15	1
1	Untrusted ▾	15	1
2	Untrusted ▾	15	1
3	Untrusted ▾	15	1
4	Untrusted ▾	15	1
5	Untrusted ▾	15	1
6	Untrusted ▾	15	1
7	Untrusted ▾	15	1
17	Untrusted ▾	15	1
18	Untrusted ▾	15	1
19	Untrusted ▾	15	1
20	Untrusted ▾	15	1
21	Untrusted ▾	15	1
22	Untrusted ▾	15	1
23	Untrusted ▾	15	1
24	Untrusted ▾	15	1

Apply **Cancel**

The following table describes the labels in this screen.

Table 76 Advanced Application > IP Source Guard > ARP Inspection > Configure > Port

LABEL	DESCRIPTION
Port	This field displays the port number. If you configure the * port, the settings are applied to all of the ports.
*	<p>Settings in this row apply to all ports.</p> <p>Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis.</p> <p>Note: Changes in this row are copied to all the ports as soon as you make them.</p>

Table 76 Advanced Application > IP Source Guard > ARP Inspection > Configure > Port (continued)

LABEL	DESCRIPTION
Trusted State	Select whether this port is a trusted port (Trusted) or an untrusted port (Untrusted). The OLT does not discard ARP packets on trusted ports for any reason. The OLT discards ARP packets on untrusted ports in the following situations: <ul style="list-style-type: none"> • The sender's information in the ARP packet does not match any of the current bindings. • The rate at which ARP packets arrive is too high. You can specify the maximum rate at which ARP packets can arrive on untrusted ports.
Limit	These settings have no effect on trusted ports.
Rate (pps)	Specify the maximum rate (1-2048 packets per second) at which the OLT receives ARP packets from each port. The OLT discards any additional ARP packets. Enter 0 to disable this limit.
Burst interval (seconds)	The burst interval is the length of time over which the rate of ARP packets is monitored for each port. For example, if the rate is 15 pps and the burst interval is 1 second, then the OLT accepts a maximum of 15 ARP packets in every one-second interval. If the burst interval is 5 seconds, then the OLT accepts a maximum of 75 ARP packets in every five-second interval. Enter the length (1-15 seconds) of the burst interval.
Apply	Click Apply to save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values in this screen to their last-saved values.

23.9.2 ARP Inspection VLAN Configure

Use this screen to enable ARP inspection on each VLAN and to specify when the OLT generates log messages for receiving ARP packets from each VLAN. To open this screen, click **Advanced Application > IP Source Guard > ARP Inspection > Configure > VLAN**.

Figure 123 Advanced Application > IP Source Guard > ARP Inspection > Configure > VLAN

VLAN	Start VID	End VID
*	No	None

The following table describes the labels in this screen.

Table 77 Advanced Application > IP Source Guard > ARP Inspection > Configure > VLAN

LABEL	DESCRIPTION
VLAN	Use this section to specify the VLANs you want to manage in the section below.
Start VID	Enter the lowest VLAN ID you want to manage in the section below.

Table 77 Advanced Application > IP Source Guard > ARP Inspection > Configure > VLAN (continued)

LABEL	DESCRIPTION
End VID	Enter the highest VLAN ID you want to manage in the section below.
Apply	Click this to display the specified range of VLANs in the section below.
VID	This field displays the VLAN ID of each VLAN in the range specified above. If you configure the * VLAN, the settings are applied to all VLANs.
Enabled	Select Yes to enable ARP inspection on the VLAN. Select No to disable ARP inspection on the VLAN.
Log	Specify when the OLT generates log messages for receiving ARP packets from the VLAN. None: The OLT does not generate any log messages when it receives an ARP packet from the VLAN. Deny: The OLT generates log messages when it discards an ARP packet from the VLAN. Permit: The OLT generates log messages when it forwards an ARP packet from the VLAN. All: The OLT generates log messages every time it receives an ARP packet from the VLAN.
Apply	Click Apply to save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values in this screen to their last-saved values.

23.10 Technical Reference

This section provides technical background information on the topics discussed in this chapter.

23.10.1 DHCP Snooping Overview

Use DHCP snooping to filter unauthorized DHCP packets on the network and to build the binding table dynamically. This can prevent clients from getting IP addresses from unauthorized DHCP servers.

23.10.1.1 Trusted vs. Untrusted Ports

Every port is either a trusted port or an untrusted port for DHCP snooping. This setting is independent of the trusted/untrusted setting for ARP inspection. You can also specify the maximum number for DHCP packets that each port (trusted or untrusted) can receive each second.

Trusted ports are connected to DHCP servers or other switches. The OLT discards DHCP packets from trusted ports only if the rate at which DHCP packets arrive is too high. The OLT learns dynamic bindings from trusted ports.

Note: If DHCP is enabled and there are no trusted ports, DHCP requests will not succeed.

Untrusted ports are connected to subscribers. The OLT discards DHCP packets from untrusted ports in the following situations:

- The packet is a DHCP server packet (for example, OFFER, ACK, or NACK).
- The source MAC address and source IP address in the packet do not match any of the current bindings.

- The packet is a RELEASE or DECLINE packet, and the source MAC address and source port do not match any of the current bindings.
- The rate at which DHCP packets arrive is too high.

23.10.1.2 DHCP Snooping Database

The OLT stores the binding table in volatile memory. If the OLT restarts, it loads static bindings from permanent memory but loses the dynamic bindings, in which case the devices in the network have to send DHCP requests again. As a result, it is recommended you configure the DHCP snooping database.

The DHCP snooping database maintains the dynamic bindings for DHCP snooping and ARP inspection in a file on an external TFTP server. If you set up the DHCP snooping database, the OLT can reload the dynamic bindings from the DHCP snooping database after the OLT restarts.

You can configure the name and location of the file on the external TFTP server. The file has the following format:

Figure 124 DHCP Snooping Database File Format

```
<initial-checksum>
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
<binding-1> <checksum-1>
<binding-2> <checksum-1-2>
...
...
<binding-n> <checksum-1-2-...-n>
END
```

The <initial-checksum> helps distinguish between the bindings in the latest update and the bindings from previous updates. Each binding consists of 72 bytes, a space, and another checksum that is used to validate the binding when it is read. If the calculated checksum is not equal to the checksum in the file, that binding and all others after it are ignored.

23.10.1.3 DHCP Relay Option 82 Information

The OLT can add information to DHCP requests that it does not discard. This provides the DHCP server more information about the source of the requests. The OLT can add the following information:

- Slot ID (1 byte), port ID (1 byte), and source VLAN ID (2 bytes)
- System name (up to 32 bytes)

This information is stored in an Agent Information field in the option 82 field of the DHCP headers of client DHCP request frames. See [Chapter 36 on page 288](#) for more information about DHCP relay option 82.

When the DHCP server responds, the OLT removes the information in the Agent Information field before forwarding the response to the original source.

You can configure this setting for each source VLAN. This setting is independent of the DHCP relay settings ([Chapter 36 on page 288](#)).

23.10.1.4 DHCP Option 82 Settings Configuration Order

Here's the configuration order for DHCP option 82 settings in different screens.

System's Option Information

Go to the following screen to set up the option 82 Circuit ID and Remote ID information for the OLT.

- 1 **IP Application > DHCP > Option (Option 82 Circuit Id)**
- 2 **IP Application > DHCP > Option (Option 82 Remote Id)**

System's Format

Go to the following screens to apply the default Circuit ID format globally on the OLT or to the specified VLAN domain of the DHCP clients.

- 1 **IP Application > DHCP > VLAN (Format)**
- 2 **IP Application > DHCP > Global (Format)**

System's Option & Information

Go to the following screens to have the OLT add the Circuit ID sub-option, Remote ID sub-option, and system name globally or in the specified VLAN.

- 1 **IP Application > DHCP > VLAN (Relay Agent Information Option 82)**
- 2 **IP Application > DHCP > VLAN (Information)**
- 3 **IP Application > DHCP > Global (Relay Agent Information Option 82)**
- 4 **IP Application > DHCP > Global (Information)**
- 5 **Advanced Application > IP Source Guard > DHCP Snooping > Configure > VLAN (Option82)**
- 6 **Advanced Application > IP Source Guard > DHCP Snooping > Configure > VLAN (Information)**

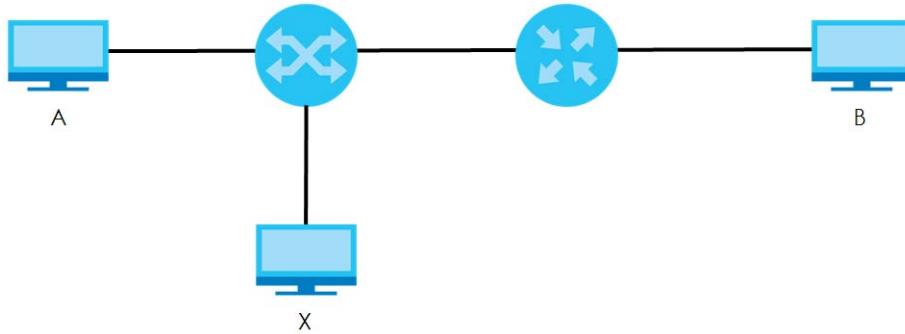
23.10.1.5 Configuring DHCP Snooping

Follow these steps to configure DHCP snooping on the OLT.

- 1 Enable DHCP snooping on the OLT.
- 2 Enable DHCP snooping on each VLAN, and configure DHCP relay option 82.
- 3 Configure trusted and untrusted ports, and specify the maximum number of DHCP packets that each port can receive per second.
- 4 Configure static bindings.

23.10.2 ARP Inspection Overview

Use ARP inspection to filter unauthorized ARP packets on the network. This can prevent many kinds of man-in-the-middle attacks, such as the one in the following example.

Figure 125 Example: Man-in-the-middle Attack

In this example, computer **B** tries to establish a connection with computer **A**. Computer **X** is in the same broadcast domain as computer **A** and intercepts the ARP request for computer **A**. Then, computer **X** does the following things:

- It pretends to be computer **A** and responds to computer **B**.
- It pretends to be computer **B** and sends a message to computer **A**.

As a result, all the communication between computer **A** and computer **B** passes through computer **X**. Computer **X** can read and alter the information passed between them.

23.10.2.1 ARP Inspection

When the OLT identifies an unauthorized ARP packet, it will drop the unauthorized ARP packet.

23.10.2.2 Trusted vs. Untrusted Ports

Every port is either a trusted port or an untrusted port for ARP inspection. This setting is independent of the trusted/untrusted setting for DHCP snooping. You can also specify the maximum rate at which the OLT receives ARP packets on untrusted ports.

The OLT does not discard ARP packets on trusted ports for any reason.

The OLT discards ARP packets on untrusted ports in the following situations:

- The sender's information in the ARP packet does not match any of the current bindings.
- The rate at which ARP packets arrive is too high.

23.10.2.3 Syslog

The OLT can send syslog messages to the specified syslog server ([Chapter 48 on page 464](#)) when it forwards or discards ARP packets. The OLT can consolidate log messages and send log messages in batches to make this mechanism more efficient.

23.10.2.4 Configuring ARP Inspection

Follow these steps to configure ARP inspection on the OLT.

- 1 Configure DHCP snooping. See [Section 23.10.1.5 on page 211](#).

Note: It is recommended you enable DHCP snooping at least one day before you enable ARP inspection so that the OLT has enough time to build the binding table.

- 2** Enable ARP inspection on each VLAN.
- 3** Configure trusted and untrusted ports, and specify the maximum number of ARP packets that each port can receive per second.

CHAPTER 24

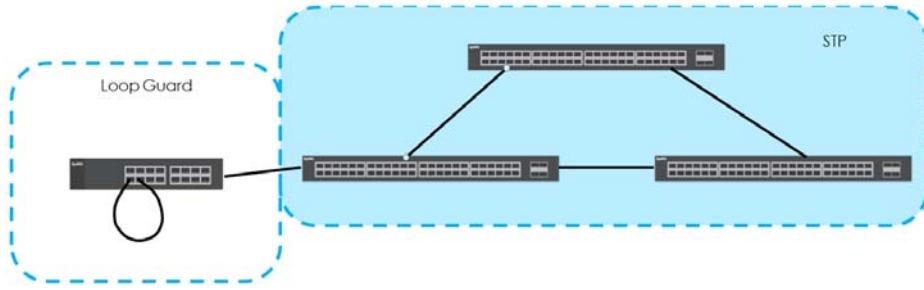
Loop Guard

24.1 Loop Guard Overview

This chapter shows you how to configure the OLT to guard against loops on the edge of your network.

Loop guard allows you to configure the OLT to shut down a port if it detects that packets sent out on that port loop back to the OLT. 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 126 Loop Guard vs. STP



Refer to [Section 24.1.2 on page 214](#) for more information.

24.1.1 What You Can Do

Use the **Loop Guard** screen ([Section 24.2 on page 215](#)) to enable loop guard on the **Switch** OLT and in specific ports.

24.1.2 What You Need to Know

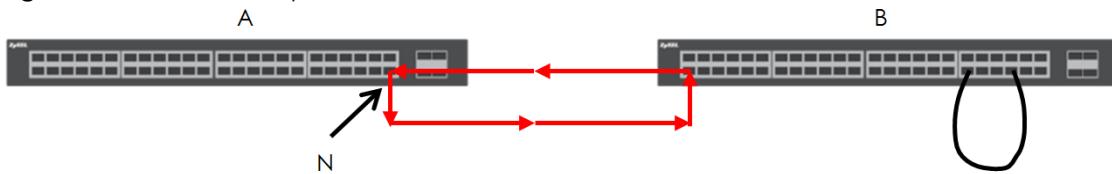
Loop guard is designed to handle loop problems on the edge of your network. This can occur when a port is connected to a OLT that is in a loop state. Loop state occurs as a result of human error. It happens when two ports on a switch are connected with the same cable. When a switch in loop state sends 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 switch **A** connected to switch **B**. Switch **B** is in loop state. When broadcast or multicast packets leave port **N** and reach switch **B**, they are sent back to port **N** on **A** as they are rebroadcast from **B**.

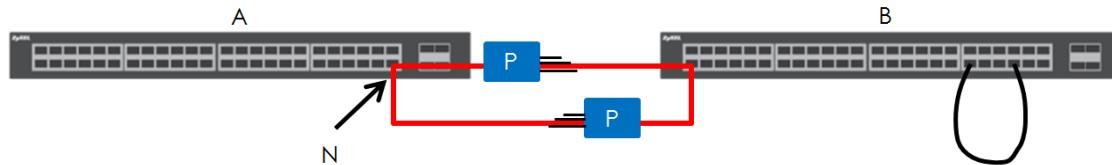
Figure 127 Switch in Loop State



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 OLT will shut down the port connected to the switch in loop state.

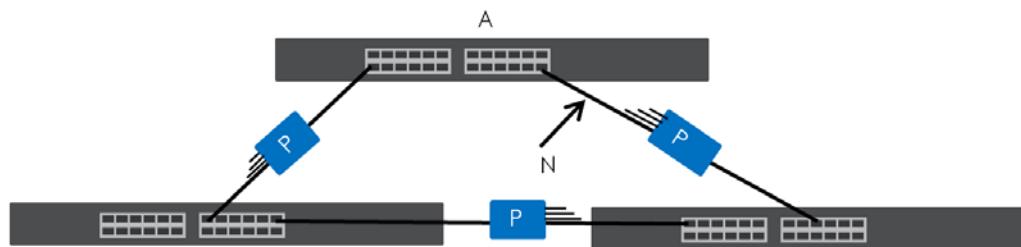
The following figure shows a loop guard enabled port **N** on switch **A** sending a probe packet **P** to switch **B**. Since switch **B** is in loop state, the probe packet **P** returns to port **N** on **A**. The OLT then shuts down port **N** to ensure that the rest of the network is not affected by the switch in loop state.

Figure 128 Loop Guard - Probe Packet



The OLT also shuts down port **N** if the probe packet returns to switch **A** on any other port. In other words loop guard also protects against standard network loops. The following figure illustrates three switches forming a loop. A sample path of the loop guard probe packet is also shown. In this example, the probe packet is sent from port **N** and returns on another port. As long as loop guard is enabled on port **N**. The OLT will shut down port **N** if it detects that the probe packet has returned to the OLT.

Figure 129 Loop Guard - Network Loop



Note: After resolving the loop problem on your network you can re-activate the disabled port via the web configurator (see [Section 8.7 on page 92](#)).

24.2 Loop Guard Setup

Click **Advanced Application > Loop Guard** in the navigation panel to display the screen as shown.

Note: The loop guard feature can not be enabled on the ports that have Spanning Tree Protocol (RSTP or MSTP) enabled.

Figure 130 Advanced Application > Loop Guard

Port	Active
*	<input checked="" type="checkbox"/>
1	<input checked="" type="checkbox"/>
2	<input checked="" type="checkbox"/>
3	<input checked="" type="checkbox"/>
4	<input checked="" type="checkbox"/>
5	<input checked="" type="checkbox"/>
6	<input checked="" type="checkbox"/>
7	<input checked="" type="checkbox"/>
8	<input checked="" type="checkbox"/>
9	<input checked="" type="checkbox"/>
10	<input checked="" type="checkbox"/>
11	<input checked="" type="checkbox"/>
12	<input checked="" type="checkbox"/>
13	<input checked="" type="checkbox"/>
14	<input checked="" type="checkbox"/>
15	<input checked="" type="checkbox"/>
16	<input checked="" type="checkbox"/>
17	<input checked="" type="checkbox"/>
18	<input checked="" type="checkbox"/>
19	<input checked="" type="checkbox"/>
20	<input checked="" type="checkbox"/>
21	<input checked="" type="checkbox"/>
22	<input checked="" type="checkbox"/>
23	<input checked="" type="checkbox"/>
24	<input checked="" type="checkbox"/>

Apply **Cancel**

The following table describes the labels in this screen.

Table 78 Advanced Application > Loop Guard

LABEL	DESCRIPTION
Active	Select this option to enable loop guard on the OLT. The OLT generates syslog, internal log messages as well as SNMP traps when it shuts down a port via the loop guard feature.
Port	This field displays the port number. * means all ports.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to enable the loop guard feature on this port. The OLT sends probe packets from this port to check if the switch it is connected to is in loop state. If the switch that this port is connected is in loop state the OLT will shut down this port. Clear this check box to disable the loop guard feature.

Table 78 Advanced Application > Loop Guard (continued)

LABEL	DESCRIPTION
Apply	Click Apply to save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

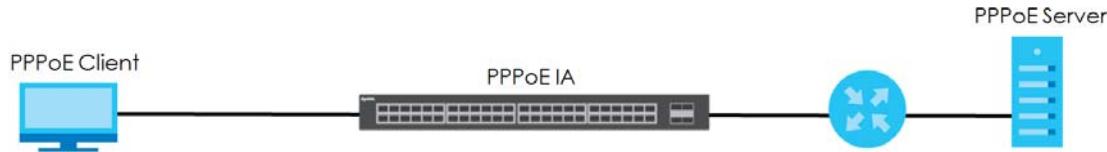
CHAPTER 25

PPPoE

25.1 PPPoE Intermediate Agent Overview

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

A PPPoE Intermediate Agent (PPPoE IA) is deployed between a PPPoE server and PPPoE clients. It helps the PPPoE server identify and authenticate clients by adding subscriber line specific information to PPPoE discovery packets from clients on a per-port or per-port-per-VLAN basis before forwarding them to the PPPoE server.



25.1.1 What You Can Do

- Use the **PPPoE** screen ([Section 25.2 on page 220](#)) to display the main PPPoE screen.
- Use the **Intermediate Agent** screen ([Section 25.3 on page 220](#)) to enable the PPPoE Intermediate Agent on the OLT.
- Use the **PPPoE IA Per-Port** screen ([Section 25.3.1 on page 222](#)) to set the port state and configure PPPoE intermediate agent sub-options on a per-port basis.
- Use the **PPPoE IA for VLAN** ([Section 25.3.2 on page 224](#)) to enable the PPPoE Intermediate Agent on a VLAN.
- Use the **PPPoE IA for ONT PPPoE Option** ([Section 25.3.3 on page 225](#)) to configure whether to have the OLT add PPPoE options for outgoing packets, and forward packets with PPPoE options.
- Use the **Static** screen ([Section 25.3.4 on page 226](#)) to view the PPPoE discovery packets status on the VLAN groups with the PPPoE Intermediate Agent enabled.

25.1.2 What You Need to Know

Read on for concepts on ARP that can help you configure the screen in this chapter.

25.1.2.1 PPPoE Intermediate Agent Tag Format

If the PPPoE Intermediate Agent is enabled, the OLT 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 79 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 0x000000DE9, 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.

25.1.2.2 Sub-Option Format

There are two types of sub-option: "Agent Circuit ID Sub-option" and "Agent Remote ID Sub-option". They have the following formats.

Table 80 PPPoE IA Circuit ID Sub-option Format: User-defined String

SubOpt	Length	Value
0x01 (1 byte)	N (1 byte)	String

Table 81 PPPoE IA Remote ID Sub-option Format: User-defined String

SubOpt	Length	Value
0x02 (1 byte)	N (1 byte)	String

The 1 in the first field identifies this as an Agent Circuit ID sub-option and 2 identifies this as an Agent Remote ID sub-option. The next field specifies the length of the field. Port State

Every port is either a trusted port or an untrusted port for the PPPoE intermediate agent. This setting is independent of the trusted/untrusted setting for DHCP snooping or ARP inspection. You can also specify the agent sub-options (Circuit ID and Remote ID) that the OLT adds to PADI and PADR packets from PPPoE clients.

Trusted ports are connected to PPPoE servers.

- If a PADO (PPPoE Active Discovery Offer), PADS (PPPoE Active Discovery Session-confirmation), or PADT (PPPoE Active Discovery Terminate) packet is sent from a PPPoE server and received on a trusted port, the OLT forwards it to all other ports.
- If a PADI or PADR packet is sent from a PPPoE client but received on a trusted port, the OLT forwards it to other trusted port(s).

Note: The OLT will drop all PPPoE discovery packets if you enable the PPPoE intermediate agent and there are no trusted ports.

Untrusted ports are connected to subscribers.

- If a PADI, PADR, or PADT packet is sent from a PPPoE client and received on an untrusted port, the OLT adds a vendor-specific tag to the packet and then forwards it to the trusted port(s).

- The OLT discards PADO and PADS packets which are sent from a PPPoE server but received on an untrusted port.

25.2 PPPoE Screen

Use this screen to configure the PPPoE Intermediate Agent on the OLT.

Click **Advanced Application > PPPoE** in the navigation panel to display the screen as shown. Click [Click Here](#) to go to the **Intermediate Agent** screen.

Figure 131 Advanced Application > PPPoE Intermediate Agent



25.3 PPPoE Intermediate Agent

Use this screen to configure the OLT to give a PPPoE termination server additional subscriber information that the server can use to identify and authenticate a PPPoE client.

Click **Advanced Application > PPPoE > Intermediate Agent** in the navigation panel to display the screen as shown.

Figure 132 Advanced Application > PPPoE > Intermediate Agent

 A screenshot of the 'Intermediate Agent' configuration screen. At the top, there's a header with tabs: 'Port', 'VLAN', 'Ont Option', and 'Intermediate Agent' (which is highlighted in blue). Below the header, there's a section labeled 'option' containing three input fields: 'VID' (with a dropdown arrow), 'Option Circuit Id' (with a dropdown arrow), and 'Option Remote Id' (with a dropdown arrow). Below these fields are three buttons: 'Add', 'Cancel', and 'Clear'. Further down, there's a table with columns: VID, Option CircuitId, Option RemoteId, and Delete. The first row of the table has entries: VID (dropdown arrow), Option CircuitId (dropdown arrow), Option RemoteId (dropdown arrow), and Delete (button). At the bottom of the table are two buttons: 'Delete' and 'Cancel'.

The following table describes the labels in this screen.

Table 82 Advanced Application > PPPoE > Intermediate Agent

LABEL	DESCRIPTION
Active	Select this option to enable the PPPoE intermediate agent globally on the OLT.
Apply	Click Apply to save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Option	
VID	Enter the VLAN ID number to which you want the settings configured here to apply.
Option Circuit Id	<p>Enter a string of up to 127 ASCII characters that the OLT adds into the Agent Circuit ID sub-option for PPPoE discovery packets received in the VLAN group. Spaces are allowed. This string should be composed of the following special characters. The special characters listed in the brackets [~`!@#\$^&*()] are not allowed except % and space.</p> <ul style="list-style-type: none"> • %%: character % • %space: character space • %mac: client source mac • %hname: host device name • %pid: pon port index • %oid: ONT index • %ocid: ONT card index • %upid: uniport index • %nnisvlan: SVLAN ID on network-network interface • %snisvlan: SVLAN ID on service-network interface • %snicvlan: CVLAN ID on service-network interface • %sn: serial number of a remote ONT • %ontname: will be translated into ONT model name • %ontdesc: will be translated into ONT description • %ontpasswd: will be translated into ONT password <p>Note: If the string is composed of more than 127 characters, the string will be truncated to the maximum number of characters allowed when the OLT transforms the string into the Circuit ID.</p>

Table 82 Advanced Application > PPPoE > Intermediate Agent (continued)

LABEL	DESCRIPTION
Option Remote Id	<p>Enter a string of up to 95 ASCII characters that the OLT adds into the Agent Remote ID sub-option for PPPoE discovery packets received in the VLAN group. Spaces are allowed. This string should be composed of the following special characters. The special characters listed in the brackets [~`@#\$^&*()] are not allowed except % and space.</p> <ul style="list-style-type: none"> • %%: character % • %space: character space • %mac: client source mac • %hname: host device name • %pid: pon port index • %oid: ONT index • %ocid: ONT card index • %upid: uniport index • %nnisvlan: SVLAN ID on network-network interface • %snisvlan: SVLAN ID on service-network interface • %snicvlan: CVLAN ID on service-network interface • %sn: serial number of a remote ONT • %ontname: will be translated into ONT model name • %ontdesc: will be translated into ONT description • %ontpasswd: will be translated into ONT password <p>Note: If the string is composed of more than 95 characters, the string will be truncated to the maximum number of characters allowed when the OLT transforms the string into the Remote ID.</p>
Add	<p>Click this to create a new entry or to update an existing one.</p> <p>This saves your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.</p>
Cancel	Click Cancel to reset the fields to your previous configuration.
Clear	Click Clear to reset the fields to the factory defaults.
VID	This field displays the VLAN ID number.
Option CircuitId	This field displays the Circuit ID information that is added in the PPPoE discovery packets.
Option Remoteld	This field displays the Remote ID information that is added in the PPPoE discovery packets.
Delete	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to begin configuring this screen afresh.

25.3.1 PPPoE IA Per-Port

Use this screen to specify whether individual ports are trusted or untrusted ports and have the OLT add extra information to PPPoE discovery packets from PPPoE clients on a per-port basis.

Note: The OLT will drop all PPPoE packets if you enable the PPPoE Intermediate Agent on the OLT and there are no trusted ports.

Click the **Port** link in the **Intermediate Agent** screen to display the screen as shown.

Figure 133 Advanced Application > PPPoE > Intermediate Agent > Port

Port	Server Trusted State
*	Untrusted ▾
1	Untrusted ▾
2	Untrusted ▾
3	Untrusted ▾
4	Untrusted ▾
5	Untrusted ▾
6	Untrusted ▾
7	Untrusted ▾
8	Untrusted ▾
9	Untrusted ▾
10	Untrusted ▾
11	Untrusted ▾
12	Untrusted ▾
13	Untrusted ▾
14	Untrusted ▾
15	Untrusted ▾
16	Untrusted ▾
17	Untrusted ▾
18	Untrusted ▾
19	Untrusted ▾
20	Untrusted ▾
21	Untrusted ▾
22	Untrusted ▾
23	Untrusted ▾
24	Untrusted ▾

Apply **Cancel**

The following table describes the labels in this screen.

Table 83 Advanced Application > PPPoE > Intermediate Agent > Port

LABEL	DESCRIPTION
Port	This field displays the port number. * means all ports.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments on a port-by-port basis. Changes in this row are copied to all the ports as soon as you make them.

Table 83 Advanced Application > PPPoE > Intermediate Agent > Port (continued)

LABEL	DESCRIPTION
Server Trusted State	Select whether this port is a trusted port (Trusted) or an untrusted port (Untrusted). Trusted ports are uplink ports connected to PPPoE servers. If a PADO (PPPoE Active Discovery Offer), PADS (PPPoE Active Discovery Session-confirmation), or PADT (PPPoE Active Discovery Terminate) packet is sent from a PPPoE server and received on a trusted port, the OLT forwards it to all other ports. If a PADI or PADR packet is sent from a PPPoE client but received on a trusted port, the OLT forwards it to other trusted port(s). Untrusted ports are downlink ports connected to subscribers. If a PADI, PADR, or PADT packet is sent from a PPPoE client and received on an untrusted port, the OLT adds a vendor-specific tag to the packet and then forwards it to the trusted port(s). The OLT discards PADO and PADS packets which are sent from a PPPoE server but received on an untrusted port.
Apply	Click Apply to save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

25.3.2 PPPoE IA for VLAN

Use this screen to set whether the PPPoE Intermediate Agent is enabled on a VLAN and whether the OLT appends the Circuit ID and/or Remote ID to PPPoE discovery packets from a specific VLAN.

Click the **VLAN** link in the **Intermediate Agent** screen to display the screen as shown.

Figure 134 Advanced Application > PPPoE > Intermediate Agent > VLAN

VID	Enabled	Circuit-id	Remote-id
*	No	<input type="checkbox"/>	<input type="checkbox"/>

The following table describes the labels in this screen.

Table 84 Advanced Application > PPPoE > Intermediate Agent > VLAN

LABEL	DESCRIPTION
Show VLAN	Use this section to specify the VLANs you want to configure in the section below.
Start VID	Enter the lowest VLAN ID you want to configure in the section below.
End VID	Enter the highest VLAN ID you want to configure in the section below.
Apply	Click Apply to display the specified range of VLANs in the section below.
VID	This field displays the VLAN ID of each VLAN in the range specified above. If you configure the * VLAN, the settings are applied to all VLANs.

Table 84 Advanced Application > PPPoE > Intermediate Agent > VLAN (continued)

LABEL	DESCRIPTION
*	Use this row to make the setting the same for all VLANs. Use this row first and then make adjustments on a VLAN-by-VLAN basis. Changes in this row are copied to all the VLANs as soon as you make them.
Enabled	Select this option to turn on the PPPoE Intermediate Agent on a VLAN.
Circuit-id	Select this option to make the Circuit ID settings for a specific VLAN take effect.
Remote-id	Select this option to make the Remote ID settings for a specific VLAN take effect.
Apply	Click Apply to save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

25.3.3 PPPoE IA for ONT PPPoE Option

Use this screen to have:

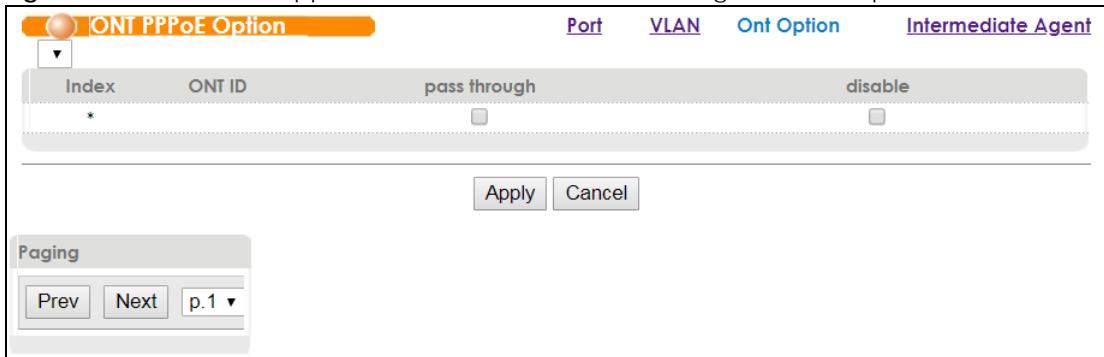
- The OLT adds PPPoE options in the outgoing packets.
- The OLT drops/forwards the incoming packets with PPPoE options from an ONT.

See [Table 85 on page 225](#) for more information.

Table 85 PPPoE Options

PPPOE GLOBAL	PPPOE OPTION	PPPOE PASS THROUGH	ACTION
Disabled	Disabled/Enabled	Disabled	<ul style="list-style-type: none"> The OLT won't add PPPoE options in the outgoing packets. The OLT drops the incoming packets with PPPoE options from an ONT
Disabled	Disabled/Enabled	Enabled	<ul style="list-style-type: none"> The OLT won't add PPPoE options in the outgoing packets. The OLT forwards the incoming packets with PPPoE options from an ONT
Enabled	Enabled	Disabled	<ul style="list-style-type: none"> The OLT adds PPPoE options in the outgoing packets. The OLT drops the incoming packets with PPPoE options from an ONT
Enabled	Disabled	Disabled	<ul style="list-style-type: none"> The OLT won't add PPPoE options in the outgoing packets. The OLT drops the incoming packets with PPPoE options from an ONT
Enabled	Enabled	Enabled	<ul style="list-style-type: none"> The OLT adds PPPoE options in the outgoing packets. The OLT forwards the incoming packets with PPPoE options from an ONT
Enabled	Disabled	Enabled	<ul style="list-style-type: none"> The OLT won't add PPPoE options in the outgoing packets. The OLT forwards the incoming packets with PPPoE options from an ONT
<p>Note: Enable or disable the PPPoE intermediate agent globally on the OLT in the Advanced Application > PPPoE > Intermediate Agent screen.</p>			

Click the **ONT Option** link in the **Intermediate Agent** screen to display the screen as shown.

Figure 135 Advanced Application > PPPoE > Intermediate Agent > ONT Option

The following table describes the labels in this screen.

Table 86 Advanced Application > PPPoE > Intermediate Agent > ONT Option

LABEL	DESCRIPTION
	Choose the GPON interface that you want the settings configured here to apply to from the drop-down list.
Index	This is the index number of the ONT connected to the GPON interface.
ONT ID	This is the identifier of an ONT. Note: When register method D or E is selected and activated in the Advanced Application > OLT Registration screen, ONT ID 121-128 are the ONT template IDs.
pass through	Select this to forward packets with PPPoE options from an ONT. Otherwise, they'll be dropped. Note: When ONT ID 121-128 are the ONT template IDs, the setting for this field applies to the Advanced Application > ONT Template screen.
disable	Deselect this to add PPPoE options in outgoing packets. You can set up PPPoE options in the Advanced Application > PPPoE > Intermediate Agent screen. Note: When ONT ID 121-128 are the ONT template IDs, the setting for this field applies to the Advanced Application > ONT Template screen.
Apply	Click Apply to save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Paging	
Prev/Next	Click Prev or Next to show the previous/next screen if all status information cannot be seen in one screen.

25.3.4 PPPoE IA Statistic

Use this screen to see the PPPoE discovery packets that are sent and received on the VLAN groups with the PPPoE Intermediate Agent enabled.

By default, you'll see a blank screen. To see the PPPoE discovery packets status:

- 1 Enable the PPPoE Intermediate Agent in the **Advanced Application > PPPoE > Intermediate Agent** screen.

- 2** Enable the PPPoE Intermediate Agent on a VLAN(s) in the **Advanced Application > PPPoE > Intermediate Agent > VLAN** screen.

Click the **Statistic** link in the **Intermediate Agent** screen to display the screen as shown.

Figure 136 Advanced Application > PPPoE > Intermediate Agent > Statistic

		Port	VLAN	Ont Option	Statistic	Intermediate Agent
VLAN	PPPoE discovery packet	Received	Forwarded	Dropped		
3	PADI	0	0	0		
	PADO	0	0	0		
	PADR	0	0	0		
	PADS	0	0	0		
	PADT	0	0	0		
	Malformed packet	0	0	0		
VLAN	PPPoE discovery packet	Received	Forwarded	Dropped		
6	PADI	0	0	0		
	PADO	0	0	0		
	PADR	0	0	0		
	PADS	0	0	0		
	PADT	0	0	0		
	Malformed packet	0	0	0		
VLAN	PPPoE discovery packet	Received	Forwarded	Dropped		
8	PADI	0	0	0		
	PADO	0	0	0		
	PADR	0	0	0		
	PADS	0	0	0		
	PADT	0	0	0		
	Malformed packet	0	0	0		

The following table describes the labels in this screen.

Table 87 Advanced Application > PPPoE > Intermediate Agent > Statistic

LABEL	DESCRIPTION
VLAN	This is the ID of the VLAN group with the PPPoE Intermediate Agent enabled
PPPoE discovery packet	<p>PADI (PPPoE Active Discovery Initiation): A PPPoE client will send a PADI packet to request a PPPoE session.</p> <p>PADO (PPPoE Active Discovery Offer): Available PPPoE servers in the network will reply with a PADO packet after receiving the PADI packet. A PADO packet include the name of the PPPoE server.</p> <p>PADR (PPPoE Active Discovery Request): The PPPoE client will select a PPPoE server according to the received PADO packets, and sends a PADR packet to indicate the PPPoE server needed.</p> <p>PADS (PPPoE Active Discovery Session): After receiving the PADR packet, the selected PPPoE server will send a PADS packet to indicate if it accepts or rejects the PPPoE session requested</p> <p>PADT (PPPoE Active Discovery Terminate): A PADT will be sent either by the PPPoE client or the PPPoE server to terminate the PPPoE session after it's established.</p> <p>Malformed packet: The PPPoE discovery packet received by the PPPoE client or server is malformed. Therefore, it's dropped.</p>
Received	This indicates the number of received PPPoE discovery packets on this VLAN group.
Forwarded	This indicates the number of transmitted packets on this VLAN group.
Dropped	This indicates the number of received packets dropped on this VLAN group.

CHAPTER 26

Error Disable

26.1 Static Routing Overview

This chapter shows you how to configure the rate limit for control packets on a port, and set the OLT to take an action (such as to shut down a port or stop sending packets) on a port when the OLT detects a pre-configured error. It also shows you how to configure the OLT to automatically undo the action after the error is gone.

26.1.1 CPU Protection Overview

Switches exchange protocol control packets in a network to get the latest networking information. If a switch receives large numbers of control packets, such as ARP, BPDU or IGMP packets, which are to be processed by the CPU, the CPU may become overloaded and be unable to handle regular tasks properly.

The CPU protection feature allows you to limit the rate of ARP, BPDU and IGMP packets to be delivered to the CPU on a port. This enhances the CPU efficiency and protects against potential DoS attacks or errors from other network(s). You then can choose to drop control packets that exceed the specified rate limit or disable a port on which the packets are received.

26.1.2 Error-Disable Recovery Overview

Some features, such as loop guard or CPU protection, allow the OLT to shut down a port or discard specific packets on a port when an error is detected on the port. For example, if the OLT detects that packets sent out the port(s) loop back to the OLT, the OLT can shut down the port(s) automatically. After that, you need to enable the port(s) or allow the packets on a port manually via the web configurator. With error-disable recovery, you can set the disabled port(s) to become active or start receiving the packets again after the time interval you specify.

26.1.3 What You Can Do

- Use the **CPU Protection** screen ([Section 26.3 on page 229](#)) to limit the maximum number of control packets (ARP, BPDU and/or IGMP) that the OLT can receive or transmit on a port.
- Use the **Errdisable Detect** screen ([Section 26.4 on page 231](#)) to have the OLT detect whether the control packets exceed the rate limit configured for a port and configure the action to take once the limit is exceeded.
- Use the **Errdisable Recovery** screen ([Section 26.5 on page 231](#)) to set the OLT to automatically undo an action after the error is gone.

26.2 Error Disable Screen

Use this screen to go to the screens where you can configure error disable related settings. Click **Advanced Application > Errdisable** in the navigation panel to open the following screen.

Figure 137 Advanced Application > Errdisable



The following table describes the labels in this screen.

Table 88 Advanced Application > Errdisable

LABEL	DESCRIPTION
CPU protection	Click this link to limit the maximum number of control packets (ARP, BPDU and/or IGMP) that the OLT can receive or transmit on a port.
Errdisable Detect	Click this link to have the OLT detect whether the control packets exceed the rate limit configured for a port and configure the action to take once the limit is exceeded.
Errdisable Recovery	Click this link to set the OLT to automatically undo an action after the error is gone.

26.3 CPU Protection Configuration

Use this screen to limit the maximum number of control packets (ARP, BPDU and/or IGMP) that the OLT can receive or transmit on a port. Click the **Click Here** link next to **CPU protection** in the **Advanced Application > Errdisable** screen to display the screen as shown.

Note: After you configure this screen, make sure you also enable error detection for the specific control packets in the **Advanced Application > Errdisable > Errdisable Detect** screen.

Figure 138 Advanced Application > Errdisable > CPU protection

Port	Rate Limit (pkt/s)
*	
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	0
18	0
19	0
20	0
21	0
22	0
23	0
24	0

Apply **Cancel**

The following table describes the labels in this screen.

Table 89 Advanced Application > Errdisable > CPU protection

LABEL	DESCRIPTION
Reason	Select the type of control packet you want to configure here.
Port	This field displays the port number. * means all ports.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments to each port if necessary. Changes in this row are copied to all the ports as soon as you make them.
Rate Limit (pkt/s)	Enter a number from 0 to 256 to specify how many control packets this port can receive or transmit per second. 0 means no rate limit. You can configure the action that the OLT takes when the limit is exceeded. See Section 26.4 on page 231 for detailed information.
Apply	Click Apply to save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

26.4 Error-Disable Detect Configuration

Use this screen to have the OLT detect whether the control packets exceed the rate limit configured for a port and configure the action to take once the limit is exceeded. Click the **Click Here** link next to Errdisable Detect link in the **Advanced Application > Errdisable** screen to display the screen as shown.

Figure 139 Advanced Application > Errdisable > Errdisable Detect

Cause	Active	Mode
*	<input type="checkbox"/>	inactive-port ▾
ARP	<input type="checkbox"/>	inactive-port ▾
BPDU	<input type="checkbox"/>	inactive-port ▾
IGMP	<input type="checkbox"/>	inactive-port ▾
PPPoE	<input type="checkbox"/>	inactive-port ▾
FTP	<input type="checkbox"/>	inactive-port ▾
ICMP	<input type="checkbox"/>	inactive-port ▾
SNMP	<input type="checkbox"/>	inactive-port ▾

Apply **Cancel**

The following table describes the labels in this screen.

Table 90 Advanced Application > Errdisable > Errdisable Detect

LABEL	DESCRIPTION
Cause	This field displays the types of control packet that may cause CPU overload.
*	Use this row to make the setting the same for all entries. Use this row first and then make adjustments to each entry if necessary. Changes in this row are copied to all the entries as soon as you make them.
Active	Select this option to have the OLT detect if the configured rate limit for a specific control packet is exceeded and take the action selected below.
Mode	Select the action that the OLT takes when the number of control packets exceed the rate limit on a port, set in the Advanced Application > Errdisable > CPU protection screen. <ul style="list-style-type: none"> inactive-port - The OLT disables the port on which the control packets are received. inactive-reason - The OLT drops all the specified control packets (such as BPDU) on the port. rate-limitation - The OLT drops the additional control packets the port(s) has to handle in every one second.
Apply	Click Apply to save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

26.5 Error-Disable Recovery Configuration

Use this screen to configure the OLT to automatically undo an action after the error is gone. Click the **Click Here** link next to **Errdisable Recovery** in the **Advanced Application > Errdisable** screen to display the screen as shown.

Figure 140 Advanced Application > Errdisable > Errdisable Recovery

Reason	Timer Status	Interval
*	<input checked="" type="checkbox"/>	
loopguard	<input checked="" type="checkbox"/>	300
ARP	<input checked="" type="checkbox"/>	300
BPDU	<input checked="" type="checkbox"/>	300
IGMP	<input checked="" type="checkbox"/>	300
PPPoE	<input checked="" type="checkbox"/>	300
FTP	<input checked="" type="checkbox"/>	300
ICMP	<input checked="" type="checkbox"/>	300
SNMP	<input checked="" type="checkbox"/>	300

Apply **Cancel**

The following table describes the labels in this screen.

Table 91 Advanced Application > Errdisable > Errdisable Recovery

LABEL	DESCRIPTION
Active	Select this option to turn on the error-disable recovery function on the OLT.
Reason	This field displays the supported features that allow the OLT to shut down a port or discard packets on a port according to the feature requirements and what action you configure.
*	Use this row to make the setting the same for all entries. Use this row first and then make adjustments to each entry if necessary. Changes in this row are copied to all the entries as soon as you make them.
Timer Status	Select this option to allow the OLT to wait for the specified time interval to activate a port or allow specific packets on a port, after the error was gone. Deselect this option to turn off this rule.
Interval	Enter the number of seconds (from 30 to 2592000) for the time interval.
Apply	Click Apply to save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

CHAPTER 27

ONT VoIP

27.0.1 ONT VoIP Profile

Use the **GPON > ONT VoIP Profile** screens to configure VoIP settings for the subscriber Optical Network Terminal (ONT) devices.

VoIP is the sending of voice signals over 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.

27.0.2 What You Can Do

- Use the **VoIP Common Profile** screen ([Section 27.1 on page 234](#)) to configure general VoIP settings for ONTs.
- Use the **VoIP SIP Profile** screen ([Section 27.2 on page 237](#)) to configure ONT VoIP SIP settings.
- Use the **VoIP Dial Plan Profile** screen ([Section 27.3 on page 240](#)) to create dial plan profiles.

27.0.3 What You Need to Know

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.

SIP Identities

A SIP account uses an identity (Sometimes referred to as a SIP address). A complete SIP identity is called a SIP URI (Uniform Resource Identifier). A SIP account's URI identifies the SIP account in a way similar to the way an e-mail address identifies an e-mail account. The format of a SIP identity is SIP-Number@SIP-Service-Domain.

SIP Number

The SIP number is the part of the SIP URI that comes before the "@" symbol. A SIP number can use letters like in an e-mail address (johndoe@your-ITSP.com for example) or numbers like a telephone number (1122334455@VoIP-provider.com for example).

SIP Service Domain

The SIP service domain of the VoIP service provider is the domain name in a SIP URI. For example, if the SIP address is 1122334455@VoIP-provider.com, then "VoIP-provider.com" is the SIP service domain

27.1 ONT VoIP Common Profile

Use this screen to configure profiles of general VoIP settings for ONTs. Click **Advanced Application > ONT VoIP** in the navigation panel to display the screen as shown.

Figure 141 Advanced Application > ONT VoIP > VoIP Common Profile

Voip-Common-Profile		Voip-Sip-Profile	Voip-Dial-Plan								
Name	<input type="text"/>										
min local port	5060	(1-65535)									
max local port	5060	(1-65535)									
dscp mark	0	(0-63)									
piggyback	<input type="checkbox"/>										
tone	<input type="checkbox"/>										
dtmf	<input type="checkbox"/>										
cas	<input type="checkbox"/>										
jitter target	60	0-5000 milliseconds									
max jitter buffer	135	(0-500)									
pstn protocol	0	(0-999)									
announce type	fas-bus ▾										
echo cancel	<input type="checkbox"/>										
fax mode	<input checked="" type="radio"/> passthru <input type="radio"/> T38										
1st-codec	PCMU ▾										
2nd-codec	PCMU ▾										
3rd-codec	PCMU ▾										
4th-codec	PCMU ▾										
1st-packet-period	20	(10-30)									
2nd-packet-period	20	(10-30)									
3rd-packet-period	20	(10-30)									
4th-packet-period	20	(10-30)									
1st silence	<input type="checkbox"/>										
2nd silence	<input type="checkbox"/>										
3rd silence	<input type="checkbox"/>										
4th silence	<input type="checkbox"/>										
oob dtmf	<input type="checkbox"/>										
signal code	loo-str ▾										
<input type="button" value="Add"/> <input type="button" value="Cancel"/> <input type="button" value="Clear"/>											
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Index</th> <th>Name</th> <th>Rule</th> <th>Delete</th> </tr> </thead> <tbody> <tr> <td>*</td> <td></td> <td></td> <td><input type="checkbox"/></td> </tr> </tbody> </table>				Index	Name	Rule	Delete	*			<input type="checkbox"/>
Index	Name	Rule	Delete								
*			<input type="checkbox"/>								
<input type="button" value="Delete"/> <input type="button" value="Cancel"/>											

The following table describes the labels in this screen.

Table 92 Advanced Application > ONT VoIP > VoIP Common Profile

LABEL	DESCRIPTION
Name	Type the name of the profile.
min local port	Specify a range (1-65535) of RTP ports to use for voice traffic.
max local port	
dscp mark	Specify the Diffserv code point (from 0 to 63) to use for outgoing RTP packets.
piggyback	Select this to turn on RTP piggyback events on or clear it to turn them off.
tone	Select this to turn the handling of tones through RTP tone events according to RFC 4733 on or clear it to turn it off.

Table 92 Advanced Application > ONT VoIP > VoIP Common Profile (continued)

LABEL	DESCRIPTION
dtmf	Select this to enable the handling of DTMF via RTP DTMF events as defined in RFC 4733. Clear it to disable the handling of DTMF via RTP DTMF events as defined in RFC 4733.
cas	Enable or disable handling of DTMF via RTP CAS (Channel Associated Signaling) events as defined in RFC 4733.
jitter target	Set the target value (from 0 to 5000) of the jitter buffer in milliseconds.
max jitter buffer	Set the maximum depth (from 0 to 500) of the jitter buffer in milliseconds.
pstn protocol	Set which variant (from 0 to 999) of POTS signaling to use on the associated UNIs.
announce type	Set the treatment for when a subscriber goes off-hook. <ul style="list-style-type: none"> • silence: Silence • reo-ton: Reorder tone • fas-bus: Fast busy tone • voi-ann: Voice announcement
echo cancel	Enable or disable echo cancellation.
fax mode	Set how to handle faxes. Use passthru to transmit faxes as voice (in-band). Use T38 to transmit faxes as separate packets (out-of-band) according to ITU-T T.38.
1st-4th codec	Specify the audio codecs to tell the remote ONT. The remote ONT must use the same codec as the peer. Here are the options, encoding names, and clock rates (in Hz). See RFC 3551 for more details. <p>PCMU: PCMU, 8000 GSM: GSM, 8000 G723: G.723, 8000 DVI4-8000: DVI4, 8000 DVI4-16000: DVI4, 16000 LPC: LPC, 8000 PCMA: PCMA, 8000 G722: G.722, 8000 L16-2: L16, 2 channels, 44100 L16-1: L16, 1 channels, 44100 QCELP: QCELP, 8000 CN: CN, 8000 MPA: MPA, 90000 G728: G.728, 8000 DVI4-11025: DVI4, 11025 DVI4-22050: DVI4, 22050 G729: G.729, 8000</p>
1st-4th packet period	Specify the packet period selection interval (in milliseconds). This value is useful when the media gateway controller does not provide the preferred compression algorithm and packet period parameter to the ONT. The range depends on the type of codec selected.
1st-4th silence	Turn the use of silence suppression with the 1st-4th codecs on or off.

Table 92 Advanced Application > ONT VoIP > VoIP Common Profile (continued)

LABEL	DESCRIPTION
oob dtmf	Turn out-of-band DTMF carriage on or off.
signal code	Set the signaling code: loo-str: Loop start gro-str: Ground start loo-rev: Loop reverse battery coi-fir: Coin first dia-ton: Dial tone first mul-par: Multi-party
Apply	Click Apply to save the changes.
Cancel	Click Cancel to clear the fields.
Clear	Click Clear to return the screen's settings to the defaults.
Index	This is the index number of an ONT common VoIP profile.
Name	This is the name of the profile.
Rule	This displays the profile's settings.
Delete	Select this for one or more profiles and click Delete to remove them.
Select	Select this to edit the profile in the fields above.
*	Use this row to select all of the profiles for deletion.
Delete	Click Delete to remove the profiles with the Delete option selected.
Cancel	Click Cancel to begin configuring the screen again.

27.2 ONT VoIP SIP Profile

Use this screen to configure profiles of ONT VoIP SIP settings. Click **Voip-Sip-Profile** in the **Advanced Application > ONT VoIP** screen to display the screen as shown.

Figure 142 Advanced Application > ONT VoIP > Voip-Sip-Profile

VoipSipProfile		Voip-Common-Profile	Voip-Dial-Plan	
Name	<input type="text"/>			
proxy service address	<input type="text"/>			
outbound proxy address	<input type="text"/>			
primary dns	<input type="text"/>			
secondary dns	<input type="text"/>			
registration expiration time(sec)	3600	(0-25200)		
re-registerion head start time(sec)	360	(0-720)		
host part uri	<input type="text"/>			
sip registrar	<input type="text"/>			
softswitch	<input type="text"/>			
caller id	<input type="checkbox"/> cal-num	<input type="checkbox"/> cal-nam	<input type="checkbox"/> cid-blo	<input type="checkbox"/> cid-num
	<input type="checkbox"/> cld-nam	<input type="checkbox"/> ACR		
call waiting	<input type="checkbox"/> cal-wai	<input type="checkbox"/> cid-ann		
call progress or transfer	<input type="checkbox"/> 3way	<input type="checkbox"/> cal-tra	<input type="checkbox"/> cal-hol	<input type="checkbox"/> cal-par
	<input type="checkbox"/> not-dis	<input type="checkbox"/> flash	<input type="checkbox"/> origin	<input type="checkbox"/> 6way
call presentation	<input type="checkbox"/> spl-rin	<input type="checkbox"/> dia-ton	<input type="checkbox"/> vis-ind	<input type="checkbox"/> cal-for
direction connect	<input type="checkbox"/> enable	<input type="checkbox"/> dia-opt		
direction connect uri	<input type="text"/>			
bridged line agent uri	<input type="text"/>			
conference factory uri	<input type="text"/>			

<input type="button" value="Add"/>	<input type="button" value="Cancel"/>	<input type="button" value="Clear"/>
------------------------------------	---------------------------------------	--------------------------------------

Index	Name	Rule	Delete
*	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>

<input type="button" value="Delete"/>	<input type="button" value="Cancel"/>
---------------------------------------	---------------------------------------

The following table describes the labels in this screen.

Table 93 Advanced Application > ONT VoIP > Voip-Sip-Profile

LABEL	DESCRIPTION
Name	Type the name of the profile.
proxy service address	Configure the IP address or URI (from 1 to 63 characters) of a proxy service.
outband proxy address	Configure an outband proxy IP address or URI (from 1 to 63 characters).
primary, secondary dns	Configure the IP addresses of the primary and secondary DNS servers for SIP.
registration expiration time	Enter the number of seconds (0-25200) the OLT lets a SIP session remain idle (without traffic) before it automatically disconnects the session.

Table 93 Advanced Application > ONT VoIP > Voip-Sip-Profile (continued)

LABEL	DESCRIPTION
re-registration head start time	Enter the number of seconds (0-720) the OLT tries again to register the SIP account before the session ends.
host part uri	Configure the host or domain part of the SIP URI (from 1 to 63 characters).
sip registrar	Configure the IP address or URI (from 1 to 63 characters) of the SIP registrar server.
softswitch	Configure the SIP gateway softswitch vendor name code (4 characters).
caller id	Configure the list of supported caller ID (CID) features. cal-num: Calling number cal-nam: Calling name cid-blo: CID blocking (both number and name) cid-num: CID number cid-nam: CID name ACR: Anonymous CID blocking
call waiting	Configure the list of supported call waiting features. cal-wai: Call waiting cid-ann: Caller ID announcement
call progress or transfer	Configure the list of supported features for calls in progress. 3way: 3-way calling cal-tra: Call transfer cal-hol: Call hold cal-par: Call park not-dis: Do not disturb flash: Flash on emergency service call origin: Emergency service origination hold 6way: 6-way calling
call presentation	Configure the list of supported call presentation features. spl-rin: Message waiting indication splash ring dia-ton: Message waiting indication special dial tone vis-ind: Message waiting indication visual indication cal-for: Call forwarding indication
direction connect	Configure the list of direct connect features. enable: Direct connect feature enabled dia-opt: Dial tone feature delay option
direction connect uri	Configure a direct connect URI (from 1 to 63 characters). Set a direct connect URI to use SIP to direct connect a VoIP Server.
bridged line agent uri	Set the bridged line agent URI (from 1 to 63 characters). An interaction SIP bridge enables agents to use an IP telephone at a remote location through a TCP/IP network to a Customer Interaction Center.

Table 93 Advanced Application > ONT VoIP > Voip-Sip-Profile (continued)

LABEL	DESCRIPTION
conference factory uri	Configure the conference factory URI (from 1 to 63 characters). A conference factory generates a unique conference ID, to identify and address a conference focus, using a call signaling interface.
Apply	Click Apply to save the changes.
Cancel	Click Cancel to clear the fields.
Clear	Click Clear to return the screen's settings to the defaults.
Index	This is the index number of an ONT SIP VoIP profile.
Name	This is the name of the profile.
Rule	This displays the profile's settings.
Delete	Select this for one or more profiles and click Apply to remove them.
*	Use this row to select all of the profiles for deletion.
Delete	Click Delete to remove the profiles with the Delete option selected.
Cancel	Click Cancel to begin configuring the screen again.

27.3 ONT VoIP Dial Plan Profile

The system uses dial plans to identify specific types of phone numbers dialed by a user, and to process the number before transmission by deleting or adding digits according to the relevant rule. The dial plan can also forward the call to a specific SIP server. Use a dial plan profile to collect a group of dial plans into a profile. Then assign the dial plan profile to a port to apply all of the dial plans included in the profile.

Use this screen to configure dial plan profiles. Click **Voip-Dial-Plan** in the **Advanced Application > ONT VoIP** screen to display the screen as shown.

Figure 143 Advanced Application > ONT VoIP > Voip-Dial-Plan

Index	Name	Rule	Delete
*			<input type="checkbox"/>

The following table describes the labels in this screen.

Table 94 Advanced Application > ONT VoIP > Voip-Dial-Plan

LABEL	DESCRIPTION
Name	Specify a name for the profile of dial plans.
max-size	Specify the maximum number (from 1 to 256) of dial plans.
critical-dial-timeout	<p>Specify the critical dial timeout (from 0 to 8000) in milliseconds.</p> <p>If you have a dial plan, the ONT uses a digit map internally to represent the number and type of digits it expects according to the dial plan. The ONT uses the inter-digit timer when checking a string of dialed digits for matches with the digit map. The ONT starts the inter-digit timer when a subscriber dials the first digit and restarts it after each new digit dialed until there is a digit map match or mismatch.</p> <p>The inter-digit timeout uses the partial digit timeout's value when at least one more digit is needed to match any of the digit map's patterns. If the string of dialed digits already matches a digit map, the ONT waits for the critical dial timeout period to make sure the next dialed digit does not cause a mismatch.</p> <p>If you do not have a dial plan, the ONT uses the value of the critical dial timeout for the inter-digit timer.</p>
partial-dial-timeout	Specify the partial dial timeout (from 0 to 32000) in milliseconds.
format	<p>Select the format:</p> <p>not-def: Not defined</p> <p>h248: H.248 format with specific plan (table entries define the dialing plan)</p> <p>NSC: NSC format</p> <p>ven-spe: Vendor specific format</p>
content-table	<p>Configure a dialing token (rule) in the dial plan table.</p> <p>Identify a dial plan table entry number (from 1 to 4) and dial plan rule (from 1 to 28 characters).</p> <p>Use the symbols in parentheses to create dial plan rules:</p> <ul style="list-style-type: none"> • Multiple Rule (): Use " " to separate multiple rules. • Numeric digit(x): Allow users to input any numeric digit (0~9). One 'x' means one digit. • A subset of keys ([I]): Allow users to input a range of digits, for example, [1-3] or [148]. • Repeat (.): Allow users to input a repeatable digit for more than one time, for example, (12.). This means 1, 12, 122, and 1222 are allowed. • Append (<:digits>): Append digits in the place of the rule, for example, <:123>. Digits "123" will be added in the rule. • Remove (<digits:>): Remove digits in the place of the rule, for example, <123:>. Digits "123" will be removed from the rule. • Replace (<digits:digits>): Replace the first set of digits (before the colon) with the second sets of digits (after the colon). For example, use <123:456> to replace '123' digits with '456' digits in the place of the rule. • Block (!): Type '!' at the end of the rule to block the number which matches the rule. • Wait Timeout to Dial (T): Type 'T' at the end of the rule. Once the dialed number is input, the call is dialed out after the timeout. • Gateway (=gw0=)(=gw3=): Type one of these at the end of the rule. When a dialed number matches the rule, the OLT transfers the call to the gateway (0: FXS port; 3: SIP).
Apply	Click Apply to save the changes.
Cancel	Click Cancel to clear the fields.
Clear	Click Clear to return the screen's settings to the defaults.
Index	This is the index number of an ONT VoIP dial plan profile.
Name	This is the name of the profile.
Rule	This displays the profile's settings.

Table 94 Advanced Application > ONT VoIP > Voip-Dial-Plan

LABEL	DESCRIPTION
Delete	Select this for one or more profiles and click Apply to remove them.
Select	Select this to edit the profile in the fields above.
*	Use this row to select all of the profiles for deletion.
Delete	Click Delete to remove the profiles with the Delete option selected.
Cancel	Click Cancel to begin configuring the screen again.

CHAPTER 28

PON DDMI

28.1 Overview

This chapter shows you how to configure profiles of ONT alarm thresholds. You can also configure high and low parameter limits for your OLT's SFP transceivers in this chapter.

28.1.1 What You Can Do

- Use the **PON DDMI** screen ([Section 28.2 on page 243](#)) to view the SFP transceiver information and operating parameters on a **PON** port.
- Use the **ONT Alarm Profile** screen ([Section 28.3 on page 245](#)) to create ONT alarm profiles and configure the thresholds settings.
- Use the **PON DDMI Setup** screen ([Section 28.4 on page 247](#)) to configure the limits of the alarm and warning thresholds for your OLT's SFP transceivers.

28.2 The PON DDMI Screen

The optical 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. This allows proactive, preventative network maintenance to help ensure service continuity.

Use this screen to view your OLT's current transceiver status. Click **Advanced Applications > PON DDMI** in the navigation panel to display the screen as shown.

Figure 144 Advanced Applications > PON DDMI

Each field is described in the following table.

Table 95 Advanced Applications > PON DDMI

LABEL	DESCRIPTION
	Choose the GPON interface that you want to display from the drop-down list.
Transceiver Information	
Port	This displays the PON port that the transceiver is connected to.
Vendor	This displays the vendor name of the optical transceiver.
Part Number	This displays the part number of the optical transceiver.
SN	This displays the serial number of the optical transceiver.
Revision	This displays the revision number of the optical transceiver.
Date Code	This displays the date when the optical transceiver was manufactured.
Transceiver	This displays whether the connection to the optical network is up or down.
Current	This displays the current status for each monitored DDMI parameter.
High Alarm Thres.	This displays the high value alarm threshold for each monitored DDMI parameter. An alarm signal is reported to the OLT if the monitored DDMI parameter reaches this value.
High Warn Thres.	This displays the high value warning threshold for each monitored DDMI parameter. A warning signal is reported to the OLT if the monitored DDMI parameter reaches this value.
Low Warn Thres.	This displays the low value warning threshold for each monitored DDMI parameter. A warning signal is reported to the OLT if the monitored DDMI parameter reaches this value.
Low Alarm Thres.	This displays the low value alarm threshold for each monitored DDMI parameter. An alarm signal is reported to the OLT if the monitored DDMI parameter reaches this value.
Temperature (C)	The transceiver's temperature in Celsius. The normal range is 0-70 degrees.
Voltage (V)	The transceiver's voltage in Volts. The normal range is 3.13-3.47 Volts.
TX Bias (mA)	The transceiver's bias current in mA. The normal range is 4-50 mA.
TX Power (dbm)	The transceiver's optical transmitting power in dBm. The normal range is .5 to 5 dBm. N/A displays when a transceiver is not connected to the PON port.
RX Power (dbm)	The transceiver's optical receiving power in dBm. The normal range is -6 to -28 dBm. N/A displays when a transceiver is not connected to the PON port.

Table 95 Advanced Applications > PON DDMI

LABEL	DESCRIPTION
ONT DDMI	
ONT AID	This is the ONT's ID in the format: ont-<pon>-<ont>
RX Power (dbm)	This displays the ONT's optical receiving power in dBm.

28.2.1 ONT DDMI

Click a hyperlink in the **ONT AID** field in the **Advanced Application > PON DDMI** screen to view the ONT's current transceiver status.

Figure 145 ONT DDMI

	Current	Low Thres.	High Thres.
Voltage (V)	3.22	N/A	N/A
RX Power (dbm)	-17.168	N/A	N/A
TX Power (dbm)	2.974	N/A	N/A
Laser Bias (mA)	13.450	N/A	N/A
Temperature (C)	44.585	N/A	N/A

The following table describes the labels in this screen.

Table 96 ONT DDMI

LABEL	DESCRIPTION
Current	This displays the current status for each monitored DDMI parameter.
Low Thres.	This displays the low value threshold for each monitored DDMI parameter. The ONTs reports a warning signal to the OLT if the monitored DDMI parameter reaches this value.
High Thres.	This displays the high value threshold for each monitored DDMI parameter. The ONTs reports an alarm signal to the OLT if the monitored DDMI parameter reaches this value.
RX Power (dbm)	The transceiver's optical receiving power in dBm. The normal range is -6 to -28 dBm. N/A displays when a transceiver is not connected to the PON port.
TX Power (dbm)	The transceiver's optical transmitting power in dBm. The normal range is .5 to 5 dBm. N/A displays when a transceiver is not connected to the PON port.
Laser Bias (mA)	The transceiver's bias current in mA. The normal range is 4-50 mA.
Temperature (C)	The transceiver's temperature in Celsius. The normal range is 0-70 degrees.

28.3 ONT Alarm Profile

Use this screen to configure alarm profiles for all connected ONTs. Configuring alarm profiles is to monitor the power and temperature status of all connected ONTs. When a threshold is reached, the ONT will send an alarm to the OLT.

Click **ONT Alarm Profile** in the **Advanced Application > PON DDMI** screen to display the screen as shown.

Figure 146 Advanced Application > PON DDMI > ONT Alarm Profile

ONT Alarm Profile		PON DDMI		PON DDMI Setup								
Name		Low	Up	(0~79 N/A) Units: mA								
Laser Bias Current Threshold		~	~	(-127~0 N/A) Units: dBm								
Receive Power Threshold	Low	Up	Up	(-15.3~6.5 N/A) Units: dBm								
Transmit Power Threshold	Low	Up	Up	(-40~100 N/A) Units: degree C								
Temperature Threshold	Low	Up	Up	(2.80~3.59 N/A) Units: V								
Power Feed Voltage Threshold	Low	Up	Up									
<input type="button" value="Add"/> <input type="button" value="Cancel"/> <input type="button" value="Clear"/>												
Index	Name	Bias Current Lower	Bias Current Upper	Rx Power Lower	Rx Power Upper	Tx Power Lower	Tx Power Upper	Temperature Lower	Temperature Upper	Feed Voltage Lower	Feed Voltage Upper	<input type="button" value="Delete"/>
*	DEFVAL	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	<input checked="" type="checkbox"/>
<input type="button" value="Delete"/> <input type="button" value="Cancel"/>												

The following table describes the labels in this screen.

Table 97 Advanced Application > PON DDMI > ONT Alarm Profile

LABEL	DESCRIPTION
Name	Type the name of the ONT alarm profile.
Laser Bias Current Threshold	Specify the lower and upper bounds in mA for the laser bias current threshold.
Receive Power Threshold	Specify the lower and upper bounds in dBm for the received power threshold.
Transmit Power Threshold	Specify the lower and upper bounds in dBm for the transmission power threshold.
Temperature Threshold	Specify the lower and upper bounds in degrees Celsius for the temperature threshold.
Power Feed Voltage Threshold	Specify the lower and upper bounds in volts for the power feed voltage threshold.
Add	Click Add to create an ONT alarm profile.
Cancel	Click Cancel to clear the fields.
Clear	Click Clear to return the screen's settings to the defaults.
Index	This is the index number of an ONT alarm profile.
Name	This is the name of the ONT alarm profile.
Bias Current Lower/Upper	This displays the lower and upper bounds for the laser bias current.
Rx Power Lower/Upper	This displays the lower and upper bounds for the received power.
Tx Power Lower/Upper	This displays the lower and upper bounds for the transmitted power.
Temperature Lower/Upper	This displays the lower and upper bounds for the temperature.
Feed Voltage Lower/Upper	This displays the lower and upper bounds for the power feed voltage threshold.
Delete	Select this for one or more profiles and click Delete to remove them.
*	Use this row to select all of the profiles for deletion.

Table 97 Advanced Application > PON DDMI > ONT Alarm Profile

LABEL	DESCRIPTION
Delete	Click Delete to remove the profiles with the Delete option selected.
Cancel	Click Cancel to begin configuring the screen again.

28.4 PON DDMI Setup

Use this screen to configure high and low parameter limits for your OLT's SFP transceivers. Click **PON DDMI Setup** in the **Advanced Application > PON DDMI** screen to display the screen as shown.

Figure 147 Advanced Applications > PON DDMI > PON DDMI Setup

Index	AID	Active	Delete
1	pon-1	No	<input type="checkbox"/>

PON DDMI	High Alarm Thres.	High Warn Thres.	Low Warn Thres.	Low Alarm Thres.
Temperature (C)	N/A	N/A	N/A	N/A
Voltage (V)	N/A	N/A	N/A	N/A
TX Bias (mA)	N/A	N/A	N/A	N/A
TX Power (dbm)	N/A	N/A	N/A	N/A
RX Power (dbm)	N/A	N/A	N/A	N/A

Each field is described in the following table.

Table 98 Advanced Applications > PON DDMI > PON DDMI Setup

LABEL	DESCRIPTION
	Choose the GPON interface that you want the settings configured here to apply to from the drop-down list.
Active	Select this to have the settings that are configured here take effect.
High Alarm	Use this column to set the high value alarm threshold for each monitored DDMI parameter. The ONTs connected to the GPON interface report an alarm signal to the OLT if the monitored DDMI parameter reaches this value.
High Warn	Use this column to set the high value warning threshold for each monitored DDMI parameter. The ONTs connected to the GPON interface report a warning signal to the OLT if the monitored DDMI parameter reaches this value.
Low Warn	Use this column to set the low value warning threshold for each monitored DDMI parameter. The ONTs connected to the GPON interface report a warning signal to the OLT if the monitored DDMI parameter reaches this value.
Low Alarm	Use this column to set the low value alarm threshold for each monitored DDMI parameter. The ONTs connected to the GPON interface report an alarm signal to the OLT if the monitored DDMI parameter reaches this value.
Temperature (C)	The transceiver's temperature in Celsius. The normal range is 0-70 degrees.
Voltage (V)	The transceiver's voltage in Volts. The normal range is 3.13-3.47 Volts.
TX Bias (mA)	The transceiver's bias current in mA. The normal range is 4-50 mA.

Table 98 Advanced Applications > PON DDMI > PON DDMI Setup

LABEL	DESCRIPTION
TX Power (dBm)	The transceiver's optical transmitting power in dBm. The normal range is .5 to 5 dBm. N/A displays when the PON port is not connected.
RX Power (dBm)	The transceiver's optical receiving power in dBm. The normal range is -6 to -28 dBm. N/A displays when the PON port is not connected.
Add	Click Add to save the parameters to the GPON interface selected from the drop-down list.
Cancel	Click Cancel to clear the fields.
Clear	Click Clear to return the screen's settings to the defaults.
Index	This is the index number of a PON DDMI entry.
AID	This displays the GPON interface of this entry.
Active	This displays whether the PON DDMI settings of this entry are enabled or not.
Delete	Select this for one or more profiles and click Delete to remove them.
Delete	Click Delete to remove the profiles with the Delete option selected.
Cancel	Click Cancel to begin configuring the screen again.
PON DDMI	
High Alarm Thres.	This displays the high value alarm threshold for each monitored DDMI parameter. The OLT reports an alarm signal to the Optical Line Terminal (OLT) if the monitored DDMI parameter reaches this value.
High Warn Thres.	This displays the high value warning threshold for each monitored DDMI parameter. The OLT reports an warning signal to the Optical Line Terminal (OLT) if the monitored DDMI parameter reaches this value.
Low Warn Thres.	This displays the low value warning threshold for each monitored DDMI parameter. The OLT reports an warning signal to the Optical Line Terminal (OLT) if the monitored DDMI parameter reaches this value.
Low Alarm Thres.	This displays the low value alarm threshold for each monitored DDMI parameter. The OLT reports an alarm signal to the Optical Line Terminal (OLT) if the monitored DDMI parameter reaches this value.
Temperature (C)	The transceiver's temperature in Celsius. The normal range is 0-70 degrees.
Voltage (V)	The transceiver's voltage in Volts. The normal range is 3.13-3.47 Volts.
TX Bias (mA)	The transceiver's bias current in mA. The normal range is 4-50 mA.
TX Power (dbm)	The transceiver's optical transmitting power in dBm. The normal range is .5 to 5 dBm. N/A displays when a transceiver is not connected to the PON port.
RX Power (dbm)	The transceiver's optical receiving power in dBm. The normal range is -6 to -28 dBm. N/A displays when a transceiver is not connected to the PON port.

CHAPTER 29

File Transfer

29.1 Overview

Use this screen to transfer a config.xml file between a specific URL and an ONT using FTP.

29.2 The File Transfer Screen

Use this screen to transfer a config.xml file between a specific URL and an ONT using FTP.

Click **Advanced Application > File Transfer** in the navigation panel to display the screen as shown.

Figure 148 Advanced Application > File Transfer

File Transfer	
ONT	<input type="button" value="▼"/>
Local File Name	<input type="text"/>
URI	<input type="text"/>
Username	<input type="text"/>
Password	<input type="text"/>
<input type="button" value="Upload"/> <input type="button" value="Download"/> <input type="button" value="Cancel"/>	

The following table describes the labels in this screen.

Table 99 Advanced Application > File Transfer

LABEL	DESCRIPTION
	Choose the GPON interface that the ONT is connected to from the drop-down list.
ONT	Select the ONT to which you want to transfer the file.
Local File Name	Type the full path of the config.xml file on the FTP server, which you want to transfer to or from the ONT.
URI	Type the URL of an FTP server with the config.xml file you want to transfer to or from the ONT.
Username	Enter the user name for the FTP server.
Password	Enter the password, up to 25 printable characters, of the user account.
Upload	Click Upload to transfer the specified file from the ONT to the FTP server.
Download	Click Download to transfer the specified file from the FTP server to the ONT.
Cancel	Click Cancel to clear the fields.

CHAPTER 30

ONT PM Counter

30.1 Overview

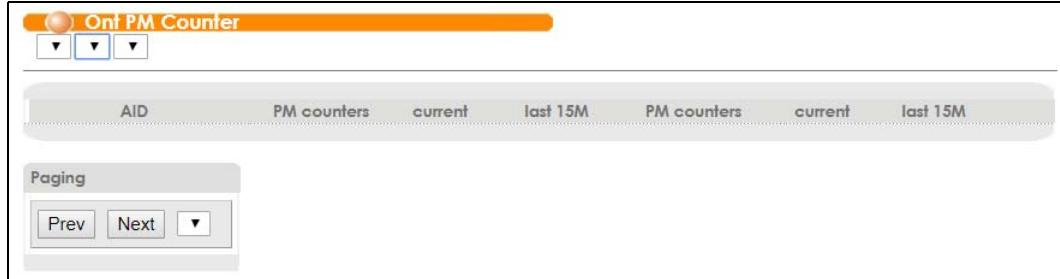
Use this screen to view the performance monitoring counters of the registered ONTs.

30.2 The ONT PM Counter Screen

Use this screen to view the performance monitoring counters of the registered ONTs.

Click **Advanced Application > ONT PM Counter** in the navigation panel to display the screen as shown.

Figure 149 Advanced Application > ONT PM Counter



The following table describes the labels in this screen.

Table 100 Advanced Application > ONT PM Counter

LABEL	DESCRIPTION
	Select the GPON interface that the ONTs are connected to from the first drop-down list.
	Select a range of the connected ONTs from the second drop-down list.
	Select the ONT that you want to view the performance monitoring counters from the third drop-down list. If you forget the ONT ID of the ONT that you want to show here, go to the Advanced Application > ONT Quick Setup screen to check.
AID	This is the ONT's ID in the format: uniport-<pon>-<ont>-<card>-<port>.
PM counters	This displays the PM counter types.
current	This displays the PM counters from the past 15 minutes.
last 15M	This displays the PM counters from the past 16 to 30 minutes.
Paging	
Prev/Next	Click Prev or Next to show the previous/next screen if all status information cannot be seen in one screen.

CHAPTER 31

QoS Profile

31.1 ONT QoS

Use the ONT QoS screens to configure Quality of Service settings for the ONT devices.

31.1.1 What You Can Do

- Use the **Ingress Profile** screen ([Section 31.2 on page 251](#)) to configure ONT QoS ingress profiles to map IEEE 802.1p priority tags to traffic classes.
- Use the **Bw-Profile** screen ([Section 31.3 on page 252](#)) to configure ONT QoS upstream and downstream bandwidth profiles.
- Use the **Pbit-Profile** screen ([Section 31.4 on page 253](#)) to configure ONT QoS profiles that translate IEEE 802.1p priority bit values to other values.

31.2 ONT QoS Ingress Profile

Use this screen to configure ONT QoS ingress profiles to map IEEE 802.1p priority tags to traffic classes.

Click **Advanced Application > QoS Profile** in the navigation panel to display the screen as shown.

Figure 150 Advanced Application > QoS Profile > Ingress Profile

Ingress-Profile		Bw-Profile	Pbit-Profile												
Ingress-Profile	Name														
	Dot1p0tc	null ▼													
	Dot1p1tc	null ▼													
	Dot1p2tc	null ▼													
	Dot1p3tc	null ▼													
	Dot1p4tc	null ▼													
	Dot1p5tc	null ▼													
	Dot1p6tc	null ▼													
Dot1p7tc	null ▼														
<input type="button" value="Add"/> <input type="button" value="Cancel"/> <input type="button" value="Clear"/>															
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 10%;">Index</th> <th style="width: 30%;">Name</th> <th style="width: 40%;">Rule</th> <th style="width: 20%;">Delete</th> </tr> </thead> <tbody> <tr> <td>*</td> <td></td> <td></td> <td><input type="checkbox"/></td> </tr> <tr> <td>1</td> <td>DEFVAL</td> <td>DOT1P0TC = 1, DOT1P1TC = 1, DOT1P2TC = 1, DOT1P3TC = 1, DOT1P4TC = 1, DOT1P5TC = 1, DOT1P6TC = 1, DOT1P7TC = 1</td> <td><input type="checkbox"/></td> </tr> </tbody> </table>				Index	Name	Rule	Delete	*			<input type="checkbox"/>	1	DEFVAL	DOT1P0TC = 1, DOT1P1TC = 1, DOT1P2TC = 1, DOT1P3TC = 1, DOT1P4TC = 1, DOT1P5TC = 1, DOT1P6TC = 1, DOT1P7TC = 1	<input type="checkbox"/>
Index	Name	Rule	Delete												
*			<input type="checkbox"/>												
1	DEFVAL	DOT1P0TC = 1, DOT1P1TC = 1, DOT1P2TC = 1, DOT1P3TC = 1, DOT1P4TC = 1, DOT1P5TC = 1, DOT1P6TC = 1, DOT1P7TC = 1	<input type="checkbox"/>												
<input type="button" value="Delete"/> <input type="button" value="Cancel"/>															

The following table describes the labels in this screen.

Table 101 Advanced Application > QoS Profile > Ingress Profile

LABEL	DESCRIPTION
Name	Specify a name for the ingress profile.
Dot1p0tc ~ Dot1p7tc	Select the traffic class values (0-7 or null) to which to map IEEE 802.1p priority tags.
Add	Click Add to add an ingress profile.
Cancel	Click Cancel to clear the fields.
Clear	Click Clear to clear the fields.
Index	This is the index number of an ONT QoS ingress profile.
Name	This is the name of the profile.
Rule	This displays the profile's settings.
Delete	Select this for one or more profiles and click Delete to remove them.
*	Use this row to select all of the profiles for deletion.
Delete	Click Delete to remove the profiles with the Delete option selected.
Cancel	Click Cancel to begin configuring the screen again.

31.3 ONT QoS Bandwidth Profile

Use this screen to configure ONT QoS upstream and downstream bandwidth profiles.

Click **Bw-Profile** in the **Advanced Application > QoS Profile** screen to display the screen as shown.

Figure 151 Advanced Application > QoS Profile > Bw-Profile

Index	Name	Ustype	Rule	Delete
1	DEFVAL	5	sir = 1024, air = 1024, pir = 2048	<input type="checkbox"/>

The following table describes the labels in this screen.

Table 102 Advanced Application > QoS Profile > Bw-Profile

LABEL	DESCRIPTION																				
Name	Specify a name for the bandwidth profile.																				
Ustype	<p>Specify the upstream bandwidth group type the profile uses.</p> <p>The upstream bandwidth group type and profile settings display below this field. Click Type Help to display all bandwidth group types and how their bandwidth is controlled by SIR, AIR, and PIR parameters respectively.</p> <p>Figure 152 ONT Templates</p> <table border="1"> <tr> <td>Type 1</td><td>Type 2</td><td>Type 3</td><td>Type 4</td><td>Type 5</td></tr> <tr> <td>sir > 0</td><td>sir = 0</td><td>sir = 0</td><td>sir = 0</td><td>sir > 0</td></tr> <tr> <td>air = 0</td><td>air > 0</td><td>air > 0</td><td>air = 0</td><td>air > 0</td></tr> <tr> <td>pir = sir</td><td>pir = air</td><td>pir > air</td><td>pir > 0</td><td>pir >= sir + air</td></tr> </table>	Type 1	Type 2	Type 3	Type 4	Type 5	sir > 0	sir = 0	sir = 0	sir = 0	sir > 0	air = 0	air > 0	air > 0	air = 0	air > 0	pir = sir	pir = air	pir > air	pir > 0	pir >= sir + air
Type 1	Type 2	Type 3	Type 4	Type 5																	
sir > 0	sir = 0	sir = 0	sir = 0	sir > 0																	
air = 0	air > 0	air > 0	air = 0	air > 0																	
pir = sir	pir = air	pir > air	pir > 0	pir >= sir + air																	
SIR	Specify the profile's Sustained Information Rate (SIR) in kbps.																				
AIR	Specify the profile's Access Information Rate (AIR) in kbps.																				
PIR	<p>Specify the profile's Peak Information Rate (PIR) in kbps.</p> <p>The PIR is the maximum bandwidth allowed for the incoming traffic flow on a port when there is no network congestion.</p>																				
Apply	Click Apply to save the changes.																				
Cancel	Click Cancel to clear the fields.																				
Clear	Click Clear to return the screen's settings to the defaults.																				
Index	This is the index number of an ONT QoS bandwidth profile.																				
Name	This is the name of the profile.																				
Ustype	This displays the upstream bandwidth group type the profile uses.																				
Rule	This displays the profile's settings.																				
Delete	Select this for one or more profiles and click Delete to remove them.																				
*	Use this row to select all of the profiles for deletion.																				
Delete	Click Delete to remove the profiles with the Delete option selected.																				
Cancel	Click Cancel to begin configuring the screen again.																				
Paging																					
Prev/Next	Click Prev or Next to show the previous/next screen if all status information cannot be seen in one screen.																				

31.4 ONT QoS Pbit Profile

Use this screen to configure ONT QoS profiles that translate IEEE 802.1p priority bit values to other values.

Click **Pbit-Profile** in the **Advanced Application > QoS Profile** screen to display the screen as shown.

Figure 153 Advanced Application > QoS Profile > Pbit-Profile

Pbit-Profile		Ingress-Profile	Bw-Profile	Cac-Profile
Pbit-Profile	Name			
	P0to	0		
	P1to	1		
	P2to	2		
	P3to	3		
	P4to	4		
	P5to	5		
	P6to	6		
P7to	7			
<input type="button" value="Add"/> <input type="button" value="Cancel"/> <input type="button" value="Clear"/>				
Index	Name	Rule	Delete	
*			<input type="checkbox"/>	
<input type="button" value="Delete"/> <input type="button" value="Cancel"/>				

The following table describes the labels in this screen.

Table 103 Advanced Application > QoS Profile > Pbit-Profile

LABEL	DESCRIPTION
Name	Specify a name for the priority bit profile.
P0to ~ P7to	Specify to which values (0-7 or drop) to translate the values of IEEE 802.1p priority tags.
Add	Click Add to add a pbit profile.
Cancel	Click Cancel to clear the fields.
Clear	Click Clear to return the screen's settings to the defaults.
Index	This is the index number of an ONT QoS priority bit profile.
Name	This is the name of the profile.
Rule	This displays the profile's settings.
Delete	Select this for one or more profiles and click Delete to remove them.
*	Use this row to select all of the profiles for deletion.
Delete	Click Delete to remove the profiles with the Delete option selected.
Cancel	Click Cancel to begin configuring the screen again.

CHAPTER 32

OLT Registration

32.1 OLT Registration Overview

The **OLT Registration** screens include **OLT Registration**, **Tca Configuration**, **ONT Summary**, **OLT Status**, **OLT Counter**, and **Tca Status**.

32.1.1 What You Can Do

- Use the **OLT Registration** screen ([Section 32.2 on page 256](#)) to configure how you want to register the ONTs that are connected to a GPON interface on the OLT.
- Use the **Tca Configuration** screen ([Section 32.3 on page 258](#)) to configure thresholds for the TCA profile.
- Use the **ONT Summary** screen ([Section 32.4 on page 260](#)) to view the status of all ONTs for each GPON interface.
- Use the **OLT Status** screen ([Section 32.5 on page 261](#)) to view the OLT status.
- Use the **OLT Counter** screen ([Section 32.6 on page 262](#)) to display the counters of the configured GPON interface.
- Use the **Tca Status** screen ([Section 32.7 on page 263](#)) to view the threshold of the TCA profile.

32.1.2 What You Need to Know

The following terms and concepts may help as you read this chapter.

Forward Error Correction (FEC)

FEC is a technique to control errors in packets and correct errors without transmitting the packets again. FEC adds redundant information in the packets, so the receivers can identify and correct the errors in the packets. This increases data quality and saves bandwidth usage of the OLT.

Authentication Process

The authentication process includes the six states below.

- **O1 Initial-state:** An ONT is in this state when it's turned on. Two alarm messages, LOS (Loss of Signal) and LOF (Loss of Frame) will be asserted. When downstream traffic is received, these alarm messages will be cleared, and the ONT goes to O2 state.
- **O2 Standby-state:** When the ONT receives the Upstream_Overhead message, relevant parameters will be configured, and the ONT goes to O3 state.
- **O3 Serial-Number-state:** The OLT requests GPON serial numbers of the ONT in this state. When the ONT is discovered, the OLT will assign a unique ONT ID. The ONT goes to O4 state when it has an ONT ID.

- **O4 Ranging-state:** An equalization delay is measured for the ONT in this state. This synchronized the upstream transmission of the ONTs located in different places. When the ONT received the Ranging_Time message, it goes to O5 state.
- **O5 Operation-state:** The ONT can send upstream data and PLOAM messaged in this state.
- **O6 POPUP-state:** When the ONT loses optical signals, the ONT goes to this state. In the meantime, the ONT stops upstream transmission, and it will detect an LOS alarm.
- **O7 Emergency-Stop-state:** The ONT goes to this state when it receives a Disable_Serial_Number message. The ONT is forbidden to transmit upstream data.

32.2 The OLT Registration Screen

Use this screen to configure how you want to register the ONTs that are connected to a GPON interface on the OLT. Click **Advanced Application > OLT Registration** in the navigation panel to display the screen as shown.

Figure 154 Advanced Application > OLT Registration

AID	Register-Method	Transceiver	Template	ONT Template Active	Fec Active	Ranging Distance	Active	Delete
							<input checked="" type="checkbox"/>	<input type="checkbox"/>

The following table describes the labels in this screen.

Table 104 Advanced Application > OLT Registration

LABEL	DESCRIPTION
Active	Select this to enable the GPON interface settings on the selected GPON interface.
AID	Choose the GPON interface that you want the settings configured here to apply to from the drop-down list.

Table 104 Advanced Application > OLT Registration

LABEL	DESCRIPTION
Register-Method	Select the method (A, C, C-autolock, or D) the OLT uses to register ONTs connected to the port. A: (used in this example) requires the serial number and password the ONT sends to match the ones you configure on the OLT. C: requires the physical layer operations and maintenance (PLOAM) password the ONT sends to match what you configure on the OLT. C-autolock: requires the serial number the ONT sends to match the one you configure on the OLT. D: automatically registers the ONT and brings it into service without checking the serial number or password. E: non-volatile auto provision by template (onu-128). Choose method D or E to apply the selected ONT template to all ONTs this GPON interface registers. For other registration methods, you can apply a different template for each ONT in the ONT Quick Setup screen.
Transceiver	Select 12 (Hisense class C+ transceiver) for the type of the default transceiver the PON port uses. A Hisense class C+ transceiver is provided along with the package.
ONT Template Active	Select this to enable the ONT template.
Template	Select the ONT template to use for the GPON interface. You can modify these templates in the Advanced Application > ONT Template screen or manually using CLI commands. Note: This field is grayed out when you select A , C , or C-autolock in the Register-Method field.
Fec Active	Select this to enable the Forward Error Correction (FEC) feature. See Section 32.1.2 on page 255 for more information about FEC.
Ranging Distance	Configure the maximum ranging distance for the GPON interface.
Add	Click Add to apply the settings to a GPON port.
Cancel	Click Cancel to clear the fields.
Clear	Click Clear to return the screen's settings to the defaults.
AID	This is the identifier for the GPON interface.
Register-Method	This displays the method (A, C, C-autolock, D, or E) the OLT registers ONTs connected to the port.
Transceiver	This displays the type of transceiver (12) the PON port uses.
Template	This displays the ONT template to use for the GPON interface.
ONT Template Active	This displays whether the ONT template is enabled or not.
Fec Active	This displays whether the Forward Error Correction (FEC) feature is enabled or not.
Ranging Distance	This displays the maximum ranging distance for the GPON interface.
Active	This displays whether the GPON interface settings for the GPON interface is active or not.
Delete	Select this for one or more profiles and click Delete to remove them.
*	Use this row to select all of the profiles for deletion.
Delete	Click Delete to remove the profiles with the Delete option selected.
Cancel	Click Cancel to begin configuring the screen again.

32.3 The Tca Configuration Screen

Use this screen to configure thresholds for the (Threshold-Crossing Alarms) TCA profile. Click **Tca Configuration** in the **Advanced Application > OLT Registration** screen to display the screen as shown.

The OLT will send threshold-crossing alarms to an ONT if the ONT's parameters go beyond the thresholds configured here.

Figure 155 Advanced Application > OLT Registration > Tca Configuration

Tca Configuration		OLT Reg	ONT Summary	OLT Status	OLT Counter	Tca Status
Tca Active	AID	<input type="checkbox"/> pon-				
FEC Code Word Threshold			[0 - 4294967295]			
FEC Corrected Byte Threshold			[0 - 4294967295]			
FEC Corrected Code Word Threshold			[0 - 4294967295]			
FEC Uncorrected Code Word Threshold			[0 - 4294967295]			
BIP byte Threshold			[0 - 4294967295]			
BIP error Threshold			[0 - 4294967295]			
Rx PLOAM CRC error Threshold			[0 - 4294967295]			
Rx PLOAM non idle Threshold			[0 - 4294967295]			
Positive drift Threshold			[0 - 4294967295]			
Negative drift Threshold			[0 - 4294967295]			
Rx OMCI Packet Threshold			[0 - 4294967295]			
Rx OMCI Packet CRC error Threshold			[0 - 4294967295]			
REI counter Threshold			[0 - 4294967295]			
Unreceived burst Threshold			[0 - 4294967295]			
LCDGI error Threshold			[0 - 4294967295]			
RDI error Threshold			[0 - 4294967295]			

The following table describes the labels in this screen.

Table 105 Advanced Application > OLT Registration > Tca Configuration

Label	Description
Tca Active	Select this to enable low rate Threshold Crossing Alert (TCA) alarm.
AID	Enter the identifier for the GPON interface that you want the settings configured here to apply to.
FEC Code Word Threshold	Enter the threshold of codewords that can be received in the Forward Error Correction (FEC) process.
FEC Corrected Byte Threshold	Enter the threshold of corrected bytes that can be received in the Forward Error Correction (FEC) process.
FEC Corrected Code Word Threshold	Enter the threshold of corrected codewords that can be received in the Forward Error Correction (FEC) process.

Table 105 Advanced Application > OLT Registration > Tca Configuration

LABEL	DESCRIPTION
FEC Uncorrected Code Word Threshold	Enter the threshold of codewords that can be received without being corrected in the Forward Error Correction (FEC) process.
BIP byte Threshold	Enter the threshold of Bit Interleaved Parity (BIP) bytes that can be received.
BIP error Threshold	Enter the threshold of Bit Interleaved Parity (BIP) errors that are allowed.
Rx PLOAM CRC error Threshold	Enter the threshold of Cyclic Redundancy Check (CRC) errors that are allowed in a received Physical Layer OAM Operations, Administrations and Maintenance (PLOAM) message.
Rx PLOAM non idle Threshold	Enter the threshold of non-idle PLOAM (Physical Layer Operation, Administration and Maintenance.) messages that can be received.
Positive drift Threshold	Enter the threshold of positive drifts that are allowed to increase the values of equalization delays.
Negative drift Threshold	Enter the threshold of negative drifts that are allowed to decrease the values of equalization delays.
Rx OMCI Packet Threshold	Enter the threshold of OMCI (Optical Network Unit Management and Control Interface) packets that can be received.
Rx OMCI Packet CRC error Threshold	Enter the threshold of OMCI packets with Cyclic Redundancy Check (CRC) errors that can be received.
REI counter Threshold	Enter the threshold of Remote Error Indication (REI) counters for BER (Bit Error Rate) reports.
Unreceived burst Threshold	Enter the threshold of burst that are allowed to be dropped.
LCDGI error Threshold	Enter the threshold of LCDGI LCDGi (Loss of GEM Channel Delineation) errors that are allowed.
RDI error Threshold	Enter the threshold of RDI (Remote Defect Indication) errors that are allowed.
Add	Click Add to add a TCA profile.
Cancel	Click Cancel to clear the fields.
Clear	Click Clear to return the screen's settings to the defaults.
AID	This is the identifier for the GPON interface.
FEC Code Word Threshold	This displays the threshold of codewords that can be received in the Forward Error Correction (FEC) process.
Positive drift Threshold	This displays the threshold of positive drifts that are allowed to increase the values of equalization delays.
FEC Corrected Byte Threshold	This displays the threshold of bytes that can be corrected by Forward Error Correction (FEC) feature.

Table 105 Advanced Application > OLT Registration > Tca Configuration

LABEL	DESCRIPTION
Negative drift Threshold	This displays the threshold of negative drifts that are allowed to decrease the values of equalization delays.
FEC Corrected Code Word Threshold	This displays the threshold of codewords that can be corrected by Forward Error Correction (FEC) feature.
Rx OMCI Packet Threshold	This displays the threshold of OMCI (Optical Network Unit Management and Control Interface) packets that can be received.
FEC Uncorrected Code Word Threshold	This displays the threshold of codewords that are allowed not to be corrected by Forward Error Correction (FEC) feature.
Rx OMCI Packet CRC error Threshold	This displays the threshold of Cyclic Redundancy Check (CRC) errors that are allowed in a received OMCI packet.
BIP byte Threshold	This displays the threshold of Bit Interleaved Parity (BIP) bytes that can be received.
REI counter Threshold	This displays the threshold of Remote Error Indication (REI) counters for BER (Bit Error Rate) reports.
BIP error Threshold	This displays the threshold of Bit Interleaved Parity (BIP) errors that are allowed.
Unreceived burst Threshold	This displays the threshold of burst that are allowed to be dropped.
Rx PLOAM CRC error Threshold	This displays the threshold of Cyclic Redundancy Check (CRC) errors that are allowed in a received Physical Layer OAM Operations, Administrations and Maintenance (PLOAM) message.
LCDGI error Threshold	This displays the threshold of LCDGI LCDGI (Loss of GEM Channel Delineation) errors that are allowed.
Rx PLOAM non idle Threshold	This displays the threshold of non-idle PLOAM messages that can be received.
RDI error Threshold	This displays the threshold of RDI (Remote Defect Indication) errors that are allowed.

32.4 The ONT Summary Screen

Use this screen to display the status of all ONTs for each GPON interface. Click **ONT Summary** in the **Advanced Application > OLT Registration** screen to display the screen as shown.

Figure 156 Advanced Application > OLT Registration > ONT Summary

ONT Summary		OLT Reg		Tca Configuration		OLT Status		OLT Counter		Tca Status		
PON AID	Unreg.	O7	IS	OOS-LO	OOS-SB	OOS-DG	OOS-LS	OOS-NR	OOS-CD	OOS-TM	OOS-NP	OOS-PF
pon-1	0	0	0	0	0	0	0	0	0	0	0	0
pon-2	0	0	0	0	0	0	0	0	0	0	0	0
pon-3	0	0	0	0	0	0	0	0	0	0	0	0
pon-4	0	0	0	0	0	0	0	0	0	0	0	0
Total	0	0	0	0	0	0	0	0	0	0	0	0

The following table describes the labels in this screen.

Table 106 Advanced Application > OLT Registration > ONT Summary

LABEL	DESCRIPTION
PON AID	This is the identifier for the GPON interface.
Unreg	This shows how many unregistered ONT devices are connected to the GPON interface.
O7	This shows how many ONTs connected to the GPON interface are forbidden to transmit upstream data.
IS	This shows how many in-service ONTs are connected to the GPON interface.
OOS-LO	This shows how many ONTs connected to the GPON interface have an Out Of Service status.
OOS-SB	This shows how many ONTs connected to the GPON interface have an Out Of Service - StandBy status.
OOS-DG	This shows how many ONTs connected to the GPON interface have an Out Of Service - Dying Gasp status.
OOS-LS	This shows how many ONTs connected to the GPON interface have an Out Of Service - Loss Of Signal status.
OOS-NR	This shows how many ONTs connected to the GPON interface have an Out Of Service - Not Registered status.
OOS-CD	This shows how many ONTs connected to the GPON interface have an Out Of Service - OMCC Down status.
OOS-TM	This shows how many ONTs connected to the GPON interface have an Out Of Service - Type Mismatch.
OOS-NP	This shows how many ONTs connected to the GPON interface have an Out Of Service - Not Provisioned status.
OOS-PF	This shows how many ONTs connected to the GPON interface have an Out Of Service - Provision Fail status.

32.5 The OLT Status Screen

Use this screen to view the OLT status. Click **OLT Status** in the **Advanced Application > OLT Registration** screen to display the screen as shown.

Figure 157 Advanced Application > OLT Registration > OLT Status

OLT Status		OLT Reg		Tca Configuration		ONT Summary		OLT Counter		Tca Status	
PON AID	State	Key_Exchange	SN_Acq	Rogue Defect	Interval SN_Acq	Interval Key_Exchange	LOS				

The following table describes the labels in this screen.

Table 107 Advanced Application > OLT Registration > OLT Status

LABEL	DESCRIPTION
PON AID	This is the identifier for the GPON interface.
State	This shows the GPON interface's ONT link status. This shows ACTIVE if the ONT is connected to the PON port.
Key_Exchang e	This shows whether the key exchange is enabled or disabled on the PON port.
SN_Acq	This shows whether serial number acquisition is enabled or disabled on the PON port. It is enabled by default.
Rogue Detect	This shows whether rogue ONT detection is enabled or disabled on the PON port. In some circumstances, some ONTs may be out of the OLT's control and impact other ONUs' data transmission. The OLT can be set to perform rogue detection to diagnose it. Note that the ONT must support rogue detection for this to work. Please use the rogue detection commands to start or stop the diagnosis.
Interval SN_Acq	This shows the interval at which the OLT broadcasts a Serial Number Acquisition message to ONTs connected to a PON port, in units of ms. When an ONT receives the SN ACQ message, it sends a DISCOVERED SN message with its serial number back to the OLT. The value is 8000 ms by default.
Interval Key_Exchang e	This shows the interval that the OLT and ONT exchange the key for AES encryption, in units of ms. If the key exchange is enabled, the OLT and ONT need a key to encrypt transmitted packets and decrypt received packets. And they need to update the key periodically for security reasons. 3600000 means the OLT and ONT exchange their key every 3600000 ms (1hr).
LOS	This shows whether a signal loss occurs on a PON port. It displays ON when the fiber optic connection is down or an ONT is disconnected from the PON port.

32.6 The OLT Counter Screen

Use this screen to display the counters of the configured GPON interface. Click **OLT Counter** in the **Advanced Application > OLT Registration** screen to display the screen as shown.

Figure 158 Advanced Application > OLT Registration > OLT Counter



The following table describes the labels in this screen.

Table 108 Advanced Application > OLT Registration > OLT Counter

LABEL	DESCRIPTION
PON AID	This is the identifier for the GPON interface.
DS	
TransPkts	This displays how many downstream packets the PON port has transmitted.
CpuPkts	This displays how many downstream CPU packets the PON port has transmitted.
TransPloams	This displays how many downstream Physical Layer Operations, Administration and Maintenance (PLOAM) packets the PON port has transmitted.
US	
PonPkts	This displays how many upstream PON packets the PON port has received.
ValidPloams	This displays the total number of upstream PLOAM massages, including idle PLOAMS.

Table 108 Advanced Application > OLT Registration > OLT Counter

LABEL	DESCRIPTION
ValidNonidlePloams	This displays number of upstream stream valid PLOAM packets, excluding idle PLOAMs.
ErrPloams	This displays how many upstream messages were dropped due to CRC errors.
FifoFullDiscardPloams	This displays how many upstream PLOAMs were dropped due to the first-in-first-out queue being full.
InvalidDiscardPkts	This displays how many assembled packets were discarded due to invalid length.
CpuPkts	This displays the number of upstream CPU packets received. CPU packets are those processed in the PON chip CPU, usually for communicating with or controlling the PON chip.
Refresh	Click Refresh to update this screen.
Clear Counter	Click Clear Counter to remove the counters.

32.7 The Tca Status Screen

Use this screen to view the threshold of the TCA profile. Click **Tca Status** in the **Advanced Application > OLT Registration** screen to display the screen as shown.

Figure 159 Advanced Application > OLT Registration > Tca Status

PON AID	TCA Status	OLT Reg	Tca Configuration	ONT Summary	OLT Status	OLT Counter
Fec Configuration						
pon-1	TCA status		OFF			
	FEC Code Word Threshold	0	FEC Corrected Byte Threshold	0		
	FEC Corrected Code Word Threshold	0	FEC Uncorrected Code Word Threshold	0		
	BIP byte Threshold	0	BIP error Threshold	0		
	Rx PLOAM CRC error Threshold	0	Rx PLOAM non idle Threshold	0		
	Positive drift Threshold	0	Negative drift Threshold	0		
	Rx OMCI Packet Threshold	0	Rx OMCI Packet CRC error Threshold	0		
	REI counter Threshold	0	Unreceived burst Threshold	0		
	LCDGI error Threshold	0	RDI error Threshold	0		
pon-2	TCA status		OFF			
	FEC Code Word Threshold	0	FEC Corrected Byte Threshold	0		
	FEC Corrected Code Word Threshold	0	FEC Uncorrected Code Word Threshold	0		
	BIP byte Threshold	0	BIP error Threshold	0		
	Rx PLOAM CRC error Threshold	0	Rx PLOAM non idle Threshold	0		
	Positive drift Threshold	0	Negative drift Threshold	0		
	Rx OMCI Packet Threshold	0	Rx OMCI Packet CRC error Threshold	0		
	REI counter Threshold	0	Unreceived burst Threshold	0		
	LCDGI error Threshold	0	RDI error Threshold	0		
pon-3	TCA status		OFF			
	FEC Code Word Threshold	0	FEC Corrected Byte Threshold	0		
	FEC Corrected Code Word Threshold	0	FEC Uncorrected Code Word Threshold	0		
	BIP byte Threshold	0	BIP error Threshold	0		
	Rx PLOAM CRC error Threshold	0	Rx PLOAM non idle Threshold	0		
	Positive drift Threshold	0	Negative drift Threshold	0		
	Rx OMCI Packet Threshold	0	Rx OMCI Packet CRC error Threshold	0		
	REI counter Threshold	0	Unreceived burst Threshold	0		
	LCDGI error Threshold	0	RDI error Threshold	0		
pon-4	TCA status		OFF			
	FEC Code Word Threshold	0	FEC Corrected Byte Threshold	0		
	FEC Corrected Code Word Threshold	0	FEC Uncorrected Code Word Threshold	0		
	BIP byte Threshold	0	BIP error Threshold	0		
	Rx PLOAM CRC error Threshold	0	Rx PLOAM non idle Threshold	0		
	Positive drift Threshold	0	Negative drift Threshold	0		
	Rx OMCI Packet Threshold	0	Rx OMCI Packet CRC error Threshold	0		
	REI counter Threshold	0	Unreceived burst Threshold	0		
	LCDGI error Threshold	0	RDI error Threshold	0		

The following table describes the labels in this screen.

Table 109 Advanced Application > OLT Registration > Tca Status

LABEL	DESCRIPTION
PON AID	This is the identifier for the GPON interface.
TCA status	This displays whether low rate Threshold Crossing Alert (TCA) alarm is enabled or not.
FEC Code Word Threshold	This displays the threshold of codewords that can be received in the Forward Error Correction (FEC) process.
FEC Corrected Byte Threshold	This displays the threshold of bytes that can be corrected by Forward Error Correction (FEC) feature.
FEC Corrected Code Word Threshold	This displays the threshold of codewords that can be corrected by Forward Error Correction (FEC) feature.
FEC Uncorrected Code Word Threshold	This displays the threshold of codewords that are allowed not to be corrected by Forward Error Correction (FEC) feature.
BIP byte Threshold	This displays the threshold of Bit Interleaved Parity (BIP) bytes that can be received.
BIP error Threshold	This displays the threshold of Bit Interleaved Parity (BIP) errors that are allowed.
Rx PLOAM CRC error Threshold	This displays the threshold of Cyclic Redundancy Check (CRC) errors that are allowed in a received Physical Layer OAM Operations, Administrations and Maintenance (PLOAM) message.
Rx PLOAM non idle Threshold	This displays the threshold of non-idle PLOAM messages that can be received.
Positive drift Threshold	This displays the threshold of positive drifts that are allowed to increase the values of equalization delays.
Negative drift Threshold	This displays the threshold of negative drifts that are allowed to decrease the values of equalization delays.
Rx OMCI Packet Threshold	This displays the threshold of OMCI (Optical Network Unit Management and Control Interface) packets that can be received.
Rx OMCI Packet CRC error Threshold	This displays the threshold of Cyclic Redundancy Check (CRC) errors that are allowed in a received OMCI packet.
REI counter Threshold	This displays the threshold of Remote Error Indication (REI) counters for BER (Bit Error Rate) reports.
Unreceived burst Threshold	This displays the threshold of burst that are allowed to be dropped.
LCDGI error Threshold	This displays the threshold of LCDGI LCDGi (Loss of GEM Channel Delineation) errors that are allowed.
RDI error Threshold	This displays the threshold of RDI (Remote Defect Indication) errors that are allowed.

CHAPTER 33

ONT Template

33.1 ONT Template Overview

Configure ONT templates to manage ONT settings. After you create ONT templates, see [Chapter 34 on page 277](#) to create ONT configurations to apply them.

An ONT template defines the general settings for an ONT, such as DHCP option 82 information, the port speed, and performance monitoring.

33.1.1 What You Can Do

- Use the **ONT Template** screen ([Section 33.2 on page 265](#)) to configure templates' settings.
- Use the **ONT Bwgroup** screen ([Section 33.2.1 on page 268](#)) to configure bandwidth group settings for ONTs.
- Use the **Uniport Queue** screen ([Section 33.2.2 on page 269](#)) to configure QoS queues for the UNI (User Network Interface) ports.
- Use the **Uniport VLAN** screen ([Section 33.2.3 on page 271](#)) to configure UNI port VLAN flow settings.
- Use the **Uniport Multicast** screen ([Section 33.2.4 on page 273](#)) to configure UNI port multicast subscriber channels.
- Use the **Uniport VoIP** screen ([Section 33.2.5 on page 275](#)) to configure UNI port VoIP settings.

33.2 The ONT Template Screen

Use this screen to edit or modify the ONT template configurations. A PON port can have up to 8 templates. Click **Advanced Application > ONT Template** in the navigation panel to display the screen as shown.

Figure 160 Advanced Application > ONT Template

The following table describes the labels in this screen.

Table 110 Advanced Application > ONT Template

LABEL	DESCRIPTION
	<p>Choose the GPON interface that you want the settings configured here to apply to from the drop-down list.</p> <p>Configure the ONT registration settings and select the ONT Template Active checkbox for a GPON interface in the OLT Registration screen. You'll have GPON interfaces to choose from the drop-down list.</p>
ONT AID	<p>Select a template from the table below by clicking a hyperlink in the AID field.</p> <p>Note: It's required to put a value in this field.</p>
Active	<p>Select this to enable the ONT template.</p> <p>Note: It's required to enable or disable the ONT template in this field.</p>
Template Description	Enter a description to aid in identifying the template.
Alarm Profile	Select the alarm profile this template uses. Click Alarm Profile Setting to configure or edit an alarm profile.
Full Bridge	Select the Enable checkbox to have the ONT allow the traffic of all the four UNI (User Network Interface) ports once any one of them is configured.
Anti MAC Spoofing	Select the Enable checkbox to activate anti-MAC spoofing for the ONT.
FEC	Select this to enable the Forward Error Correction (FEC) feature. See Section 32.1.2 on page 255 for more information about FEC.
Plan Version	<p>Enter the ONT planned version of up to 14 characters to upgrade the ONT's firmware via OMCI.</p> <p>The planned version is the firmware ID of the firmware that you want the ONT to use.</p>
Option 82	See Table 85 on page 225 and Table 85 on page 225 for more information about DHCP/PPPoE options and DHCP/PPPoE passthrough.
Circuit ID	Enter a string of up to 63 ASCII characters that the OLT adds into the Circuit ID sub-option. Spaces are allowed.

Table 110 Advanced Application > ONT Template

LABEL	DESCRIPTION
Remote ID	Enter a string of up to 63 ASCII characters that the OLT adds into the Remote ID sub-option. Spaces are allowed.
Disable	Deselect DHCP to add DHCP options in outgoing packets. You can set up DHCP options in the Circuit ID and Remote ID fields. Deselect PPPoE to add PPPoE options in outgoing packets. You can set up DHCP options in the Circuit ID and Remote ID fields.
Pass Through	Select DHCP to forward packets with DHCP options from an ONT. Otherwise, they'll be dropped. Select PPPoE to forward packets with PPPoE options from an ONT. Otherwise, they'll be dropped.
UNI Port	
CardID 1 10_100_1000B ASET	Select this to have the Ethernet ports on an ONT, such as Zyxel's PMG1005, PMG1006, and PMG3000 ONT series to use 10 Mbps, 100 Mbps, or 1000 Mbps.
CardID 2 VEIP	Select this to use a virtual Ethernet card on a router mode ONT such as Zyxel's PMG53XX, and PMG56XX ONT series.
CardID 3 POTS	Select this to use a virtual VoIP card on an ONT such as Zyxel's PMG5317.
CardID 4 VIDEO	Select this to use a virtual video card on an ONT such as Zyxel's PMG5323.
CardID 5 10_100BASET	Select this to have the Ethernet ports on an ONT to use 10 Mbps or 100 Mbps.
CardID 6 10_100_1000B ASET_VEIP	Select this to have the Ethernet ports on an ONT, such as Zyxel's PMG1006 to use 10 Mbps, 100 Mbps, or 1000 Mbps, and use a virtual Ethernet card on a router mode ONT.
Uniport List	Enter the numbers of the ports on the ONT.
Speed	Select the auto detection configuration attribute in the physical path termination point. Use auto or a specific rate and duplex mode.
PMenable	Select DISABLE to disable pm (performance monitoring) on the virtual card type. Select 64-bit to enable PM (performance monitoring) to get 64-bit counters on this virtual card type by getting IP host performance monitoring history data ME as defined in G.988. Select 32-bit to enable PM (performance monitoring) to get 32-bit counters on this virtual card type by getting IP host performance monitoring history data ME as defined in G.984.4.
AID	This is the ONT's ID in the format: ont-<pon>-<ont>.
Active	This shows whether the ONT is enabled or disabled.
Template-Description	This displays the description to aid in identifying the template.
AlarmProfile	This displays the alarm profile this template uses.
FullBridge	This displays Y if you have the ONT allow the traffic of all the four UNI ports once any one of them is configured.
AntiMACSpoof	This displays Y if you have anti-MAC spoofing activated for the ONT.
FEC	This displays whether the Forward Error Correction (FEC) feature is enabled or not.
PlanVersion	This displays the ONT's plan version.
Ontcard ID	These are the virtual card ID numbers (1-16 possible) of the ONT.

Table 110 Advanced Application > ONT Template

LABEL	DESCRIPTION
Ontcard Type	This displays the ONT virtual card type. 10_100BASET: for Ethernet ports on an ONT such as Zyxel's PMG1006 to use 10 Mbps or 100 Mbps. VEIP: for a virtual Ethernet card on a router mode ONT such as Zyxel's PMG5318. POTS: for a virtual VoIP card on an ONT such as Zyxel's PMG5323-B20A. VDSL2: for VDSL ports on an MDU such as Zyxel's IES4005. 10_100_1000BASET: for Ethernet ports on an ONT such as Zyxel's PMG1006 to use 10 Mbps, 100 Mbps, or 1000 Mbps. VIDEO: for a virtual video card on an ONT such as Zyxel's PMG5323-B20A.
Uniport List	This displays the numbers of the ports on the ONT.
Speed	This displays the speed of the physical path termination point.
PMenable	This displays whether PM (performance monitoring) is enabled or not on the virtual card type.
Apply	Click Apply to save the changes.
Cancel	Click Cancel to begin configuring the screen again.

33.2.1 ONT Bandwidth Group

Use this screen to configure bandwidth group settings for ONTs. Click **ONT Bwgroup** in the **Advanced Application > ONT Template** screen to display the screen as shown.

Figure 161 Advanced Application > ONT Template > ONT Bwgroup

The following table describes the labels in this screen.

Table 111 Advanced Application > ONT Template > ONT Bwgroup

LABEL	DESCRIPTION
	Choose the GPON interface that you want the settings configured here to apply to from the first drop-down list.
	Choose the template that you want the settings configured here to apply to from the second drop-down list.
ID	Enter the bandwidth group ID number.
Ustype	This displays the upstream bandwidth group type the profile uses. The upstream bandwidth group type is selected automatically by the OLT after you select a bandwidth profile for the ONT's upstream traffic in the US BW Profile field.

Table 111 Advanced Application > ONT Template > ONT Bwgroup

LABEL	DESCRIPTION
US BW Profile	Select the bandwidth profile to apply to the ONT's upstream traffic. Click Bandwidth Profile Setting to display the settings of the bandwidth profiles.
DS BW Profile	Select the bandwidth profile to apply to the ONT's downstream traffic. Click Bandwidth Profile Setting to display the settings of the bandwidth profiles.
Add	Click Add to add an ONT Bwgroup entry.
Cancel	Click Cancel to clear the fields.
Clear	Click Clear to return the screen's settings to the defaults.
Index	This is the index number of an ONT bandwidth group.
AID	This is the ONT's ID in the format: ont-<pon>-<ont>.
ID	This displays the bandwidth group ID number.
USType	This displays the upstream bandwidth group type the ONT bandwidth group uses.
US BW Profile	This displays the bandwidth profile the ONT bandwidth group applies to the ONT's upstream traffic.
DS BW Profile	This displays the bandwidth profile the ONT bandwidth group applies to the ONT's downstream traffic.
Delete	Select this for one or more profiles and click Delete to remove them.
*	Use this row to select all of the profiles for deletion.
Delete	Click Delete to remove the profiles with the Delete option selected.
Cancel	Click Cancel to begin configuring the screen again.

33.2.2 Uniport Queue

Use this screen to configure QoS queues for the UNI (User Network Interface) ports. Click **Uniport Queue** in the **Advanced Application > ONT Template** screen to display the screen as shown.

Figure 162 Advanced Application > ONT Template > Uniport Queue

The following table describes the labels in this screen.

Table 112 Advanced Application > ONT Template > Uniport Queue

LABEL	DESCRIPTION
	Choose the GPON interface that you want the settings configured here to apply to from the first drop-down list.
	Choose the template that you want the settings configured here to apply to from the second drop-down list.
Active	Select this to have the settings configured here take effect.
Uniport AID	Select a UNI port on the ONT. The UNI ports are represented by the format: uniport-<pon>-<ont>-<card>-<port>.
TC	Select the QoS traffic class (0~7) of traffic to which this queue is applied.
Priority	Select the priority level of traffic (0~7) to which this queue is applied. At the time of writing, this field is not workable.
Weight	Specify the weight of traffic to which this queue is applied. At the time of writing, this field is not workable.
US BW Profile	Select the bandwidth profile to apply to the UNI port's upstream traffic. Click BW Profile Setting to display the settings of the bandwidth profiles.
DS BW Profile	Select the bandwidth profile to apply to the UNI port's downstream traffic. Click BW Profile Setting to display the settings of the bandwidth profiles.
DS Option	Select whether to apply the downstream rate limit function to the OLT (olt) or the ONT (ont).
BW Share Groupid	Select the IDs of the (already configured) bandwidth group on this ONT to put the upstream and downstream QoS queues into. You created the bandwidth group when you configured the ONT setup. The UNI port will share the bandwidth defined by the bandwidth group.
DS BW Share Groupid	Specify the ID (1-40) of the downstream bandwidth group on this ONT to put the QoS queues into. You created the bandwidth group when you configured the ONT setup. The UNI port will share the downstream bandwidth defined by the bandwidth group. The OLT uses the value in the BW Share Groupid field as the default value.
Add	Click Add to add a uniport queue entry.
Cancel	Click Cancel to clear the fields.
Clear	Click Clear to return the screen's settings to the defaults.
Index	This is the index number of a UNI port queue.
AID	This is the UNI port's ID in the format: uniport-<pon>-<ont>-<card>-<port>.
Active	This shows whether the uniport queue is enabled or disabled.
TC	This is the QoS traffic class (0~7) of traffic to which to apply this queue.
Priority	This is the priority level of traffic (0~7) to which to apply this queue.
Weight	This is the weight of traffic to which to apply this queue.
US BW Profile	This displays the bandwidth profile the UNI port queue applies to the UNI port's upstream traffic.
DS BW Profile	This displays the bandwidth profile the UNI port queue applies to the UNI port's downstream traffic.
DS Option	This shows whether the UNI port queue applies the downstream rate limit function to the OLT (olt) or the ONT (ont).
Bw Share Groupid (US/DS)	This displays the IDs of the (already configured) bandwidth group on this ONT to put the upstream and downstream QoS queues into.
Delete	Select this for one or more entries and click Delete to remove them.
*	Use this row to select all of the entries for deletion.

Table 112 Advanced Application > ONT Template > Uniport Queue (continued)

LABEL	DESCRIPTION
Delete	Click Delete to remove the entries with the Delete option selected.
Cancel	Click Cancel to begin configuring the screen again.

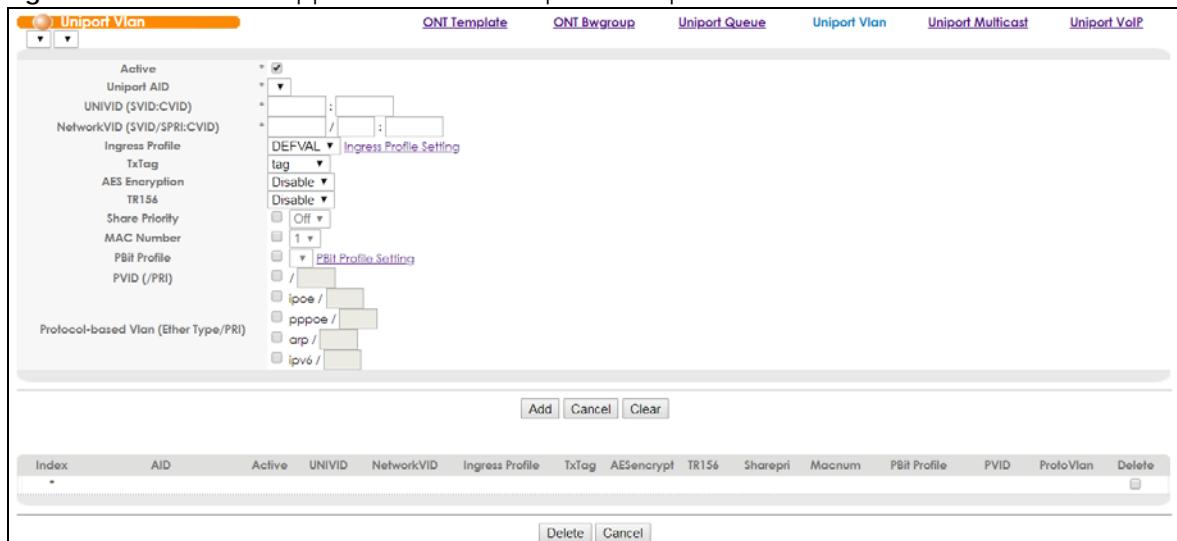
33.2.3 Uniport VLAN

Use this screen to configure UNI port VLAN flow settings. Click **Uniport VLAN** in the **Advanced Application > ONT Template** screen to display the screen as shown.

You can also use VLAN stacking on the OLT. See [Chapter 20 on page 165](#) for more information.

See [Section 6.5 on page 73](#) for tutorials on how to use VLAN stacking on ONTs.

Figure 163 Advanced Application > ONT Template > Uniport VLAN



The following table describes the labels in this screen.

Table 113 Advanced Application > ONT Template > Uniport VLAN

LABEL	DESCRIPTION
	Choose the GPON interface that you want the settings configured here to apply to from the first drop-down list.
	Choose the template that you want the settings configured here to apply to from the second drop-down list.
Active	Select this to enable the VLAN flow setting rule on the UNI port.
Uniport AID	Select a UNI port on the ONT. The UNI ports are represented by the format: uniport-<pon>-<ont>-<card>-<port>.
UNIVID (SVID:CVID)	Enter the UNI Service provider VLAN ID (SVID) and Customer VLAN ID (CVID) (1~4094) of traffic on the UNI port to which to apply the VLAN flow settings.

Table 113 Advanced Application > ONT Template > Uniport VLAN (continued)

LABEL	DESCRIPTION
NetworkVID (SVID/ SPRI:CVID)	<p>Enter the Network Node Interface (NNI) VIDs (1~4094) to which the ONT translates the UNI port VLAN ID before sending traffic to the OLT. Use a number different from the UNI port VLAN to apply VLAN translation.</p> <p>SVID: Service provider VLAN ID</p> <p>SPRI: Specify the IEEE 802.1p priority level (0-7) for the service provider tag. "0" is the lowest priority level and "7" is the highest.</p> <p>CVID: Customer VLAN ID</p>
Ingress Profile	Select the QoS ingress profile to apply to the VLAN's traffic (IEEE 802.1p priority bit to TC mapping profile). Click Ingress Profile Setting to view the details of the profiles.
TxTag	Sets whether the ONT sends downstream traffic with a VLAN tag (tag), a priority tag (priotag) or no tag (untag).
AES Encryption	Select Enable to enable gem port AES encryption.
TR156	Enable or disable TR156 mode. TR156 mode adds a VLAN tag based on the GEM tag of incoming upstream packets.
Share Priority	Select the share priority in a downstream share group. The value "off" means discard the downstream share group setting. If other VLANs have "0-7" set in the same downstream share group, the value cannot be set to "off". The priority value means the priority of VLAN of downstream rate limit and is unique in the same downstream bandwidth group. 7 has the highest priority.
MAC Number	<p>You can set the maximum number (1-6) of metered downstream MAC addresses per GEM port. Excess MAC addresses can transmit traffic without bandwidth metering.</p> <p>If the share priority in a downstream share group is not selected in the Share Priority field, there's no limitation of metered downstream MAC addresses per GEM port.</p>
PBit Profile	Select a priority bit profile to apply to this traffic class. Click Pbit Profile Setting to view the details of the profiles.
PVID (/PRI)	Select the priority level (0~7) to apply to the VLAN's traffic. Select None to not set a priority level tag value.
Protocol-based Vlan (Ether Type/ PRI)	<p>Use this section to apply the VLAN flow setting to specific protocols of packets. The system converts it to the corresponding Ethernet type as follows:</p> <p>IPoE packet ethertype = 0x0800</p> <p>PPPoE packet ethertype = 0x8863 , 0x8864</p> <p>ARP packet ethertype = 0x0806</p> <p>IPv6 packet ethertype = 0x86DD</p> <p>Select the priority bit the ONT inserts into the protocol packets.</p>
Add	Click Add to add a UNI port VLAN entry.
Cancel	Click Cancel to clear the fields.
Clear	Click Clear to return the screen's settings to the defaults.
Index	This is the index number of a UNI port VLAN flow setting.
AID	This is the UNI port's ID in the format: uniport-<pon>-<ont>-<card>-<port>.
Active	This displays whether the UNI port VLAN flow setting is active (Y) or not (N).
UNIVID	This displays the UNI SVID and CVID of traffic on the UNI port to which the VLAN flow settings apply.
NetworkVID	This displays the NNI VIDs to which the ONT translates the UNI port VLAN ID before sending traffic to the OLT.
Ingress Profile	This displays the QoS ingress profile the VLAN flow applies to the VLAN's traffic (IEEE 802.1p priority bit to TC mapping profile).

Table 113 Advanced Application > ONT Template > Uniport VLAN (continued)

LABEL	DESCRIPTION
TxTag	This display whether the ONT sends downstream traffic with a VLAN tag (tag) or untagged (untag) or priority tagged (priotag).
AESencrypt	This displays whether or not gem port AES encryption is enabled for the VLAN flow.
TR156	This displays whether TR156 mode is enabled or disabled. TR156 mode adds a VLAN tag based on the GEM tag of incoming upstream packets.
Sharepri	This displays the share priority in a downstream share group. The value "off" means discard the downstream share group setting.
MACMUM	This displays the maximum number of downstream traffic MAC addresses.
PBit Profile	This displays the priority bit profile the VLAN flow applies to this traffic class.
PVID	This displays the priority level (0~7) the VLAN flow applies to the VLAN's traffic. None means it does not set a priority level tag value.
ProtoVlan	This displays Y if the VLAN flow setting applies to specific protocols of packets.
Delete	Select this for one or more entries and click Delete to remove them.
*	Select this to select all of the entries for deletion.
Delete	Click Delete to remove the entries with the Delete option selected.
Cancel	Click Cancel to begin configuring the screen again.

33.2.4 Uniport Multicast

Use this screen to configure UNI port multicast subscriber channels. Click **Uniport Multicast** in the **Advanced Application > ONT Template** screen to display the screen as shown.

Figure 164 Advanced Application > ONT Template > Uniport Multicast

The following table describes the labels in this screen.

Table 114 Advanced Application > ONT Template > Uniport Multicast

LABEL	DESCRIPTION
	Choose the GPON interface that you want the settings configured here to apply to from the first drop-down list.
	Choose the template that you want the settings configured here to apply to from the second drop-down list.
Active	Select this to activate this multicast channel on the UNI port.
Uniport AID	Select a UNI port on the ONT. The UNI ports are represented by the format: uniport-<pon>-<ont>-<card>-<port>.
UNIVID	Select the VLAN ID of the multicast channel.
Version	Select the IGMP version for the multicast traffic transmission over this multicast channel, either igmpv2 or igmpv3 .
Cac Profile	Select a QoS CAC profile which contains multicast bandwidth settings. Click CAC Profile Setting to view the profile details.
Maxgroup	Enter the maximum number of multicast groups a client can join concurrently.
Maxmsg	Enter the maximum number of IGMP reports a client can send per second.
Singnalng on	Select this to enable the IGMP signaling mode. It lets the OLT control and decide the multicast table of the ONT. The ONT must also support this feature.
Previewpkg	<p>Configure a list of package members with preview privilege. That is, IGMP clients can join groups in these package members only in a period of time.</p> <p>You can enter individual packages separated by a comma or a range of packages by using a dash.</p> <p>Example:</p> <p>2, 4, 6 indicates that packages 2, 4 and 6 are the package members.</p> <p>2-6 indicates that packages 2 through 6 are the package members.</p> <p>Use the mcast-channel command to create the package members. The ONT must also support this feature.</p>
Fullviewpkg	<p>Configure a list of package members with full view privilege. That is, IGMP clients can join groups in these package members all the time. Use the mcast-channel command to create the package members.</p> <p>You can enter individual packages separated by a comma or a range of packages by using a dash.</p> <p>Example:</p> <p>2, 4, 6 indicates that packages 2, 4 and 6 are the package members.</p> <p>2-6 indicates that packages 2 through 6 are the package members.</p>
Tx-tag	<p>Select untag to not tag downstream multicast traffic.</p> <p>Select transparent to tag downstream multicast traffic according to the ONT VLAN TX tag setting.</p> <p>Select replace to replace the original VLAN with a specific VID. Enter the VID in the field to the right.</p>
Add	Click Add to add a UNI port multicast entry.
Cancel	Click Cancel to clear the fields.
Clear	Click Clear to return the screen's settings to the defaults.
Index	This is the index number of a UNI port multicast channel setting.
AID	This is the UNI port's ID in the format: uniport-<pon>-<ont>-<card>-<port>.

Table 114 Advanced Application > ONT Template > Uniport Multicast

LABEL	DESCRIPTION
Active	This displays whether the UNI port multicast channel setting is active (Y) or not (N).
UNIVID	This displays the VLAN ID of the multicast channel.
Rule	This displays the multicast channel settings.
Delete	Select this for one or more entries and click Delete to remove them.
*	Select this to select all of the entries for deletion.
Delete	Click Delete to remove the entries with the Delete option selected.
Cancel	Click Cancel to begin configuring the screen again.

33.2.5 Uniport VoIP

Use this screen to configure UNI port VoIP settings. Click **Uniport VoIP** in the **Advanced Application > ONT Template** screen to display the screen as shown.

Figure 165 Advanced Application > ONT Template > Uniport VoIP

Index	AID	Active	VID	Rule	Delete
*					<input type="checkbox"/>

The following table describes the labels in this screen.

Table 115 Advanced Application > ONT Template > Uniport VoIP

LABEL	DESCRIPTION
	Choose the GPON interface that you want the settings configured here to apply to from the first drop-down list.
	Choose the template that you want the settings configured here to apply to from the second drop-down list.
Active	Select this to activate the VoIP rule on the UNI port.
Uniport AID	Select a UNI port on the ONT. The UNI ports are represented by the format: uniport-<pon>-<ont>-<card>-<port>.
Vlan	Select the VLAN ID for the UNI port to use for VoIP traffic.
Common Profile	Select the VoIP common profile to have this VoIP rule apply. Click Voip-Common-Profile to view the profile details.

Table 115 Advanced Application > ONT Template > Uniport VoIP

LABEL	DESCRIPTION
Sip-profile	Select the SIP profile to apply to have this VoIP rule apply. Click Voip-Sip-Profile to view the profile details.
Username	Type 1 to 25 characters for the user name used for VoIP authentication.
Password	Type 1 to 25 printable characters for the password used for VoIP authentication.
Dial-plan	Select the dial plan profile to apply to this VoIP rule. Click Voip-Dial-Plan to view the profile details.
Aor	Type the user identification part of the address of record (from 1 to 63 characters).
Dispname	Type the customer ID (up to 25 characters) used for the display attribute in outgoing SIP messages.
Vmail-uri	Enter the IP address or URL (up to 63 characters) of the SIP voicemail server for signaling messages.
Vmail-extimer	Enter the voicemail subscription expiration time (from 0 to 3600 seconds).
Release-timer	Enter the release timer (from 0 to 30 seconds).
Roh-timer	Enter the time (from 0 to 30 seconds) for deciding the receiver is off hook.
Add	Click Add to add a UNI port VoIP entry.
Cancel	Click Cancel to clear the fields.
Clear	Click Clear to return the screen's settings to the defaults.
Index	This is the index number of a UNI port VoIP rule.
AID	This is the UNI port's ID in the format: uniport-<pon>-<ont>-<card>-<port>.
Active	This displays whether the VoIP rule is active (Y) or not (N).
VID	This displays the VLAN ID the UNI port uses for VoIP traffic.
Rule	This displays the VoIP rule settings for UNI ports.
Delete	Select this for one or more entries and click Delete to remove them.
*	Select this to select all of the entries for deletion.
Delete	Click Delete to remove the entries with the Delete option selected.
Cancel	Click Cancel to begin configuring the screen again.

CHAPTER 34

ONT Quick Setup

34.1 Overview

Use the **ONT Quick Setup** screens to create, modify, and delete an ONT configuration.

34.1.1 What You Can Do

- Use the **ONT Quick Setup** screen ([Section 34.2 on page 277](#)) to register an ONT to the OLT.
- Use the **ONT Status** screen ([Section 34.3 on page 279](#)) to display the ONT status.
- Use the **ONT Alarm** screen ([Section 34.4 on page 279](#)) to display the ONT alarms.
- Use the **ONT Bandwidth Group** screen ([Section 34.5 on page 281](#)) to display the ONT's bandwidth group settings.
- Use the **Unregistered ONT** screen ([Section 34.6 on page 282](#)) to display the unregistered ONTs connected to the GPON interface.
- Use the **ONT WAN** screen ([Section 34.7 on page 283](#)) to display the WAN information of the ONTs.

34.2 The ONT Quick Setup Screen

Use this screen to register an ONT to the OLT. Click **Advanced Application > ONT Quick Setup** in the navigation panel to display the screen as shown.

Note: For each GPON interface, there are up to 120 ONT IDs available for ONT registration
(The ONT IDs 121~128 are reserved for the ONT templates.)

Figure 166 Advanced Application > ONT Quick Setup

The screenshot shows the 'ONT Quick Setup' screen with the following details:

- Header:** Status, Alarm, Bwgroup, Unreg, Wan.
- Text:** Notice: Registration method D/E can only support ont auto provision. (Cannot modify SerialNumber/Password/Template)
- Table:** A grid for managing ONTs. Columns include: ONT AID, Active, Serial Number, Step, Password, Description, Template Description, Template, and Action. The table contains 32 rows, each with a unique ONT AID from -1 to -32.
- Buttons:** Apply, Cancel.
- Paging:** Prev, Next, p. 1 •

The following table describes the labels in this screen.

Table 116 Advanced Application > ONT Quick Setup

LABEL	DESCRIPTION
	Choose the GPON interface that you want the settings configured here to apply to from the drop-down list.
ONT AID	This is the identifier for the ONT connected to the selected GPON interface.
Active	Select this to have the OLT manage the ONT.
Serial Number	Enter the serial number of the ONT.
Step	Select this to arrange the list in numerical order according to the GPON serial numbers of the ONTs.
Password	Enter the GPON password of the ONT.
Description	Enter the description for the ONT.
Template Description	Enter the description to aid in identifying the template.
Template	Select an ONT template.
Action	Null: Select this to have the entry stay as it is. Add: Select this to add an entry. Modify: Select this to edit the entry. Delete: Select this to unregister the ONT.
Apply	Click Apply to save the changes.
Cancel	Click Cancel to begin configuring the screen again.
Paging	
Prev/Next	Click Prev or Next to show the previous/next screen if all status information cannot be seen in one screen.

34.3 The ONT Status Screen

Use this screen to view the ONT status. Click **Status** in the **Advanced Application > ONT Quick Setup** screen to display the screen as shown.

Figure 167 Advanced Application > ONT Quick Setup > Status



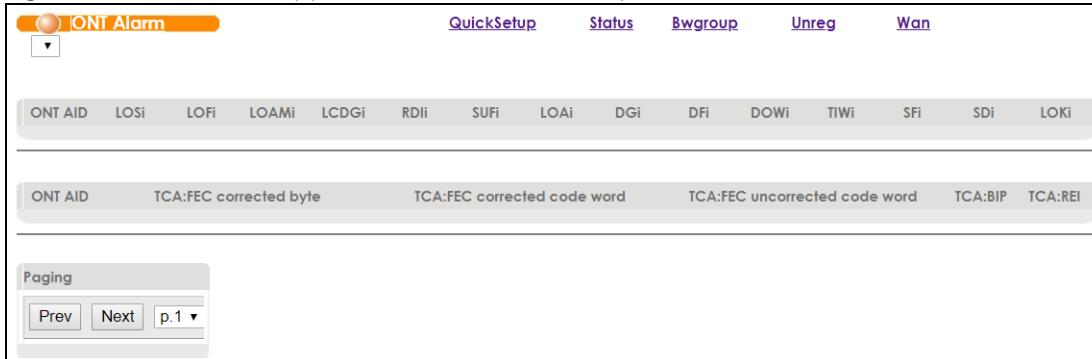
The following table describes the labels in this screen.

Table 117 Advanced Application > ONT Quick Setup > Status

LABEL	DESCRIPTION
	Choose the GPON interface to see the status of the ONT connected to it from the drop-down list.
ONT AID	This displays the ONT's ID in the format: ont-<pon>-<ont>.
Type	Config: This displays the configurations you've set up for the ONT. Actual: This displays the configurations the ONT is having.
Sn	This displays the GPON serial number of the ONT.
Password	This displays the GPON password of the ONT.
Status	This displays the registration status of the ONT, and whether it's active or not.
Image	This displays the index numbers of the firmware images.
Active	This displays which firmware image is in use.
Version	This displays the version numbers of the firmware images
Vendor/Model	This displays the vendor and models names of the ONT.
Paging	
Prev/Next	Click Prev or Next to show the previous/next screen if all status information cannot be seen in one screen.

34.4 The ONT Alarm Screen

Use this screen to display the ONT alarms. Click **Alarm** in the **Advanced Application > ONT Quick Setup** screen to display the screen as shown.

Figure 168 Advanced Application > ONT Quick Setup > Alarm

The following table describes the labels in this screen.

Table 118 Advanced Application > ONT Quick Setup > Alarm

LABEL	DESCRIPTION
	Choose the GPON interface to see the alarm status of the ONT connected to it from the drop-down list.
ONT AID	This displays the ONT's ID in the format: ont-<pon>-<ont>.
LOSi	This displays the LOSi (Loss of Signal for ONU) alarm status. The OLT will detect a LOSi alarm when it doesn't receive optical signals from an ONT.
LOFi	This displays the LOFi (Loss of Frame of ONU) alarm status. The OLT will detect a LOFi alarm when it received 4 consecutive invalid delimiters.
LOAMi	This displays the LOAMi (Loss of PLOAM of ONU) alarm status. The OLT will detect a LOAMi alarm when it fails to receive three consecutive PLOAM messages from an ONT after sending a PLOAMu request to the ONT.
LCDGi	This displays the LCDGi (Loss of GEM Channel Delineation) alarm status. The OLT will detect a LCDGi alarm when it fails to receive GEM fragment delineation of an ONT.
RDli	This displays the RDli (Remote Defect Indication of ONU) alarm status. The OLT will detect a RDli alarm when it transmits defected data to an ONT.
SUFi	This displays the SUFi (Start-up Failure of ONU) alarm status. The OLT will detect a SUFi alarm when an ONT fails to initiate the ranging process for two consecutive times.
LOAi	This displays the LOAi (Loss of Acknowledge with ONU) alarm status. The OLT will detect a LCDGi alarm when it doesn't receive an acknowledgment for upstream traffic from an ONT.
DGi	This displays the DGi (Receive Dying-gasp of ONU) alarm status. The OLT will detect a DGi alarm when it receives a dying gasp message from on ONT. A dying message is generated when the ONT loses power.
DFi	This displays the DFi (Deactivate Failure of ONU) alarm status. The OLT will detect a DFi alarm when an ONT doesn't react correctly after the OLT sends the messages in the parentheses for three times (Deactivate_ONU-ID and Disable_Serial_Number).
DOWi	To avoid frequent updates on an equalization delay, two thresholds, the lower and upper thresholds, are needed. The lower threshold sets a limit to the transmission deviation that is allowed. A new equalization delay will be calculated when the old one exceeds the lower threshold. When an equalization delay exceeds the upper threshold, it means an ONT doesn't respond to the equalization delay correction commands. An ONT will be disabled when this happens. This displays the DOWi (Drift of Window of ONU) alarm status. The OLT will detect a DOWi alarm when the equalization delay of an ONT exceeds the lower threshold.

Table 118 Advanced Application > ONT Quick Setup > Alarm

LABEL	DESCRIPTION
TIWi	To avoid frequent updates on an equalization delay, two thresholds, the lower and upper thresholds, are needed. The lower threshold sets a limit to the transmission deviation that is allowed. A new equalization delay will be calculated when the old one exceeds the lower threshold. When an equalization delay exceeds the upper threshold, it means an ONT doesn't respond to the equalization delay correction commands. An ONT will be disabled when this happens. This displays the TIWi (Transmission Interference Warning) alarm status. The OLT will detect a TIWi alarm when the equalization delay of an ONT exceeds the upper threshold.
SFi	This displays the SFi (Signal Fail of ONUi) alarm status. The OLT will detect a SFi alarm when the upstream BER (Bit Error Rate) of an ONT exceeds the default value.
SDi	This displays the SDi (Signal Degraded of ONUi) alarm status. The OLT will detect a SDi alarm when the upstream BER (Bit Error Rate) of an ONT exceeds the default value.
LOKi	This displays the LOKi (Loss of Key Synch with ONUi) alarm status. The OLT will detect a LOKi alarm when an ONT fails to respond to the key exchange initiated by the OLT for three consecutive times.
ONT AID	This displays the ONT's ID in the format: ont-<pon>-<ont>.
TCA:FEC corrected byte	This displays the number of bytes that is corrected by Forward Error Correction (FEC).
TCA:FEC corrected code word	This displays the number of codewords that is corrected by Forward Error Correction (FEC).
TCA:FEC uncorrected code word	This displays the number of codewords that haven't been corrected by Forward Error Correction (FEC).
TCA:BIP	This displays the number of the interleaved parity of the received bytes.
TCA:REI	This displays the number of BIP (bit interleaved parity) errors that are detected during the BER interval.
Paging	
Prev/Next	Click Prev or Next to show the previous/next screen if all status information cannot be seen in one screen.

34.5 The ONT Bandwidth Group Screen

Use this screen to display the ONT's bandwidth group settings. Click **Bwgroup** in the **Advanced Application > ONT Quick Setup** screen to display the screen as shown.

Figure 169 Advanced Application > ONT Quick Setup > Bwgroup

ONT AID	ID	Status	Upstream	Downstream
<div style="display: flex; justify-content: space-between;"> Paging Prev Next p.1 ▾ </div>				

The following table describes the labels in this screen.

Table 119 Advanced Application > ONT Quick Setup > Bwgroup

LABEL	DESCRIPTION
	Choose the GPON interface to see the maximum upstream and downstream bandwidth of the ONT connected to it from the drop-down list.
ONT AID	This displays the ONT's ID in the format: ont-<pon>-<ont>.
ID	This displays the bandwidth group ID number.
Status	This displays the registration status of the ONT, and whether it's active or not.
Upstream	This displays the maximum bandwidth allowed in kilobits per second (Kbps) for the out-going traffic flow on an ONT.
Downstream	This displays the maximum bandwidth allowed in kilobits per second (Kbps) for the incoming traffic flow on an ONT.
Paging	
Prev/Next	Click Prev or Next to show the previous/next screen if all status information cannot be seen in one screen.

34.6 The Unregistered ONT Screen

Use this screen to display the unregistered ONTs connected to the GPON interface. Click **Unreg** in the **Advanced Application > ONT Quick Setup** screen to display the screen as shown.

Figure 170 GPON > ONT Quick Setup > Unreg

The screenshot shows the 'ONT Unreg' screen with the following details:

- Header:** ONT Unreg, with tabs for Quick Setup, Status, Alarm, Bwgroup, and Wan.
- Table Headers:** Index, ONT ID, SN, Password, Status, Template, Register.
- Table Data:** A single row is visible with values Null, Null, Null, Null, Null, Null, Null.
- Buttons:** Apply, Cancel.
- Paging:** Prev, Next, p.1.

The following table describes the labels in this screen.

Table 120 Advanced Application > ONT Quick Setup > Unreg

LABEL	DESCRIPTION
	Choose the GPON interface to show the unregistered ONTs connected to it from the drop-down list.
Index	This is the index number of an unregistered ONT.
ONT ID	This is the identifier of an ONT.
SN	This displays the GPON serial number of the unregistered ONT.
Password	This displays the GPON password of the unregistered ONT.
Status	This displays the registration status of the ONT.
Template	This displays the template that the unregistered ONT uses.
Register	Select this to register the ONT.

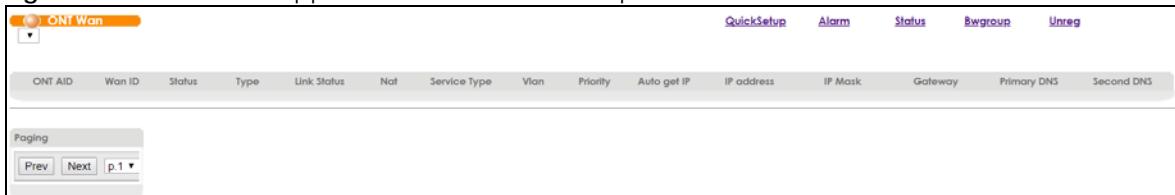
Table 120 Advanced Application > ONT Quick Setup > Unreg

LABEL	DESCRIPTION
Apply	Click Apply to save the changes.
Cancel	Click Cancel to begin configuring the screen again.
Paging	
Prev/Next	Click Prev or Next to show the previous/next screen if all status information cannot be seen in one screen.

34.7 The ONT WAN Screen

Use this screen to display the WAN information of the ONTs. Click **Wan** in the **Advanced Application > ONT Quick Setup** screen to display the screen as shown.

Figure 171 Advanced Application > ONT Quick Setup > Wan



The following table describes the labels in this screen.

Table 121 Advanced Application > ONT Quick Setup > Wan

LABEL	DESCRIPTION
	This is the identifier for the GPON interface.
ONT AID	This field displays the ONT's ID in the format: ont-<pon>-<ont>.
Wan ID	This field displays the WAN interface ID of the ONT.
Status	This field displays whether the WAN interface is active or not.
Type	This field displays the WAN encapsulation method.
Link Status	This field displays whether the WAN connection is up or down.
Nat	This field displays whether NAT is enabled or not on the ONT.
Service Type	This field displays the current encapsulation method.
Vlan	This field displays the VLAN group that the ONT belongs to.
Priority	This field displays the priority level of the VLAN group.
Auto get IP	This field displays whether the ONT is using a DHCP IP address or a static IP address. Enable - The WAN interface can obtain an IP address from a DHCP server. Disable - The WAN interface is using a static IP address.
IP address	This field displays the current IP address of the ONT in the WAN.
IP Mask	This field displays the current subnet mask in the WAN.
Gateway	This field displays the IP address of the default gateway.
Primary DNS	This field displays the first DNS server address assigned by the ISP.
Second DNS	This field displays the second DNS server address assigned by the ISP.

Table 121 Advanced Application > ONT Quick Setup > Wan

LABEL	DESCRIPTION
Paging	
Prev/Next	Click Prev or Next to show the previous/next screen if all status information cannot be seen in one screen.

CHAPTER 35

Static Route

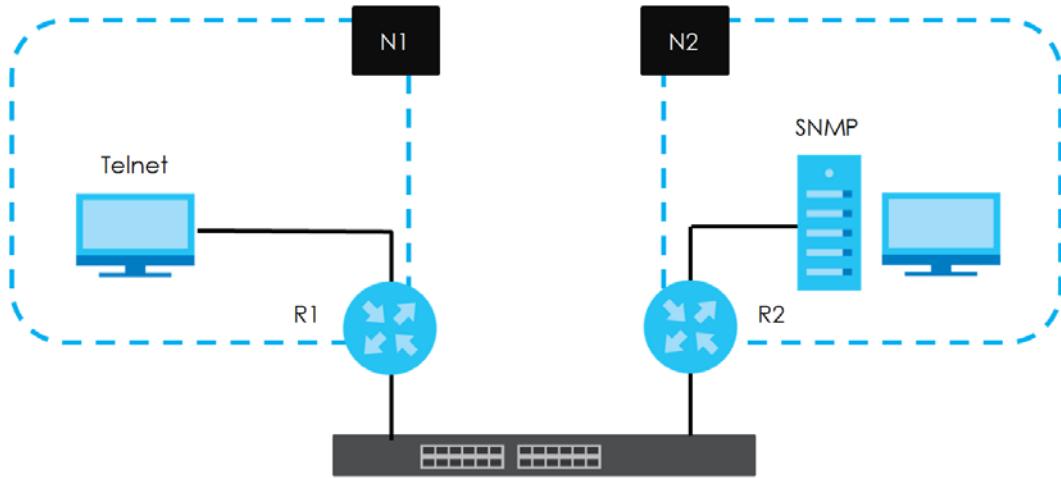
35.1 Static Routing Overview

This chapter shows you how to configure static routes.

The OLT uses IP for communication with management computers, for example using HTTP, Telnet, SSH, or SNMP. Use IP static routes to have the OLT respond to remote management stations that are not reachable through the default gateway. The OLT 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.

This figure shows a **Telnet** session coming in from network **N1**. The OLT sends reply traffic to default gateway **R1** which routes it back to the manager's computer. The OLT needs a static route to tell it to use router **R2** to send traffic to an SNMP trap server on network **N2**.

Figure 172 Static Routing Overview



35.1.1 What You Can Do

- Use the **Static Routing** screen ([Section 35.2 on page 285](#)) to configure and enable an IPv4 static route.

35.2 Static Routing

Use this screen to configure and enable an IPv4 static route. Click **IP Application > Static Routing** in the navigation panel to display the screen as shown.

Figure 173 IP Application > Static Routing

Index	Active	Name	Destination Address	Subnet Mask	Gateway Address	Metric	Delete
	<input type="checkbox"/>						<input type="button" value="Delete"/>
							<input type="button" value="Cancel"/>

The following table describes the related labels you use to create a static route.

Table 122 IP Application > Static Routing

LABEL	DESCRIPTION
Active	This field allows you to activate/deactivate this static route.
Name	Enter a descriptive name (up to 10 printable ASCII characters) for identification purposes.
Destination IP Address	This parameter specifies the IP network address of the final destination.
IP Subnet Mask	Enter the subnet mask for this destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your OLT that will forward the packet to the destination. The gateway must be a router on the same segment as your OLT.
Metric	The metric represents the "cost" of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Add	Click Add to insert a new static route to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the above fields to your previous configuration.
Clear	Click Clear to set the above fields back to the factory defaults.
Index	This field displays the index number of the route. Click a number to edit the static route entry.
Active	This field displays Yes when the static route is activated and NO when it is deactivated.
Name	This field displays the descriptive name for this route. This is for identification purposes only.
Destination Address	This field displays the IP network address of the final destination.
Subnet Mask	This field displays the subnet mask for this destination.
Gateway Address	This field displays the IP address of the gateway. The gateway is an immediate neighbor of your OLT that will forward the packet to the destination.

Table 122 IP Application > Static Routing

LABEL	DESCRIPTION
Metric	This field displays the cost of transmission for routing purposes.
Delete	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the check boxes.

CHAPTER 36

DHCP

36.1 DHCP Overview

This chapter shows you how to configure the DHCP feature.

DHCP (Dynamic Host Configuration Protocol RFC 2131 and RFC 2132) allows individual computers to obtain TCP/IP configuration at start-up from a server. If you configure the OLT as a DHCP relay agent, then the OLT forwards DHCP requests to DHCP server on your network. If you don't configure the OLT as a DHCP relay agent then you must have a DHCP server in the broadcast domain of the client computers or else the client computers must be configured manually.

36.1.1 What You Can Do

- Use the **DHCP Status** screen ([Section 36.2 on page 289](#)) to display the relay mode.
- Use the **DHCP Relay** screen ([Section 36.3 on page 291](#)) to enable and configure global DHCPv4 relay.
- Use the **VLAN Setting** screen ([Section 36.4 on page 294](#)) to configure your DHCPv4 settings based on the VLAN domain of the DHCPv4 clients.
- Use the **DHCP L2 Agent** screen ([Section 36.5 on page 295](#)) to configure the DHCP relay agent information and Lightweight DHCPv6 Relay Agent (LDRA) settings.
- Use the **ONT Option** screen ([Section 36.6 on page 299](#)) to configure whether to have the OLT add DHCP options for outgoing packets, and forward packets with DHCP options.

36.1.2 What You Need to Know

Read on for concepts on DHCP that can help you configure the screens in this chapter.

DHCP Modes

If there is already a DHCP server on your network, then you can configure the OLT as a DHCP relay agent. When the OLT receives a request from a computer on your network, it contacts the DHCP server for the necessary IP information, and then relays the assigned information back to the computer.

DHCPv4 Configuration Options

The DHCPv4 configuration on the OLT is divided into **Global** and **VLAN** screens. The screen you should use for configuration depends on the DHCP services you want to offer the DHCP clients on your network. Choose the configuration screen based on the following criteria:

- **Global** - The OLT forwards all DHCP requests to the same DHCP server.

- **VLAN** - The OLT is configured on a VLAN by VLAN basis. The OLT can be configured to relay DHCP requests to different DHCP servers for clients in different VLAN.

36.2 DHCP Status

Click **IP Application > DHCP** in the navigation panel. The **DHCP Status** screen displays.

Figure 174 IP Application > DHCP

	DHCP Status	Global	VLAN	Option
Server Status				
Index	VID	Server Status	IP Pool Size	
1	2	1.0.1.1	2048	
Relay Status				
Relay Mode	None			

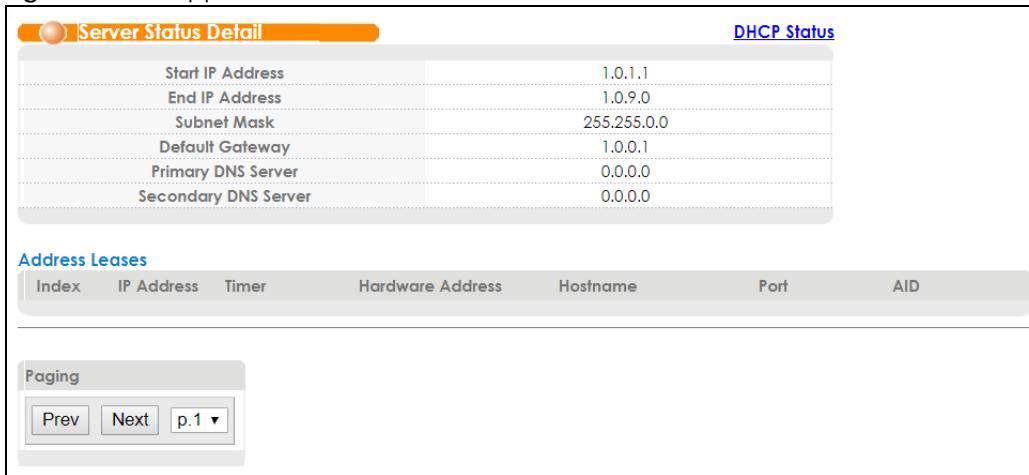
The following table describes the labels in this screen.

Table 123 IP Application > DHCP

LABEL	DESCRIPTION
Server Status	
Index	This field displays the index number.
VID	This field displays the VLAN ID number.
Server Status	For DHCP server configuration, this field displays the starting IP address. For DHCP relay configuration, this field displays the first remote DHCP server IP address.
IP Pool Size	This field displays the size of the IP address pool.
Relay Status	This section displays configuration settings related to the OLT's DHCP relay mode.
Relay Mode	This field displays: None - if the OLT is not configured as a DHCP relay agent. Global - if the OLT is configured as a DHCP relay agent only. VLAN - followed by a VLAN ID or multiple VLAN IDs if it is configured as a relay agent for specific VLAN(s).

36.2.1 DHCP Status Detail

Use this screen to view DHCP status details. Click a number in the **Index** column in the **DHCP** screen to display the screen as shown next.

Figure 175 IP Application > DHCP > DHCP Status Details

The following table describes the labels in this screen.

Table 124 IP Application > DHCP > DHCP Status Details

LABEL	DESCRIPTION
Start IP Address	This field displays the starting IP address of the IP address pool configured for this DHCP server instance.
End IP Address	This field displays the last IP address of the IP address pool configured for this DHCP server instance.
Subnet Mask	This field displays the subnet mask value sent to clients from this DHCP server instance.
Default Gateway	This field displays the default gateway value sent to clients from this DHCP server instance.
Primary DNS Server	This field displays the primary DNS server value sent to clients from this DHCP server instance.
Secondary DNS Server	This field displays the secondary DNS server value sent to clients from this DHCP server instance.
Address Leases	
Index	This field displays a sequential number for each DHCP request handled by the OLT.
IP Address	This is the IP address issued to a DHCP client.
Timer	This field displays the time remaining before the DHCP client has to renew its IP address.
Hardware Address	This field displays the MAC address of the DHCP client. It may also display SELF OCCUPIED ADDRESS if the IP address cannot be used for DHCP because it is already assigned to the OLT itself.
Hostname	This field displays the system name of the client.
Port	This field displays the GPON interface that the DHCP client is connected to.
AID	This displays the ONT's ID in the format: ont-<slot>-<pon>-<ont>.
Paging	
Prev/Next	Click Prev or Next to show the previous/next screen if all status information cannot be seen in one screen.

36.3 DHCPv4 Relay

Configure DHCP relay on the OLT if the DHCP clients and the DHCP server are not in the same broadcast domain. During the initial IP address leasing, the OLT helps to relay network information (such as the IP address and subnet mask) between a DHCP client and a DHCP server. Once the DHCP client obtains an IP address and can connect to the network, network information renewal is done between the DHCP client and the DHCP server without the help of the OLT.

The OLT can be configured as a global DHCP relay. This means that the OLT forwards all DHCP requests from all domains to the same DHCP server. You can also configure the OLT to relay DHCP information based on the VLAN membership of the DHCP clients.

36.3.1 DHCPv4 Relay Agent Information

The OLT can add information about the source of client DHCP requests that it relays to a DHCP server by adding **Relay Agent Information**. This helps provide authentication about the source of the requests. The DHCP server can then provide an IP address based on this information. Please refer to RFC 3046 for more details.

The DHCP **Relay Agent Information** feature adds an Agent Information field (also known as the **Option 82** field) to DHCP requests. The **Option 82** field is in the DHCP headers of client DHCP request frames that the OLT relays to a DHCP server.

36.3.1.1 DHCPv4 Relay Agent Information Format

A DHCP Relay Agent Information option has the following format.

Table 125 DHCP Relay Agent Information Option Format

Code (82)	Length (N)	i1	i2	...	iN
--------------	---------------	----	----	-----	----

i1, i2 and iN are DHCP relay agent sub-options, which contain additional information about the DHCP client. You need to define at least one sub-option.

36.3.1.2 Sub-Option Format

There are two types of sub-option: “Agent Circuit ID Sub-option” and “Agent Remote ID Sub-option”. They have the following formats.

Table 126 DHCP Relay Agent Circuit ID Sub-option Format

SubOpt Code	Length	Value
1 (1 byte)	N (1 byte)	String

Table 127 DHCP Relay Agent Remote ID Sub-option Format

SubOpt Code	Length	Value
2 (1 byte)	N (1 byte)	String

The 1 in the first field identifies this as an Agent Circuit ID sub-option and 2 identifies this as an Agent Remote ID sub-option. The next field specifies the length of the field.

36.3.2 Configuring DHCPv4 Global Relay

Use this screen to configure global DHCPv4 relay. Click **IP Application > DHCP >** in the navigation panel and click the **Global** link to display the screen as shown.

See [Section 23.10.1.4 on page 210](#) for more information about the configuration order for DHCP option 82 settings in different screens.

Figure 176 IP Application > DHCP > Global

The following table describes the labels in this screen.

Table 128 IP Application > DHCP > Global

LABEL	DESCRIPTION
Active	Select this check box to enable DHCPv4 relay.
Remote DHCP Server 1 .. 3	Enter the IP address of a DHCPv4 server in dotted decimal notation.
Relay Agent Information	<p>Select the Option 82 checkbox to have the OLT add the following information to client DHCP requests that relays to a DHCP server.</p> <p>The OLT will perform the following actions when the Option 82 checkbox is selected:</p> <ul style="list-style-type: none"> • The Port ID and VLAN ID of the DHCP client are added in the Circuit ID sub-option for DHCP packets. • The MAC address of the DHCP client is added in the Remote ID sub-option for DHCP packets.
Format	<p>Select the Format checkbox to have the OLT add the following information to client DHCP requests that relays to a DHCP server.</p> <p>The following information will be added in the Circuit ID sub-option for DHCP packets when the Format checkbox is selected:</p> <p>SystemName /PortID:NNISVLAN.SNISVLAN ONTID/ONTSerialNumber</p> <p>Example: OLTLAB /1:1000.1000 10/5A59584535044326</p>
Information	<p>Select the Information checkbox to add this name into the client DHCP requests.</p> <p>The system name of the OLT will be added in the Circuit ID sub-option for DHCP packets when both of the Option 82 and Information checkboxes are selected. Note that the system name is added after Port ID and VLAN id in the Circuit ID sub-option for DHCP packets.</p> <p>You can configure the system name in the Basic Settings > General Setup screen.</p>

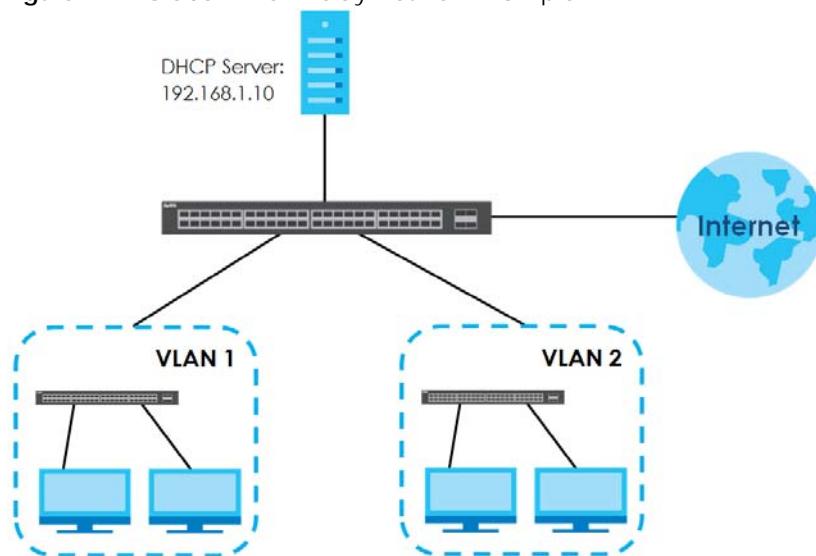
Table 128 IP Application > DHCP > Global (continued)

LABEL	DESCRIPTION
Apply	Click Apply to save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

36.3.3 Global DHCP Relay Configuration Example

The follow figure shows a network example where the OLT is used to relay DHCP requests for the **VLAN1** and **VLAN2** domains. There is only one DHCP server that services the DHCP clients in both domains.

Figure 177 Global DHCP Relay Network Example



Configure the **DHCP Relay** screen as shown. Make sure you select a DHCP option 82 profile (**default1** in this example) to set the OLT to send additional information (such as the VLAN ID) together with the DHCP requests to the DHCP server. This allows the DHCP server to assign the appropriate IP address according to the VLAN ID.

Figure 178 DHCP Relay Configuration Example

DHCP Relay		Status
Active		<input checked="" type="checkbox"/>
Remote DHCP Server 1	192.168.1.100	
Remote DHCP Server 2	0.0.0.0	
Remote DHCP Server 3	0.0.0.0	
Relay Agent Information		<input checked="" type="checkbox"/> Option 82
Format	<input type="checkbox"/> Format	<input type="checkbox"/> Format
Information	OLT1404A	
EXAMPLE		
Apply Cancel		

36.4 Configuring DHCP VLAN Settings

Use this screen to configure your DHCP settings based on the VLAN domain of the DHCP clients. Click **IP Application > DHCP** in the navigation panel, then click the **VLAN** link in the **DHCP Status** screen that displays.

See [Section 23.10.1.4 on page 210](#) for more information about the configuration order for DHCP option 82 settings in different screens.

Note: You must set up a management IP address for each VLAN that you want to configure DHCP settings for on the OLT. See [Section 5.2 on page 61](#) for information on how to do this.

Figure 179 IP Application > DHCP > VLAN

VID	Type	DHCP Status	Delete
2	Server	1.0.1.1/2048	<input type="button" value="Delete"/>

The following table describes the labels in this screen.

Table 129 IP Application > DHCP > VLAN

LABEL	DESCRIPTION
VID	Enter the ID number of the VLAN to which these DHCP settings apply.
DHCP Status	Select Server to have the OLT act as a DHCP server. Select Relay to have the OLT forward DHCP requests to the DHCP server.
Server	

Table 129 IP Application > DHCP > VLAN (continued)

LABEL	DESCRIPTION
Client IP Pool Starting Address	Specify the first of the contiguous addresses in the IP address pool.
Size of Client IP Pool	Specify the size of the IP address pool.
IP Subnet Mask	Type the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default).
Default Gateway	Enter the default gateway of the OLT.
Primary/Secondary DNS Server	Enter the primary/secondary DNS server IP address for the OLT.
Relay	Use this section if you want to configure the OLT to function as a DHCP relay for this VLAN.
Remote DHCP Server 1 .. 3	Enter the IP address of a DHCP server in dotted decimal notation.
Relay Agent Information	Select Option 82 to have the OLT add information (slot number, port number and VLAN ID) and the Circuit ID and Remote ID sub-options to client DHCP requests that it relays to a DHCP server.
Format	Select this to have the OLT use the default Circuit ID format for DHCP packets.
Information	Enter a string of up to 32 ASCII or binary characters that the OLT adds into the client DHCP requests. Spaces are allowed. Otherwise, use the system name you configure in the General Setup screen.
Add	Click this to create a new entry or to update an existing one. This saves your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Clear	Click Clear to reset the fields to the factory defaults.
VID	This field displays the ID number of the VLAN group to which this DHCP settings apply.
Type	This field displays Server or Relay for the DHCP mode.
DHCP Status	For DHCP server configuration, this field displays the starting IP address and the size of the IP address pool. For DHCP relay configuration, this field displays the first remote DHCP server IP address.
Delete	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Select the configuration entries you want to remove and click Delete to remove them.
Cancel	Click Cancel to clear the check boxes.

36.5 DHCP L2 Agent

Use this screen to configure the DHCP relay agent information and Lightweight DHCPv6 Relay Agent (LDRA) settings. Click **IP Application** > **DHCP** in the navigation panel, then click the **Option** link In the **DHCP Status** screen that displays.

See [Section 23.10.1.4 on page 210](#) for more information about the configuration order for DHCP option 82 settings in different screens.

Figure 180 IP Application > DHCP > Option

DHCP L2 Agent		Status	Global	VLAN	Option	ONT Option
VID	<input type="text"/>					
Option 82 Circuit Id	<input type="text"/>					
Option 82 Remote Id	<input type="text"/>					
Option 18 Interface Id	<input type="text"/>					
Option 37 Remote Id	<input type="text"/>					
LDRA ENABLE	<input checked="" type="checkbox"/>					
<input type="button" value="Add"/> <input type="button" value="Cancel"/> <input type="button" value="Clear"/>						
VID	Option 82 Circuit Id	Option 82 Remote Id	Option 18 Interface Id	Option 37 Remote Id	LDRA	Delete
<input type="button" value="Delete"/> <input type="button" value="Cancel"/>						

The following table describes the labels in this screen.

Table 130 IP Application > DHCP > Option

LABEL	DESCRIPTION
VID	Enter a VLAN ID (between 1 and 4094) to be served with DHCPv6 LDRA. Make sure the VLAN ID exists before you configure a DHCPv6 LDRA entry.
Option 82 Circuit Id	<p>Specify up to 127 ASCII characters of option 82 Circuit ID information for the OLT to add to the DHCP requests that it relays to a DHCP server. Spaces are allowed.</p> <p>This string should be composed of the following special characters. The special characters listed in the brackets [~!@#\$^&*()] are not allowed except % and space.</p> <ul style="list-style-type: none"> • %%: character % • %space: character space • %mac: client source mac • %hname: host device name • %pid: pon port index • %oid: ONT index • %ocid: ONT card index • %upid: uniport index • %nnisvlan: SVLAN ID on network-network interface • %snsisvlan: SVLAN ID on service-network interface • %snicvlan: CVLAN ID on service-network interface • %sn: serial number of a remote ONT • %ontname: will be translated into ONT model name • %ontdesc: will be translated into ONT description • %ontpasswd: will be translated into ONT password <p>Note: If the string is composed of more than 127 characters, the string will be truncated to the maximum number of characters allowed when the OLT transforms the string into the Circuit ID.</p>

Table 130 IP Application > DHCP > Option

LABEL	DESCRIPTION
Option 82 Remote Id	<p>Specify up to 95 ASCII characters of option 82 Remote ID information for the OLT to add to the DHCP requests that it relays to a DHCP server. Spaces are allowed.</p> <p>This string should be composed of the following special characters. The special characters listed in the brackets [~`!@#\$^&*()] are not allowed except % and space.</p> <ul style="list-style-type: none"> • %%: character % • %space: character space • %mac: client source mac • %hname: host device name • %pid: pon port index • %oid: ONT index • %ocid: ONT card index • %upid: uniport index • %nnisvlan: SVLAN ID on network-network interface • %snisvlan: SVLAN ID on service-network interface • %snicvlan: CVLAN ID on service-network interface • %sn: serial number of a remote ONT • %ontname: will be translated into ONT model name • %ontdesc: will be translated into ONT description • %ontpasswd: will be translated into ONT password <p>Note: If the string is composed of more than 95 characters, the string will be truncated to the maximum number of characters allowed when the OLT transforms the string into the Remote ID.</p>
Option 18 Interface Id	<p>Option 18 is required for LDRA. Select LDRA Enable and specify up to 127 ASCII characters for the OLT to add to the interface ID sub-option. Spaces are allowed.</p> <p>This string should be composed of the following special characters. The special characters listed in the brackets [~`!@#\$^&*()] are not allowed except % and space.</p> <ul style="list-style-type: none"> • %%: character % • %space: character space • %mac: client source mac • %hname: host device name • %pid: pon port index • %oid: ONT index • %ocid: ONT card index • %upid: uniport index • %nnisvlan: SVLAN ID on network-network interface • %snisvlan: SVLAN ID on service-network interface • %snicvlan: CVLAN ID on service-network interface • %sn: serial number of a remote ONT • %ontname: will be translated into ONT model name • %ontdesc: will be translated into ONT description • %ontpasswd: will be translated into ONT password <p>Note: If the string is composed of more than 127 characters, the string will be truncated to the maximum number of characters allowed when the OLT transforms the string into the Interface ID.</p>

Table 130 IP Application > DHCP > Option

LABEL	DESCRIPTION
Option 37 Remote Id	<p>Option 37 (Remote ID Info) is the DHCPv6 equivalent for the Dynamic Host Configuration Protocol for IPv4 (DHCPv4) Relay Agent Option's Remote-ID sub-option.</p> <p>Select LDRA Enable and specify up to 95 ASCII characters for the OLT to add to the Remote ID sub-option. Spaces are allowed.</p> <p>This string should be composed of the following special characters. The special characters listed in the brackets [~!@#\$^&*()] are not allowed except % and space.</p> <ul style="list-style-type: none"> • %%: character % • %space: character space • %mac: client source mac • %hname: host device name • %pid: pon port index • %oid: ONT index • %ocid: ONT card index • %upid: uniport index • %nnisvlan: SVLAN ID on network-network interface • %snsvlan: SVLAN ID on service-network interface • %snicvlan: CVLAN ID on service-network interface • %sn: serial number of a remote ONT • %ontname: will be translated into ONT model name • %ontdesc: will be translated into ONT description • %ontpasswd: will be translated into ONT password <p>Note: If the string is composed of more than 95 characters, the string will be truncated to the maximum number of characters allowed when the OLT transforms the string into the Remote ID.</p>
LDRA ENABLE	Lightweight DHCPv6 Relay Agent (LDRA) adds information to client DHCPv6 requests before forwarding them to the DHCPv6 server. Select Enable to add information such as this system's host name and subscriber port from which the request was received. Clear Enable to have the system forward DHCPv6 requests for this VLAN without adding information.
Add	<p>Click this to create a new entry or to update an existing one.</p> <p>This saves your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.</p>
Cancel	Click Cancel to begin configuring this screen afresh.
Clear	Click Clear to reset the fields to the factory defaults.
VID	This field displays the ID number of the VLAN group to which this DHCP settings apply.
Option 82 Circuit Id	This field displays the option 82 Circuit ID information that is added in DHCP packets.
Option 82 Remote Id	This field displays the option 82 Remote ID information that is added in DHCP packets.
Option 18 Interface Id	This field displays the option 18 (Interface ID) information to add to the client DHCPv6 requests forwarded for this VLAN to identify the interface which received the client message.
Option 37 Remote Id	This field displays the option 37 (Remote ID) information to add to the client DHCPv6 requests forwarded for this VLAN.
LDRA	This field displays whether LDRA is enabled or not on this VLAN.
Delete	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Select the configuration entries you want to remove and click Delete to remove them.
Cancel	Click Cancel to clear the check boxes.

36.6 ONT Option

Use this screen to have:

- The OLT adds DHCP options in the outgoing packets.
- The OLT drops/forwards the incoming packets with DHCP options from an ONT.

See [Table 131 on page 299](#) for more information.

Table 131 DHCP Options

DHCP OPTION82 RULE	DHCP OPTION	DHCP PASS THROUGH	ACTION
Not Configured	Disabled/Enabled	Disabled	<ul style="list-style-type: none"> The OLT won't add DHCP options in the outgoing packets. The OLT drops the incoming packets with DHCP options from an ONT
Not Configured	Disabled/Enabled	Enabled	<ul style="list-style-type: none"> The OLT won't add DHCP options in the outgoing packets. The OLT forwards the incoming packets with DHCP options from an ONT
Configured	Enabled	Disabled	<ul style="list-style-type: none"> The OLT adds DHCP options in the outgoing packets. The OLT drops the incoming packets with DHCP options from an ONT
Configured	Disabled	Disabled	<ul style="list-style-type: none"> The OLT won't add DHCP options in the outgoing packets. The OLT drops the incoming packets with DHCP options from an ONT
Configured	Enabled	Enabled	<ul style="list-style-type: none"> The OLT adds DHCP options in the outgoing packets. The OLT forwards the incoming packets with DHCP options from an ONT
Configured	Disabled	Enabled	<ul style="list-style-type: none"> The OLT won't add DHCP options in the outgoing packets. The OLT forwards the incoming packets with DHCP options from an ONT
Note: See Section 26.10.1.4 on page 208 for more information about the configuration order for DHCP option 82 settings in different screens.			

Click **IP Application > DHCP > Option** in the navigation panel, then click the **ONT Option** link to open the following screen.

Figure 181 IP Application > DHCP > Option > ONT Option

Index	ONT ID	pass through	disable
*	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Apply Cancel

Paging

Prev Next ▾

The following table describes the labels in this screen.

Table 132 IP Application > DHCP > Option > ONT Option

LABEL	DESCRIPTION
	Choose the GPON interface that you want the settings configured here to apply to from the drop-down list.
Index	This is the index number of the ONT connected to the GPON interface.
ONT ID	This is the identifier of an ONT. Note: When register method D or E is selected and activated in the Advanced Application > OLT Registration screen, ONT ID 121-128 are the ONT template IDs.
pass through	Select this to forward packets with DHCP options from an ONT. Otherwise, they'll be dropped. Note: When ONT ID 121-128 are the ONT template IDs, the setting for this field applies to the Advanced Application > ONT Template screen.
disable	Deselect this to add DHCP options in outgoing packets. You can set up DHCP options in the IP Application > DHCP > Option screen. Note: When ONT ID 121-128 are the ONT template IDs, the setting for this field applies to the Advanced Application > ONT Template screen.
Apply	Click Apply to save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Paging	
Prev/Next	Click Prev or Next to show the previous/next screen if all status information cannot be seen in one screen.

CHAPTER 37

Maintenance

37.1 Overview

This chapter explains how to configure the screens that let you maintain the firmware and configuration files.

37.1.1 What You Can Do

- Use the **Maintenance** screen ([Section 37.2 on page 301](#)) to erase running configuration, save a configuration file or restart the OLT.
- Use the **Firmware Upgrade** screen ([Section 37.6 on page 303](#)) to upload the latest firmware.
- Use the **Restore Configuration** screen ([Section 37.7 on page 304](#)) to upload a stored device configuration file.
- Use the **Backup Configuration** screen ([Section 37.8 on page 304](#)) to save your configurations for later use.

37.2 The Maintenance Screen

Use this screen to manage firmware and your configuration files. Click **Management > Maintenance** in the navigation panel to open the following screen.

Figure 182 Management > Maintenance



The following table describes the labels in this screen.

Table 133 Management > Maintenance

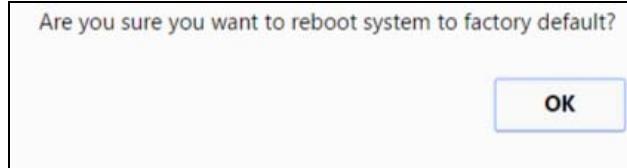
LABEL	DESCRIPTION
Current	This field displays which configuration (Configuration 1 or Configuration 2) is currently operating on the OLT.
Config	This field displays the firmware that was loaded to the OLT.
Firmware Upgrade	Click Click Here to go to the Firmware Upgrade screen.
Restore Configuration	Click Click Here to go to the Restore Configuration screen.
Backup Configuration	Click Click Here to go to the Backup Configuration screen.
Load Factory Default	Click Click Here to reset the current configuration of the OLT. Note that this will not reset the configuration to the factory default settings.
Save Configuration	Click Config 1 to save the current configuration settings to Configuration 1 on the OLT. Click Config 2 to save the current configuration settings to Configuration 2 on the OLT.
Reboot System	Click Config 1 to reboot the system and load Configuration 1 on the OLT. Click Config 2 to reboot the system and load Configuration 2 on the OLT. Note: Make sure to click the Save button in any screen to save your settings to the current configuration on the OLT.

37.3 Load Factory Default

Follow the steps below to reset the OLT back to the factory defaults.

- 1 Click the **Click Her** button next to the **Load Factory Default** field.
- 2 Click **OK** to continue or **Cancel** to abort.

Figure 183 Load Factory Default: Start



If you want to access the OLT web configurator again, you may need to change the IP address of your computer to be in the same subnet as that of the default OLT IP address (192.168.1.1 or DHCP-assigned IP).

37.4 Save Configuration

Click **Config 1** to save the current configuration settings permanently to **Configuration 1** on the OLT.

Click **Config 2** to save the current configuration settings permanently to **Configuration 2** on the OLT.

Alternatively, click **Save** on the top right-hand corner in any screen to save the configuration changes to the current configuration.

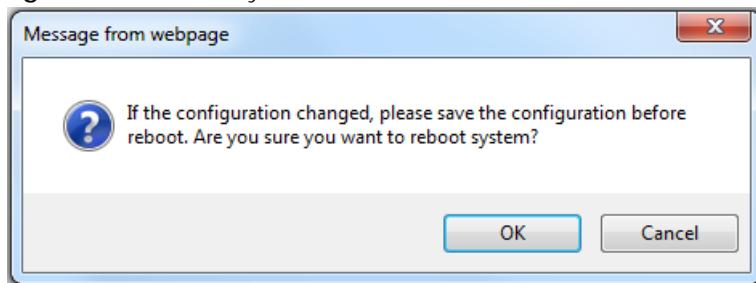
Note: Clicking the **Apply** or **Add** button does NOT save the changes permanently. All unsaved changes are erased after you reboot the OLT.

37.5 Reboot System

Reboot System allows you to restart the OLT without physically turning the power off. It also allows you to load configuration one (**Config 1**) or configuration two (**Config 2**) when you reboot. Follow the steps below to reboot the OLT.

- 1 In the **Maintenance** screen, click a configuration button next to **Reboot System** to reboot and load that configuration file. The following screen displays.

Figure 184 Reboot System: Confirmation



- 2 Click **OK** again and then wait for the OLT to restart. This takes up to two minutes. This does not affect the OLT's configuration.

Click **Config 1** and follow steps 1 to 2 to reboot and load configuration one on the OLT.

Click **Config 2** and follow steps 1 to 2 to reboot and load configuration two on the OLT.

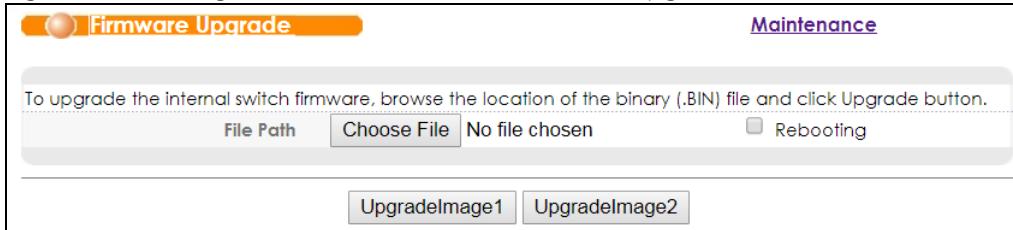
37.6 Firmware Upgrade

Use the following screen to upgrade your OLT to the latest firmware. The OLT supports dual firmware images, **Firmware 1** and **Firmware 2**. Use this screen to specify which image is updated when firmware is uploaded using the web configurator and to specify which image is loaded when the OLT starts up.

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.

Click **Management > Maintenance > Firmware Upgrade** to view the screen as shown next.

Figure 185 Management > Maintenance > Firmware Upgrade

Click **Choose File** to locate the file name of the firmware file that you wish to upload to the OLT (Firmware upgrades are only applied after a reboot). Click **UpgradedImage1** or **UpgradedImage2** to load the new firmware.

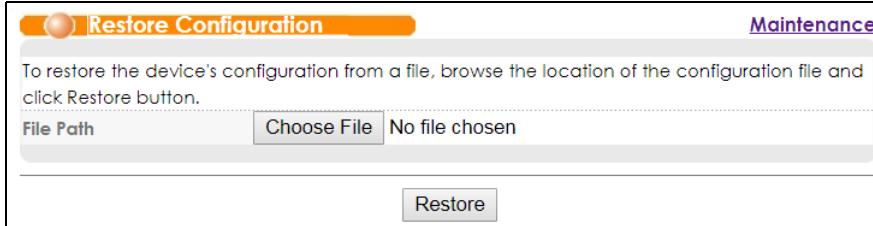
After the firmware upgrade process is complete, see the **System Info** screen to verify your current firmware version number.

Table 134 Management > Maintenance > Firmware Upgrade

LABEL	DESCRIPTION
File Path	Click Choose File to locate the file name of the firmware file that you wish to upload to the OLT.
Rebooting	Select the Rebooting check box to reboot the OLT after the firmware upgrade process is complete.
UpgradedImage1/2	Click this to upgrade the firmware of the firmware image 1/2.

37.7 Restore Configuration

Use this screen to restore a previously saved configuration from your computer to the OLT.

Figure 186 Management > Maintenance > Restore Configuration

Click **Choose File** to locate file name of the configuration file you wish to restore. After you have specified the file, click **Restore**. "config" is the name of the configuration file on the OLT, so your backup configuration file is automatically renamed when you restore using this screen.

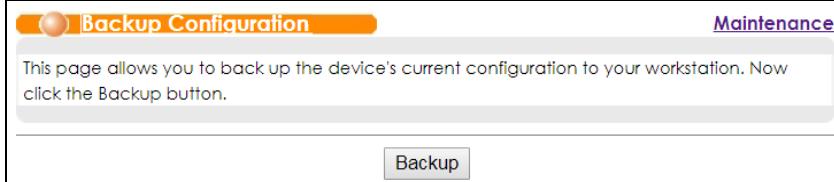
37.8 Backup Configuration

Use this screen to save and store your current device settings.

Backing up your OLT configurations allows you to create various "snap shots" of your device from which you may restore at a later date.

Back up your current OLT configuration to a computer using the **Backup Configuration** screen.

Figure 187 Management > Maintenance > Backup Configuration



Follow the steps below to back up the current OLT configuration to your computer in this screen.

- 1 Click **Backup**.
- 2 If the current configuration file is open and/or downloaded to your computer automatically, you can click **File > Save As** to save the file to a specific place.
If a dialog box pops up asking whether you want to open or save the file, click **Save** or **Save File** to download it to the default downloads folder on your computer. If a **Save As** screen displays after you click **Save** or **Save File**, 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.

37.9 Technical Reference

This section provides technical background information on the topics discussed in this chapter.

37.9.1 FTP Command Line

This section shows some examples of uploading to or downloading files from the OLT using FTP commands. First, understand the filename conventions.

37.9.2 Filename Conventions

The configuration file contains the settings in the screens such as OLT setup, IP Setup, and so on. Once you have custom the OLT's settings, they can be saved back to your computer under a filename of your choosing.

ZyNOS (Zyxel Network Operating System sometimes referred to as the "ras" file) is the system firmware and has a "bin" filename extension.

Table 135 Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	config	*.cfg	This is the configuration filename on the OLT. Uploading the config file replaces the specified configuration file system, including your OLT configurations.
Firmware	ras	*.bin	This is the generic name for the ZyNOS firmware on the OLT.

37.9.2.1 Example FTP Commands

```
ftp> put firmware.bin ras
```

This is a sample FTP session showing the transfer of the computer file "firmware.bin" to the OLT.

```
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 OLT only recognizes "config" and "ras". Be sure you keep unaltered copies of both files for later use.

Be sure to upload the correct model firmware as uploading the wrong model firmware may damage your device.

37.9.3 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 OLT.
- 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 OLT, for example, `put firmware.bin ras` transfers the firmware on your computer (firmware.bin) to the OLT and renames it to "ras". Similarly, `put config.cfg config` transfers the configuration file on your computer (config.cfg) to the OLT and renames it to "config". Likewise `get config config.cfg` transfers the configuration file on the OLT to your computer and renames it to "config.cfg". See [Table 135 on page 305](#) for more information on filename conventions.
- 7 Enter `quit` to exit the ftp prompt.

37.9.4 GUI-based FTP Clients

The following table describes some of the commands that you may see in GUI-based FTP clients.

General Commands for GUI-based FTP Clients

COMMAND	DESCRIPTION
Host Address	Enter the address of the host server.
Login Type	Anonymous. This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option. Normal. The server requires a unique User ID and Password to login.
Transfer Type	Transfer files in either ASCII (plain text format) or in binary mode. Configuration and firmware files should be transferred in binary mode.
Initial Remote Directory	Specify the default remote directory (path).
Initial Local Directory	Specify the default local directory (path).

37.9.5 FTP Restrictions

FTP will not work when:

- FTP service is disabled in the **Service Access Control** screen.
- The IP address(es) in the **Remote Management** screen does not match the client IP address. If it does not match, the OLT will disconnect the FTP session immediately.

CHAPTER 38

Access Control

38.1 Access Control Overview

This chapter describes how to control access to the OLT.

FTP is allowed one session. Telnet and SSH share five sessions. Up to five Web sessions (five different user names and passwords) and/or limitless SNMP access control sessions are allowed.

Table 136 Access Control Overview

SSH	Telnet	FTP	Web	SNMP
Share up to five sessions	One session	Up to five accounts	No limit	

38.1.1 What You Can Do

- Use the **Access Control** screen ([Section 38.2 on page 308](#)) to display the main screen.
- Use the **SNMP** screen ([Section 38.3 on page 309](#)) to configure your SNMP settings.
- Use the **Trap Group** screen ([Section 38.3.1 on page 310](#)) to specify the types of SNMP traps that should be sent to each SNMP manager.
- Use the **User Information** screen ([Section 38.3.2 on page 311](#)) to create SNMP users for authentication with managers using SNMP v3 and associate them to SNMP groups.
- Use the **Logins** screens ([Section 38.4 on page 313](#)) to assign which users can access the OLT via web configurator at any one time.
- Use the **Service Access Control** screen ([Section 38.5 on page 314](#)) to decide what services you may use to access the OLT.
- Use the **Remote Management** screen ([Section 38.6 on page 315](#)) to specify a group of one or more “trusted computers” from which an administrator may use a service to manage the OLT.

38.2 The Access Control Main Screen

Use this screen to display the main screen.

Click **Management > Access Control** in the navigation panel to display the main screen as shown.

Figure 188 Management > Access Control

38.3 Configuring SNMP

Use this screen to configure your SNMP settings.

Click **Management > Access Control > SNMP** to view the screen as shown.

Figure 189 Management > Access Control > SNMP

General Setting			
Version	IP	Port	Username
v2c	public		

Trap Destination			
Version	IP	Port	Username
v2c	0.0.0.0	162	

Apply **Cancel**

The following table describes the labels in this screen.

Table 137 Management > Access Control > SNMP

LABEL	DESCRIPTION
General Setting	Use this section to specify the SNMP version and community (password) values.
Version	Select the SNMP version for the OLT. The SNMP version on the OLT must match the version on the SNMP manager. Choose SNMP version 2c (v2c), SNMP version 3 (v3) or both (v3v2c). SNMP version 2c is backwards compatible with SNMP version 1.
Get Community	Enter the Get Community string, which is the password for the incoming Get- and GetNext- requests from the management station. The Get Community string is only used by SNMP managers using SNMP version 2c or lower.

Table 137 Management > Access Control > SNMP (continued)

LABEL	DESCRIPTION
Set Community	Enter the Set Community , which is the password for incoming Set- requests from the management station. The Set Community string is only used by SNMP managers using SNMP version 2c or lower.
Trap Community	Enter the Trap Community string, which is the password sent with each trap to the SNMP manager. The Trap Community string is only used by SNMP managers using SNMP version 2c or lower.
Trap Destination	Use this section to configure where to send SNMP traps from the OLT.
Version	Specify the version of the SNMP trap messages.
IP	Enter the IP addresses of up to four managers to send your SNMP traps to.
Port	Enter the port number upon which the manager listens for SNMP traps.
Username	Enter the username to be sent to the SNMP manager along with the SNMP v3 trap. This username must match an existing account on the OLT (configured in Management > Access Control > Logins screen).
Apply	Click Apply to save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

38.3.1 Configuring SNMP Trap Group

From the **SNMP** screen, click **Trap Group** to view the screen as shown. Use the **Trap Group** screen to specify the types of SNMP traps that should be sent to each SNMP manager.

Figure 190 Management > Access Control > SNMP > Trap Group

Type	Options
System	<input type="checkbox"/> * <input type="checkbox"/> coldstart <input type="checkbox"/> warmstart <input type="checkbox"/> fanspeed <input type="checkbox"/> temperature <input type="checkbox"/> voltage <input type="checkbox"/> reset <input type="checkbox"/> timesync <input type="checkbox"/> intrusionlock <input type="checkbox"/> loopguard <input type="checkbox"/> errdisable <input type="checkbox"/> externalalarm <input type="checkbox"/> maintainence
Interface	<input type="checkbox"/> * <input type="checkbox"/> linkup <input type="checkbox"/> linkdown <input type="checkbox"/> autonegotiation <input type="checkbox"/> lldp <input type="checkbox"/> transceiver-ddm <input type="checkbox"/> ploam <input type="checkbox"/> omci <input type="checkbox"/> rogue <input type="checkbox"/> remote-ont
AAA	<input type="checkbox"/> * <input type="checkbox"/> authentication <input type="checkbox"/> accounting
IP	<input type="checkbox"/> * <input type="checkbox"/> ping <input type="checkbox"/> traceroute
Switch	<input type="checkbox"/> * <input type="checkbox"/> stp <input type="checkbox"/> mactable <input type="checkbox"/> rmon <input type="checkbox"/> cfm

Apply **Cancel**

The following table describes the labels in this screen.

Table 138 Management > Access Control > SNMP > Trap Group

LABEL	DESCRIPTION
Trap Destination IP	Select one of your configured trap destination IP addresses. These are the IP addresses of the SNMP managers. You must first configure a trap destination IP address in the SNMP Setting screen. Use the rest of the screen to select which traps the OLT sends to that SNMP manager.
Type	Select the categories of SNMP traps that the OLT is to send to the SNMP manager.
Options	Select the individual SNMP traps that the OLT is to send to the SNMP station. See SNMP Traps on page 318 for individual trap descriptions. The traps are grouped by category. Selecting a category automatically selects all of the category's traps. Clear the check boxes for individual traps that you do not want the OLT to send to the SNMP station. Clearing a category's check box automatically clears all of the category's trap check boxes (the OLT only sends traps from selected categories).
Apply	Click Apply to save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

38.3.2 Configuring SNMP User

From the **SNMP** screen, click **User** to view the screen as shown. Use the **User** screen to create SNMP users for authentication with managers using SNMP v3 and associate them to SNMP groups. An SNMP user is an SNMP manager.

Figure 191 Management > Access Control > SNMP > User

User Information		SNMP Setting	
Username	<input type="text"/>	Security Level	noauth ▾
Authentication	MD5 ▾	Password	<input type="password"/>
Privacy	DES ▾	Password	<input type="password"/>
Group	admin ▾		
<input type="button" value="Add"/> <input type="button" value="Cancel"/> <input type="button" value="Clear"/>			
<input type="button" value="Index"/> <input type="button" value="Username"/> <input type="button" value="SecurityLevel"/> <input type="button" value="Authentication"/> <input type="button" value="Privacy"/> <input type="button" value="Group"/> <input type="button" value="Delete"/>			
<input type="button" value="Delete"/> <input type="button" value="Cancel"/>			

The following table describes the labels in this screen.

Table 139 Management > Access Control > SNMP > User

LABEL	DESCRIPTION
User Information	Note: Use the username and password of the login accounts you specify in this screen to create accounts on the SNMP v3 manager.
Username	Specify the username of a login account on the OLT.

Table 139 Management > Access Control > SNMP > User (continued)

LABEL	DESCRIPTION
Security Level	Select whether you want to implement authentication and/or encryption for SNMP communication from this user. Choose: <ul style="list-style-type: none"> noauth - to use the username as the password string to send to the SNMP manager. This is equivalent to the Get, Set and Trap Community in SNMP v2c. This is the lowest security level. auth - to implement an authentication algorithm for SNMP messages sent by this user. priv - to implement authentication and encryption for SNMP messages sent by this user. This is the highest security level. <p>Note: The settings on the SNMP manager must be set at the same security level or higher than the security level settings on the OLT.</p>
Authentication	Select an authentication algorithm. MD5 (Message Digest 5) and SHA (Secure Hash Algorithm) are hash algorithms used to authenticate SNMP data. SHA authentication is generally considered stronger than MD5, but is slower.
Password	Enter the password of up to 32 ASCII characters for SNMP user authentication.
Privacy	Specify the encryption method for SNMP communication from this user. You can choose one of the following: <ul style="list-style-type: none"> DES - Data Encryption Standard is a widely used (but breakable) method of data encryption. It applies a 56-bit key to each 64-bit block of data. AES - Advanced Encryption Standard is another method for data encryption that also uses a secret key. AES applies a 128-bit key to 128-bit blocks of data.
Password	Enter the password of up to 32 ASCII characters for encrypting SNMP packets.
Group	SNMP v3 adopts the concept of View-based Access Control Model (VACM) group. SNMP managers in one group are assigned common access rights to MIBs. Specify in which SNMP group this user is. <p>admin - Members of this group can perform all types of system configuration, including the management of administrator accounts.</p> <p>readwrite - Members of this group have read and write rights, meaning that the user can create and edit the MIBs on the OLT, except the user account and AAA configuration.</p> <p>readonly - Members of this group have read rights only, meaning the user can collect information from the OLT.</p>
Add	Click this to create a new entry or to update an existing one. This saves your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields to your previous configuration.
Clear	Click Clear to reset the fields to the factory defaults.
Index	This is a read-only number identifying a login account on the OLT. Click on an index number to view more details and edit an existing account.
Username	This field displays the username of a login account on the OLT.
Security Level	This field displays whether you want to implement authentication and/or encryption for SNMP communication with this user.
Authentication	This field displays the authentication algorithm used for SNMP communication with this user.
Privacy	This field displays the encryption method used for SNMP communication with this user.
Group	This field displays the SNMP group to which this user belongs.
Delete	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to begin configuring this screen afresh.

38.4 Logins

Up to five people (one administrator and four non-administrators) may access the OLT via web configurator at any one time.

- An administrator is someone who can both view and configure OLT changes. The username for the Administrator is always **admin**. The default administrator password is **1234**.

Note: It is highly recommended that you change the default administrator password (**1234**).

- A non-administrator (username is something other than **admin**) is someone who can view but not configure OLT settings.

Click **Management > Access Control > Logins** to view the screen as shown.

Figure 192 Management > Access Control > Logins

Login	User Name	Password	Retype to confirm	Privilege
1				0 ▾
2				0 ▾
3				0 ▾
4				0 ▾

The following table describes the labels in this screen.

Table 140 Management > Access Control > Logins

LABEL	DESCRIPTION
Administrator	This is the default administrator account with the "admin" user name. You cannot change the default administrator user name. Only the administrator has read/write access.
Old Password	Type the existing system password (1234 is the default password when shipped).
New Password	Enter your new system password.
Retype to confirm	Retype your new system password for confirmation.
Edit Logins	You may configure passwords for up to four users.
User Name	Set a user name (up to 32 ASCII characters long).
Password	Enter your new system password.

Table 140 Management > Access Control > Logins (continued)

LABEL	DESCRIPTION
Retype to confirm	Retype your new system password for confirmation.
Privilege	<p>Type the privilege level for this user. At the time of writing, users may have a privilege level of 0, 3, 13, or 14 representing different configuration rights as shown below.</p> <ul style="list-style-type: none"> • 0 - Display basic system information. • 3 - Display configuration or status. • 13 - Configure features except for login accounts, SNMP user accounts, the authentication method sequence and authorization settings, multiple logins, administrator and enable passwords, and configuration information display. • 14 - Configure login accounts, SNMP user accounts, the authentication method sequence and authorization settings, multiple logins, and administrator and enable passwords, and display configuration information. <p>Users can run command lines if the session's privilege level is greater than or equal to the command's privilege level. The session privilege initially comes from the privilege of the login account. For example, if the user has a privilege of 5, he/she can run commands that require privilege level of 5 or less but not more.</p>
Apply	Click Apply to save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

38.5 Service Access Control

Service Access Control allows you to decide what services you may use to access the OLT. You may also change the default service port and configure "trusted computer(s)" for each service in the **Remote Management** screen (discussed later). Click **Access Control** to go back to the main **Access Control** screen.

Figure 193 Management > Access Control > Service Access Control

Service Access Control		Access Control	
Services	Active	Service Port	Timeout
Telnet	<input checked="" type="checkbox"/>	23	
SSH	<input checked="" type="checkbox"/>	22	
FTP	<input checked="" type="checkbox"/>	21	
HTTP	<input checked="" type="checkbox"/>	80	60 Minutes
HTTPS	<input checked="" type="checkbox"/>	443	
ICMP	<input checked="" type="checkbox"/>		
SNMP	<input checked="" type="checkbox"/>		

Apply **Cancel**

The following table describes the fields in this screen.

Table 141 Management > Access Control > Service Access Control

LABEL	DESCRIPTION
Services	Services you may use to access the OLT are listed here.
Active	Select this option for the corresponding services that you want to allow to access the OLT.

Table 141 Management > Access Control > Service Access Control (continued)

LABEL	DESCRIPTION
Service Port	For Telnet, SSH, FTP, HTTP or HTTPS services, you may change the default service port by typing the new port number in the Service Port field. If you change the default port number then you will have to let people (who wish to use the service) know the new port number for that service.
Timeout	Type how many minutes (from 1 to 255) a management session can be left idle before the session times out. After it times out you have to log in with your password again. Very long idle timeouts may have security risks.
Apply	Click Apply to save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

38.6 Remote Management

Use this screen to specify a group of one or more "trusted computers" from which an administrator may use a service to manage the OLT.

Click **Management > Access Control > Remote Management** to view the screen as shown next.

You can specify a group of one or more "trusted computers" from which an administrator may use a service to manage the OLT. Click **Access Control** to return to the **Access Control** screen.

Figure 194 Management > Access Control > Remote Management

Secured Client Setup			Access Control							
Entry	Active	Start Address	End Address	Telnet	FTP	HTTP	ICMP	SNMP	SSH	HTTPS
1	<input checked="" type="checkbox"/>	0.0.0.0	0.0.0.0	<input checked="" type="checkbox"/>						
2	<input type="checkbox"/>	0.0.0.0	0.0.0.0	<input type="checkbox"/>						
3	<input type="checkbox"/>	0.0.0.0	0.0.0.0	<input type="checkbox"/>						
4	<input type="checkbox"/>	0.0.0.0	0.0.0.0	<input type="checkbox"/>						
5	<input type="checkbox"/>	0.0.0.0	0.0.0.0	<input type="checkbox"/>						
6	<input type="checkbox"/>	0.0.0.0	0.0.0.0	<input type="checkbox"/>						
7	<input type="checkbox"/>	0.0.0.0	0.0.0.0	<input type="checkbox"/>						
8	<input type="checkbox"/>	0.0.0.0	0.0.0.0	<input type="checkbox"/>						
9	<input type="checkbox"/>	0.0.0.0	0.0.0.0	<input type="checkbox"/>						
10	<input type="checkbox"/>	0.0.0.0	0.0.0.0	<input type="checkbox"/>						
11	<input type="checkbox"/>	0.0.0.0	0.0.0.0	<input type="checkbox"/>						
12	<input type="checkbox"/>	0.0.0.0	0.0.0.0	<input type="checkbox"/>						
13	<input type="checkbox"/>	0.0.0.0	0.0.0.0	<input type="checkbox"/>						
14	<input type="checkbox"/>	0.0.0.0	0.0.0.0	<input type="checkbox"/>						
15	<input type="checkbox"/>	0.0.0.0	0.0.0.0	<input type="checkbox"/>						
16	<input type="checkbox"/>	0.0.0.0	0.0.0.0	<input type="checkbox"/>						

Apply **Cancel**

The following table describes the labels in this screen.

Table 142 Management > Access Control > Remote Management

LABEL	DESCRIPTION
Entry	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 OLT.
Active	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	Configure the IP address range of trusted computers from which you can manage this OLT.
End Address	The OLT checks if the client IP address of a computer requesting a service or protocol matches the range set here. The OLT immediately disconnects the session if it does not match.
Telnet/FTP/ HTTP/ICMP/ SNMP/SSH/ HTTPS	Select services that may be used for managing the OLT from the specified trusted computers.
Apply	Click Apply to save your changes to the OLT’s run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

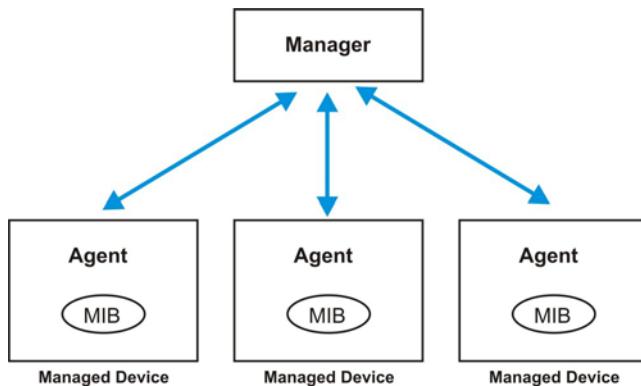
38.7 Technical Reference

This section provides technical background information on the topics discussed in this chapter.

38.7.1 About SNMP

Simple Network Management Protocol (SNMP) is an application layer protocol used to manage and monitor TCP/IP-based devices. SNMP is used to exchange management information between the network management system (NMS) and a network element (NE). A manager station can manage and monitor the OLT through the network via SNMP version 1 (SNMPv1), SNMP version 2c or SNMP version 3. The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

Figure 195 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 OLT (the OLT). An agent translates the local management information from the managed OLT 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 OLT. Examples of variables include number of packets received, node port status and so on. 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 143 SNMP Commands

LABEL	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.

SNMP v3 and Security

SNMP v3 enhances security for SNMP management. SNMP managers can be required to authenticate with agents before conducting SNMP management sessions.

Security can be further enhanced by encrypting the SNMP messages sent from the managers. Encryption protects the contents of the SNMP messages. When the contents of the SNMP messages are encrypted, only the intended recipients can read them.

Supported MIBs

MIBs let administrators collect statistics and monitor status and performance.

The OLT supports the following MIBs:

- SNMP MIB II (RFC 1213)
- RFC 1157 SNMP v1
- RFC 1493 Bridge MIBs
- RFC 1643 Ethernet MIBs
- RFC 1155 SMI
- RFC 2674 SNMPv2, SNMPv2c
- RFC 1757 RMON
- SNMPv2, SNMPv2c or later version, compliant with RFC 2011 SNMPv2 MIB for IP, RFC 2012 SNMPv2 MIB for TCP, RFC 2013 SNMPv2 MIB for UDP

SNMP Traps

The OLT sends traps to an SNMP manager when an event occurs. The following tables outline the SNMP traps by category.

An OID (Object ID) that begins with "1.3.6.1.4.1.890.1.5.17" is defined in private MIBs. Otherwise, it is a standard MIB OID.

The OIDs beginning with "1.3.6.1.4.1.890.1.5.17.5" are specific to OLT1404.

The OIDs beginning with "1.3.6.1.4.1.890.1.5.17.6" are specific to OLT1408.

Table 144 SNMP System Traps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
coldstart	coldStart	1.3.6.1.6.3.1.1.5.1	This trap is sent when the OLT is turned on.
warmstart	warmStart	1.3.6.1.6.3.1.1.5.2	This trap is sent when the OLT restarts.
fanspeed	FanSpeedEventOn	1.3.6.1.4.1.890.1.5.17.5.31.2.1 1.3.6.1.4.1.890.1.5.17.6.31.2.1	This trap is sent when the fan speed goes above or below the normal operating range.
	FanSpeedEventClear	1.3.6.1.4.1.890.1.5.17.5.31.2.2 1.3.6.1.4.1.890.1.5.17.6.31.2.2	This trap is sent when the fan speed returns to the normal operating range.
temperature	TemperatureEventOn	1.3.6.1.4.1.890.1.5.17.5.31.2.1 1.3.6.1.4.1.890.1.5.17.6.31.2.1	This trap is sent when the temperature goes above or below the normal operating range.
	TemperatureEventClear	1.3.6.1.4.1.890.1.5.17.5.31.2.2 1.3.6.1.4.1.890.1.5.17.6.31.2.2	This trap is sent when the temperature returns to the normal operating range.
voltage	VoltageEventOn	1.3.6.1.4.1.890.1.5.17.5.31.2.1 1.3.6.1.4.1.890.1.5.17.6.31.2.1	This trap is sent when the voltage goes above or below the normal operating range.
	VoltageEventClear	1.3.6.1.4.1.890.1.5.17.5.31.2.2 1.3.6.1.4.1.890.1.5.17.6.31.2.2	This trap is sent when the voltage returns to the normal operating range.
reset	UncontrolledResetEventOn	1.3.6.1.4.1.890.1.5.17.5.31.2.1 1.3.6.1.4.1.890.1.5.17.6.31.2.1	This trap is sent when the OLT automatically resets.
	ControlledResetEventOn	1.3.6.1.4.1.890.1.5.17.5.31.2.1 1.3.6.1.4.1.890.1.5.17.6.31.2.1	This trap is sent when the OLT resets by an administrator through a management interface.
	RebootEvent	1.3.6.1.4.1.890.1.5.1.1.2	This trap is sent when the OLT reboots by an administrator through a management interface.
timesync	RTCNotUpdatedEventOn	1.3.6.1.4.1.890.1.5.17.5.31.2.1 1.3.6.1.4.1.890.1.5.17.6.31.2.1	This trap is sent when the OLT fails to get the time and date from a time server.
	RTCNotUpdatedEventClear	1.3.6.1.4.1.890.1.5.17.5.31.2.2 1.3.6.1.4.1.890.1.5.17.6.31.2.2	This trap is sent when the OLT gets the time and date from a time server.
intrusionlock	IntrusionLockEventOn	1.3.6.1.4.1.890.1.5.17.5.31.2.1 1.3.6.1.4.1.890.1.5.17.6.31.2.1	This trap is sent when intrusion lock occurs on a port.
loopguard	LoopguardEventOn	1.3.6.1.4.1.890.1.5.17.5.31.2.1 1.3.6.1.4.1.890.1.5.17.6.31.2.1	This trap is sent when loopguard shuts down a port.

Table 144 SNMP System Traps (continued)

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
errdisable	zyErrdisableDetect	1.3.6.1.4.1.890.1.5.17.5.130.4.1 1.3.6.1.4.1.890.1.5.17.6.130.4.1	This trap is sent when an error is detected on a port, such as a loop occurs or the rate limit for specific control packets is exceeded.
	zyErrdisableRecovery	1.3.6.1.4.1.890.1.5.17.5.130.4.2 1.3.6.1.4.1.890.1.5.17.6.130.4.2	This trap is sent when the OLT ceases the action taken on a port, such as shutting down the port or discarding packets on the port, after the specified recovery interval.
externalalarm	ExternalAlarmEventOn	1.3.6.1.4.1.890.1.5.17.5.31.2.1 1.3.6.1.4.1.890.1.5.17.6.31.2.1	This trap is sent when an external alarm is received.
	ExternalAlarmEventClear	1.3.6.1.4.1.890.1.5.17.5.31.2.2 1.3.6.1.4.1.890.1.5.17.6.31.2.2	This trap is sent when an external alarm stops sending an alert.
maintenance	CpuAlarmEventOn	1.3.6.1.4.1.890.1.5.17.5.31.2.1 1.3.6.1.4.1.890.1.5.17.6.31.2.1	This trap is sent when the cpu utilization alarm is received.
	CpuAlarmEventClear	1.3.6.1.4.1.890.1.5.17.5.31.2.2 1.3.6.1.4.1.890.1.5.17.6.31.2.2	This trap is sent when the cpu utilization alarm is cleared.
	MemoryAlarmEventOn	1.3.6.1.4.1.890.1.5.17.5.31.2.1 1.3.6.1.4.1.890.1.5.17.6.31.2.1	This trap is sent when the memory utilization alarm is received.
	MemoryAlarmEventClear	1.3.6.1.4.1.890.1.5.17.5.31.2.2 1.3.6.1.4.1.890.1.5.17.6.31.2.2	This trap is sent when the memory utilization alarm is cleared.

Table 145 SNMP Interface Traps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
linkup	linkUp	1.3.6.1.6.3.1.1.5.4	This trap is sent when the Ethernet link is up.
	LinkDownEventClear	1.3.6.1.4.1.890.1.5.17.5.31.2.2 1.3.6.1.4.1.890.1.5.17.6.31.2.2	This trap is sent when the Ethernet link is up.
linkdown	linkDown	1.3.6.1.6.3.1.1.5.3	This trap is sent when the Ethernet link is down.
	LinkDownEventOn	1.3.6.1.4.1.890.1.5.17.5.31.2.1 1.3.6.1.4.1.890.1.5.17.6.31.2.1	This trap is sent when the Ethernet link is down.
autonegotiation	AutonegotiationFailedEventOn	1.3.6.1.4.1.890.1.5.17.5.31.2.1 1.3.6.1.4.1.890.1.5.17.6.31.2.1	This trap is sent when an Ethernet interface fails to auto-negotiate with the peer Ethernet interface.
	AutonegotiationFailedEventClear	1.3.6.1.4.1.890.1.5.17.5.31.2.2 1.3.6.1.4.1.890.1.5.17.6.31.2.2	This trap is sent when an Ethernet interface auto-negotiates with the peer Ethernet interface.

Table 145 SNMP Interface Traps (continued)

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
lldp	lldpRemTablesChange	1.0.8802.1.1.2.0.0.1	The trap is sent when entries in the remote database have any updates. Link Layer Discovery Protocol (LLDP), defined as IEEE 802.1ab, enables LAN devices that support LLDP to exchange their configured settings. This helps eliminate configuration mismatch issues.
transceiver-ddm	DDMIRxPowerEventOn	1.3.6.1.4.1.890.1.5.17.5.31.2.1	This trap is sent when one of the device operating parameters (such as transceiver temperature, laser bias current, transmitted optical power, received optical power, and transceiver supply voltage) is above or below a factory set normal range.
	DDMITemperatureEventOn	1.3.6.1.4.1.890.1.5.17.6.31.2.1	
	DDMITxBiasEventOn		
	DDMITxPowerEventOn		
	DDMIVoltageEventOn		
	DDMIRxPowerEventClear	1.3.6.1.4.1.890.1.5.17.5.31.2.2	This trap is sent when all device operating parameters return to the normal operating range.
	DDMITemperatureEventClear	1.3.6.1.4.1.890.1.5.17.6.31.2.2	
	DDMITxBiasEventClear		
	DDMITxPowerEventClear		
	DDMIVoltageEventClear		
ploam	ONTLOSIEventOn	1.3.6.1.4.1.890.1.5.17.5.31.2.1 1.3.6.1.4.1.890.1.5.17.6.31.2.1	This trap is sent when the LOSi (Loss of signal for ONUi) is received.
	ONTLOSIEventClear	1.3.6.1.4.1.890.1.5.17.5.31.2.2 1.3.6.1.4.1.890.1.5.17.6.31.2.2	This trap is sent when the LOSi (Loss of signal for ONUi) is cleared.
	ONTLOFIEventOn	1.3.6.1.4.1.890.1.5.17.5.31.2.1 1.3.6.1.4.1.890.1.5.17.6.31.2.1	This trap is sent when the LOFi (Loss of frame of ONUi) is received.
	ONTLOFIEventClear	1.3.6.1.4.1.890.1.5.17.5.31.2.2 1.3.6.1.4.1.890.1.5.17.6.31.2.2	This trap is sent when the LOFi (Loss of frame of ONUi) is cleared.
	ONTLOAMIEventOn	1.3.6.1.4.1.890.1.5.17.5.31.2.1 1.3.6.1.4.1.890.1.5.17.6.31.2.1	This trap is sent when the LOAMi (Loss of PLOAM for ONUi) is received.
	ONTLOAMIEventClear	1.3.6.1.4.1.890.1.5.17.5.31.2.2 1.3.6.1.4.1.890.1.5.17.6.31.2.2	This trap is sent when the LOAMi (Loss of PLOAM for ONUi) is cleared.
	ONTLCDGIEventOn	1.3.6.1.4.1.890.1.5.17.5.31.2.1 1.3.6.1.4.1.890.1.5.17.6.31.2.1	This trap is sent when the LCDGi (Loss of GEM channel delineation) is received.
	ONTLCDGIEventClear	1.3.6.1.4.1.890.1.5.17.5.31.2.2 1.3.6.1.4.1.890.1.5.17.6.31.2.2	This trap is sent when the LCDGi (Loss of GEM channel delineation) is cleared.
	ONTRDIIEventOn	1.3.6.1.4.1.890.1.5.17.5.31.2.1 1.3.6.1.4.1.890.1.5.17.6.31.2.1	This trap is sent when the RDII (Remote defect indication of ONUi) is received.
	ONTRDIIEventClear	1.3.6.1.4.1.890.1.5.17.5.31.2.2 1.3.6.1.4.1.890.1.5.17.6.31.2.2	This trap is sent when the RDII (Remote defect indication of ONUi) is cleared.

Table 145 SNMP Interface Traps (continued)

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
ploam	ONTSUFIEventOn	1.3.6.1.4.1.890.1.5.17.5.31.2.1 1.3.6.1.4.1.890.1.5.17.6.31.2.1	This trap is sent when the SUFi (Start-up failure of ONUi) is received.
	ONTSUFIEventClear	1.3.6.1.4.1.890.1.5.17.5.31.2.2 1.3.6.1.4.1.890.1.5.17.6.31.2.2	This trap is sent when the SUFi (Start-up failure of ONUi) is cleared.
	ONTLOAIEventOn	1.3.6.1.4.1.890.1.5.17.5.31.2.1 1.3.6.1.4.1.890.1.5.17.6.31.2.1	This trap is sent when the LOAi (Loss of acknowledge with ONUi) is received.
	ONTLOAIEventClear	1.3.6.1.4.1.890.1.5.17.5.31.2.2 1.3.6.1.4.1.890.1.5.17.6.31.2.2	This trap is sent when the LOAi (Loss of acknowledge with ONUi) is cleared.
	ONTDGIEventOn	1.3.6.1.4.1.890.1.5.17.5.31.2.1 1.3.6.1.4.1.890.1.5.17.6.31.2.1	This trap is sent when the DGi (Receive dyinggasp of ONUi) is received.
	ONTDGIEventClear	1.3.6.1.4.1.890.1.5.17.5.31.2.2 1.3.6.1.4.1.890.1.5.17.6.31.2.2	This trap is sent when the DGi (Receive dyinggasp of ONUi) is cleared.
	ONTDFIEventOn	1.3.6.1.4.1.890.1.5.17.5.31.2.1 1.3.6.1.4.1.890.1.5.17.6.31.2.1	This trap is sent when the DFi (Deactivate failure of ONUi) is received.
	ONTDFIEventClear	1.3.6.1.4.1.890.1.5.17.5.31.2.2 1.3.6.1.4.1.890.1.5.17.6.31.2.2	This trap is sent when the DFi (Deactivate failure of ONUi) is cleared.
	ONTDOWiEventOn	1.3.6.1.4.1.890.1.5.17.5.31.2.1 1.3.6.1.4.1.890.1.5.17.6.31.2.1	This trap is sent when the DOWi (Drift of window of ONUi) is received.
	ONTDOWiEventClear	1.3.6.1.4.1.890.1.5.17.5.31.2.2 1.3.6.1.4.1.890.1.5.17.6.31.2.2	This trap is sent when the DOWi (Drift of window of ONUi) is cleared.
	ONTTIWIEventOn	1.3.6.1.4.1.890.1.5.17.5.31.2.1 1.3.6.1.4.1.890.1.5.17.6.31.2.1	This trap is sent when the TIWi (Transmission interference warning) is received.
	ONTTIWIEventClear	1.3.6.1.4.1.890.1.5.17.5.31.2.2 1.3.6.1.4.1.890.1.5.17.6.31.2.2	This trap is sent when the TIWi (Transmission interference warning) is cleared.
	ONTSFIEventOn	1.3.6.1.4.1.890.1.5.17.5.31.2.1 1.3.6.1.4.1.890.1.5.17.6.31.2.1	This trap is sent when the SFi (Signal fail of ONUi) is received.
	ONTSFIEventClear	1.3.6.1.4.1.890.1.5.17.5.31.2.2 1.3.6.1.4.1.890.1.5.17.6.31.2.2	This trap is sent when the SFi (Signal fail of ONUi) is cleared.
	ONTSDIEventOn	1.3.6.1.4.1.890.1.5.17.5.31.2.1 1.3.6.1.4.1.890.1.5.17.6.31.2.1	This trap is sent when the SDi (Signal degraded of ONUi) is received.
	ONTSDIEventClear	1.3.6.1.4.1.890.1.5.17.5.31.2.2 1.3.6.1.4.1.890.1.5.17.6.31.2.2	This trap is sent when the SDi (Signal degraded of ONUi) is cleared.
	ONTLOKIEventOn	1.3.6.1.4.1.890.1.5.17.5.31.2.1 1.3.6.1.4.1.890.1.5.17.6.31.2.1	This trap is sent when the LOKi (Loss of key synch with ONUi) is received.
	ONTLOKIEventClear	1.3.6.1.4.1.890.1.5.17.5.31.2.2 1.3.6.1.4.1.890.1.5.17.6.31.2.2	This trap is sent when the LOKi (Loss of key synch with ONUi) is cleared.

Table 145 SNMP Interface Traps (continued)

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
ploam	ONTTCAFECCcorrbyteEventOn	1.3.6.1.4.1.890.1.5.17.5.31.2.1 1.3.6.1.4.1.890.1.5.17.6.31.2.1	This trap is sent when an alert for going over the FEC corrected byte threshold is received.
	ONTTCAFECCcorrbyteEventClear	1.3.6.1.4.1.890.1.5.17.5.31.2.2 1.3.6.1.4.1.890.1.5.17.6.31.2.2	This trap is sent when an alert for going over the FEC corrected byte threshold is cleared.
	ONTTCAFECCcorrCodewordEventOn	1.3.6.1.4.1.890.1.5.17.5.31.2.1 1.3.6.1.4.1.890.1.5.17.6.31.2.1	This trap is sent when an alert for going over the FEC corrected code word threshold is received.
	ONTTCAFECCcorrCodewordEventClear	1.3.6.1.4.1.890.1.5.17.5.31.2.2 1.3.6.1.4.1.890.1.5.17.6.31.2.2	This trap is sent when an alert for going over the FEC corrected code word threshold is cleared.
	ONTTCAFEUnCcorrCodewordEventOn	1.3.6.1.4.1.890.1.5.17.5.31.2.1 1.3.6.1.4.1.890.1.5.17.6.31.2.1	This trap is sent when an alert for going over the FEC uncorrected code word threshold is received.
	ONTTCAFEUnCcorrCodewordEventClear	1.3.6.1.4.1.890.1.5.17.5.31.2.2 1.3.6.1.4.1.890.1.5.17.6.31.2.2	This trap is sent when an alert for going over the FEC uncorrected code word threshold is cleared.
	ONTTCABIPEventOn	1.3.6.1.4.1.890.1.5.17.5.31.2.1 1.3.6.1.4.1.890.1.5.17.6.31.2.1	This trap is sent when an alert for going over the bit interleaved parity threshold is received.
	ONTTCABIPEventClear	1.3.6.1.4.1.890.1.5.17.5.31.2.2 1.3.6.1.4.1.890.1.5.17.6.31.2.2	This trap is sent when an alert for going over the bit interleaved parity threshold is cleared.
	ONTTCAREIEventOn	1.3.6.1.4.1.890.1.5.17.5.31.2.1 1.3.6.1.4.1.890.1.5.17.6.31.2.1	This trap is sent when an alert for going over the remote error indication threshold is received.
	ONTTCAREIEventClear	1.3.6.1.4.1.890.1.5.17.5.31.2.2 1.3.6.1.4.1.890.1.5.17.6.31.2.2	This trap is sent when an alert for going over the remote error indication threshold is cleared.
omci	OMCILanLosEventOn OMCIDyingGaspEventOn OMCIEndToEndLossOfContinuityEventOn OMCIFreqMismatchEventOn OMCILineInitializationFailureEventOn	1.3.6.1.4.1.890.1.5.17.5.31.2.1 1.3.6.1.4.1.890.1.5.17.6.31.2.1	The trap is sent when an alert is sent by OMCI because of LanLos or dying gasp.
	OMCILanLosEventClear OMCIDyingGaspEventClear OMCIEndToEndLossOfContinuityEventClear OMCIFreqMismatchEventClear OMCILineInitializationFailureEventClear	1.3.6.1.4.1.890.1.5.17.5.31.2.2 1.3.6.1.4.1.890.1.5.17.6.31.2.2	The trap is sent when an event alert is cleared by OMCI.
	RogueOntDetectEventOn	1.3.6.1.4.1.890.1.5.17.5.31.2.1 1.3.6.1.4.1.890.1.5.17.6.31.2.1	This trap is sent when a rogue ONT is detected.

Table 145 SNMP Interface Traps (continued)

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
remote-ont	SwdIStartEventOn	1.3.6.1.4.1.890.1.5.17.5.31.2.1	The trap is sent when an alert is sent because of an ONT software download or ONT discovery.
	SwdISuccessEventOn	1.3.6.1.4.1.890.1.5.17.6.31.2.1	
	SwdIFailEventOn		
	DiscoverUnregOntEventOn		
	SwdIStartEventClear	1.3.6.1.4.1.890.1.5.17.5.31.2.2	The trap is sent when an alert for an ONT software download or ONT discovery is cleared.
	SwdISuccessEventClear	1.3.6.1.4.1.890.1.5.17.6.31.2.2	
	SwdIFailEventClear		
	DiscoverUnregOntEventClear		

Table 146 SNMP AAA Traps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
authentication	authenticationFailure	1.3.6.1.6.3.1.1.5.5	This trap is sent when authentication fails due to incorrect user name and/or password.
	AuthenticationFailureEventOn	1.3.6.1.4.1.890.1.5.17.5.31.2.1	
		1.3.6.1.4.1.890.1.5.17.6.31.2.1	
	RADIUSNotReachableEventOn	1.3.6.1.4.1.890.1.5.17.5.31.2.1	
		1.3.6.1.4.1.890.1.5.17.6.31.2.1	This trap is sent when there is no response message from the RADIUS server.
	RADIUSNotReachableEventClear	1.3.6.1.4.1.890.1.5.17.5.31.2.2	
		1.3.6.1.4.1.890.1.5.17.6.31.2.2	
accounting	RADIUSAacctNotReachableEvent On	1.3.6.1.4.1.890.1.5.17.5.31.2.1	This trap is sent when there is no response message from the RADIUS accounting server.
		1.3.6.1.4.1.890.1.5.17.6.31.2.1	
	RADIUSAacctNotReachableEvent Clear	1.3.6.1.4.1.890.1.5.17.5.31.2.2	This trap is sent when the RADIUS accounting server can be reached.
		1.3.6.1.4.1.890.1.5.17.6.31.2.2	

Table 147 SNMP IP Traps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
ping	pingProbeFailed	1.3.6.1.2.1.80.0.1	This trap is sent when a single ping probe fails.
	pingTestFailed	1.3.6.1.2.1.80.0.2	This trap is sent when a ping test (consisting of a series of ping probes) fails.
	pingTestCompleted	1.3.6.1.2.1.80.0.3	This trap is sent when a ping test is completed.
traceroute	traceRouteTestFailed	1.3.6.1.2.1.81.0.2	This trap is sent when a traceroute test fails.
	traceRouteTestCompleted	1.3.6.1.2.1.81.0.3	This trap is sent when a traceroute test is completed.

Table 148 SNMP Switch Traps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
stp	STPNewRoot	1.3.6.1.2.1.17.0.1	This trap is sent when the STP root switch changes.
	MRSTPNewRoot	1.3.6.1.4.1.890.1.5.17.5. 42.2.1 1.3.6.1.4.1.890.1.5.17.6. 42.2.1	This trap is sent when the MRSTP root switch changes.
	MSTPNewRoot	1.3.6.1.4.1.890.1.5.17.5. 107.70.1 1.3.6.1.4.1.890.1.5.17.6. 107.70.1	This trap is sent when the MSTP root switch changes.
	STPTopologyChange	1.3.6.1.2.1.17.0.2	This trap is sent when the STP topology changes.
	MRSTPTopologyChange	1.3.6.1.4.1.890.1.5.17.5. 42.2.2 1.3.6.1.4.1.890.1.5.17.6. 42.2.2	This trap is sent when the MRSTP topology changes.
	MSTPTopologyChange	1.3.6.1.4.1.890.1.5.17.5. 107.70.2 1.3.6.1.4.1.890.1.5.17.6. 107.70.2	This trap is sent when the MSTP root switch changes.
mactable	MacTableFullEventOn	1.3.6.1.4.1.890.1.5.17.5. 31.2.1 1.3.6.1.4.1.890.1.5.17.6. 31.2.1	This trap is sent when more than 99% of the MAC table is used.
	MacTableFullEventClear	1.3.6.1.4.1.890.1.5.17.5. 31.2.2 1.3.6.1.4.1.890.1.5.17.6. 31.2.2	This trap is sent when less than 95% of the MAC table is used.
rmon	RmonRisingAlarm	1.3.6.1.2.1.16.0.1	This trap is sent when a variable goes over the RMON "rising" threshold.
	RmonFallingAlarm	1.3.6.1.2.1.16.0.2	This trap is sent when the variable falls below the RMON "falling" threshold.
cfm	dot1agCfmFaultAlarm	1.3.111.2.802.1.1.8.0.1	The trap is sent when the OLT detects a connectivity fault.

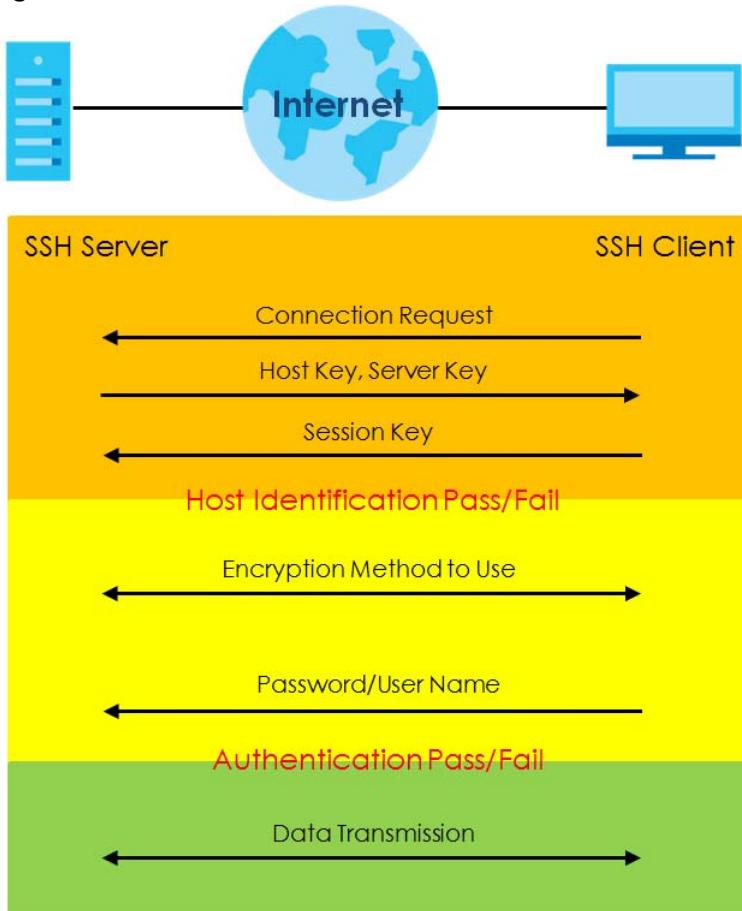
38.7.2 SSH Overview

Unlike Telnet or FTP, which transmit data in clear text, SSH (Secure Shell) is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network.

Figure 196 SSH Communication Example

38.7.2.1 How SSH works

The following table summarizes how a secure connection is established between two remote hosts.

Figure 197 How SSH Works

1 Host Identification

The SSH client sends a connection request to the SSH server. The server identifies itself with a host key. The client encrypts a randomly generated session key with the host key and server key and sends the result back to the server.

The client automatically saves any new server public keys. In subsequent connections, the server public key is checked against the saved version on the client computer.

2 Encryption Method

Once the identification is verified, both the client and server must agree on the type of encryption method to use.

3 Authentication and Data Transmission

After the identification is verified and data encryption activated, a secure tunnel is established between the client and the server. The client then sends its authentication information (user name and password) to the server to log in to the server.

38.7.2.2 SSH Implementation on the Switch

Your OLT supports SSH version 2 using RSA authentication and three encryption methods (DES, 3DES and Blowfish). The SSH server is implemented on the OLT for remote management and file transfer on port 22. Only one SSH connection is allowed at a time.

38.7.2.3 Requirements for Using SSH

You must install an SSH client program on a client computer (Windows or Linux operating system) that is used to connect to the OLT over SSH.

38.7.3 Introduction to HTTPS

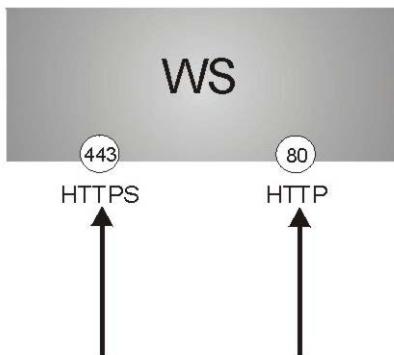
HTTPS (HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a web protocol that encrypts and decrypts web pages. Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data by ensuring confidentiality (an unauthorized party cannot read the transferred data), authentication (one party can identify the other party) and data integrity (you know if data has been changed).

It relies upon certificates, public keys, and private keys.

HTTPS on the OLT is used so that you may securely access the OLT using the web configurator. The SSL protocol specifies that the SSL server (the OLT) must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the OLT), whereas the SSL client only should authenticate itself when the SSL server requires it to do so. Authenticating client certificates is optional and if selected means the SSL-client must send the OLT a certificate. You must apply for a certificate for the browser from a Certificate Authority (CA) that is a trusted CA on the OLT.

Please refer to the following figure.

- 1** HTTPS connection requests from an SSL-aware web browser go to port 443 (by default) on the OLT's WS (web server).
- 2** HTTP connection requests from a web browser go to port 80 (by default) on the OLT's WS (web server).

Figure 198 HTTPS Implementation

Note: If you disable HTTP in the Service Access Control screen, then the OLT blocks all HTTP connection attempts.

38.7.3.1 HTTPS Example

If you haven't changed the default HTTPS port on the OLT, then in your browser enter "https://OLT IP Address/" as the web site address where "OLT IP Address" is the IP address or domain name of the OLT you wish to access.

Internet Explorer Warning Messages

Internet Explorer 6

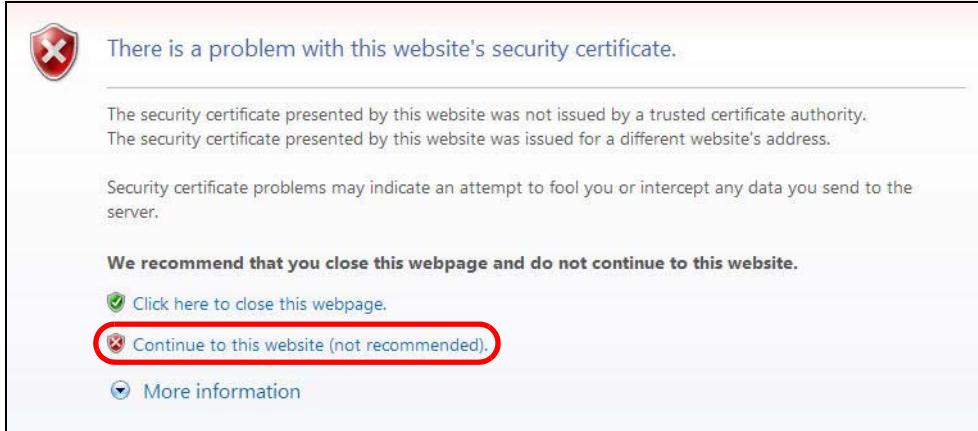
When you attempt to access the OLT HTTPS server, a Windows dialog box pops up asking if you trust the server certificate.

You see the following **Security Alert** screen in Internet Explorer. Select **Yes** to proceed to the web configurator login screen; if you select **No**, then web configurator access is blocked.

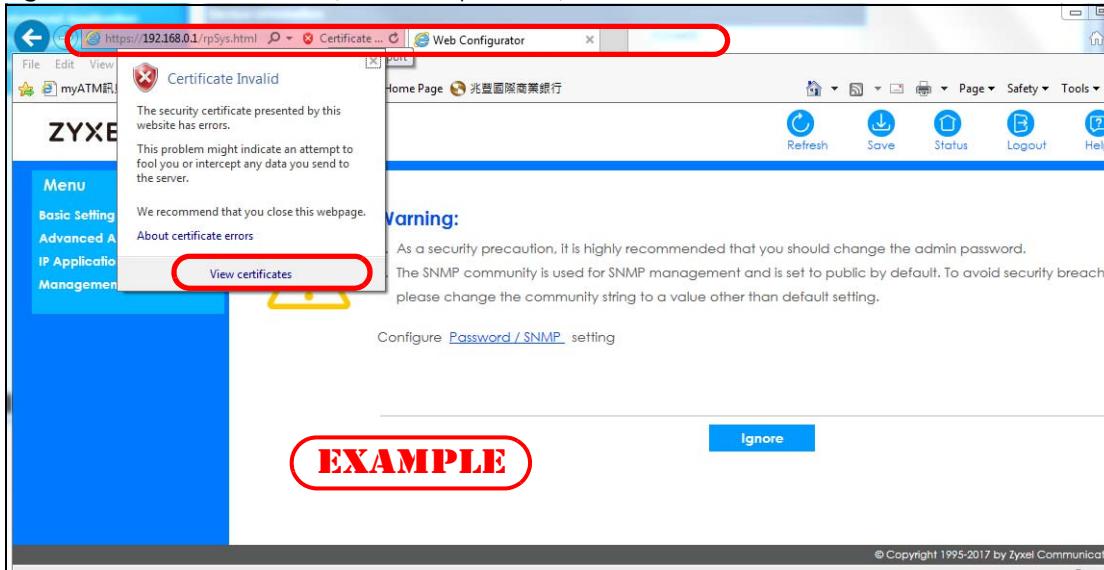
Figure 199 Security Alert Dialog Box (Internet Explorer 6)

Internet Explorer 7 later version

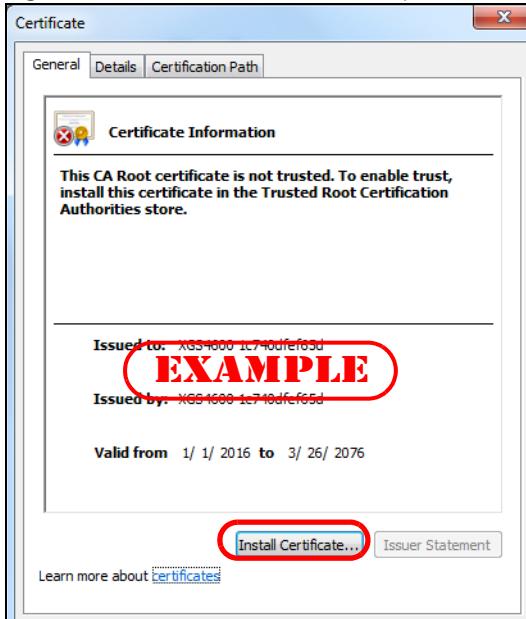
When you attempt to access the OLT HTTPS server, a screen with the message "There is a problem with this website's security certificate." may display. If that is the case, click **Continue to this website (not recommended)** to proceed to the web configurator login screen.

Figure 200 Security Certificate Warning (Internet Explorer 11)

After you log in, you will see the red address bar with the message **Certificate Error**. Click on **Certificate Error** next to the address bar and click **View certificates**.

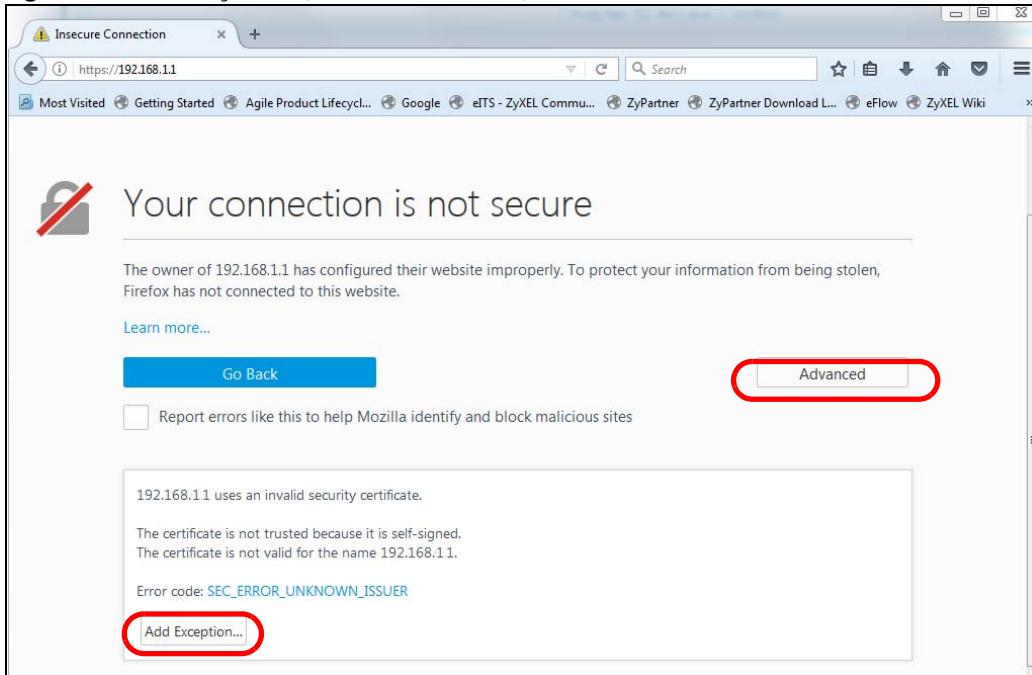
Figure 201 Certificate Error (Internet Explorer 11)

Click **Install Certificate...** and follow the on-screen instructions to install the certificate in your browser.

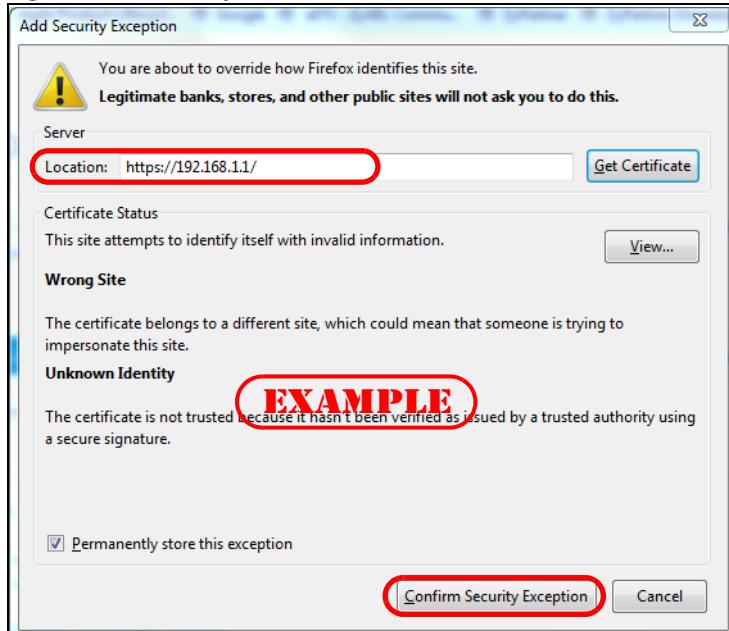
Figure 202 Certificate (Internet Explorer 11)

Mozilla Firefox Warning Messages

When you attempt to access the OLT HTTPS server, a **This Connection is Untrusted** or **Your connection is not secure** screen may display. If that is the case, click **I Understand the Risks** or **Advanced** and then the **Add Exception...** button.

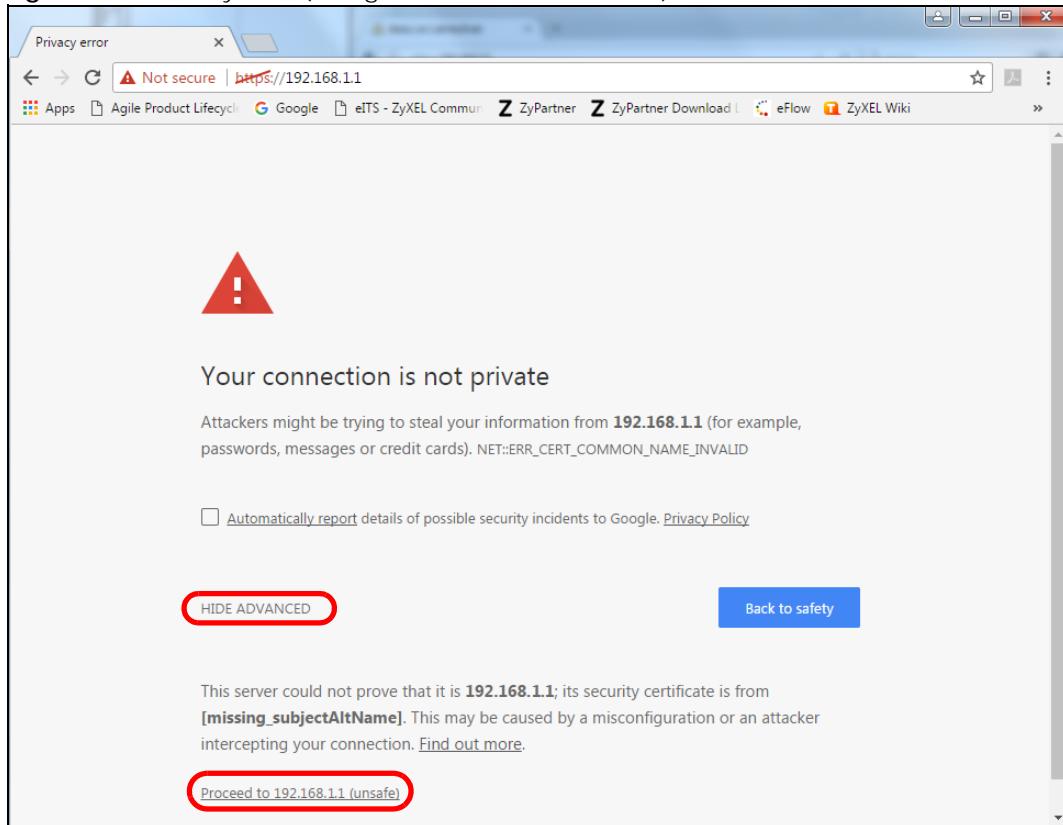
Figure 203 Security Alert (Mozilla Firefox 53.0)

Confirm the HTTPS server URL matches. Click **Confirm Security Exception** to proceed to the web configurator login screen.

Figure 204 Security Alert (Mozilla Firefox 53.0)

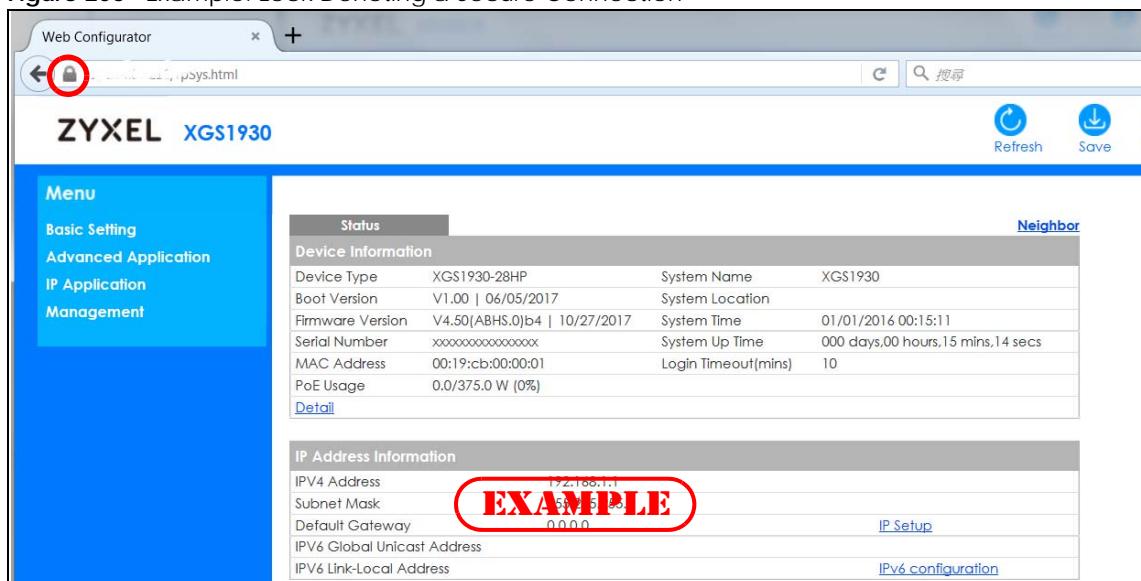
38.7.4 Google Chrome Warning Messages

When you attempt to access the OLT HTTPS server, a **Your connection is not private** screen may display. If that is the case, click **Advanced** and then **Proceed to x.x.x.x (unsafe)** to proceed to the web configurator login screen.

Figure 205 Security Alert (Google Chrome 58.0.3029.110)

38.7.4.1 The Main Screen

After you accept the certificate and enter the login username and password, the OLT main screen appears. The lock displayed in the bottom right of the browser status bar or next to the website address denotes a secure connection.

Figure 206 Example: Lock Denoting a Secure Connection

CHAPTER 39

Diagnostic

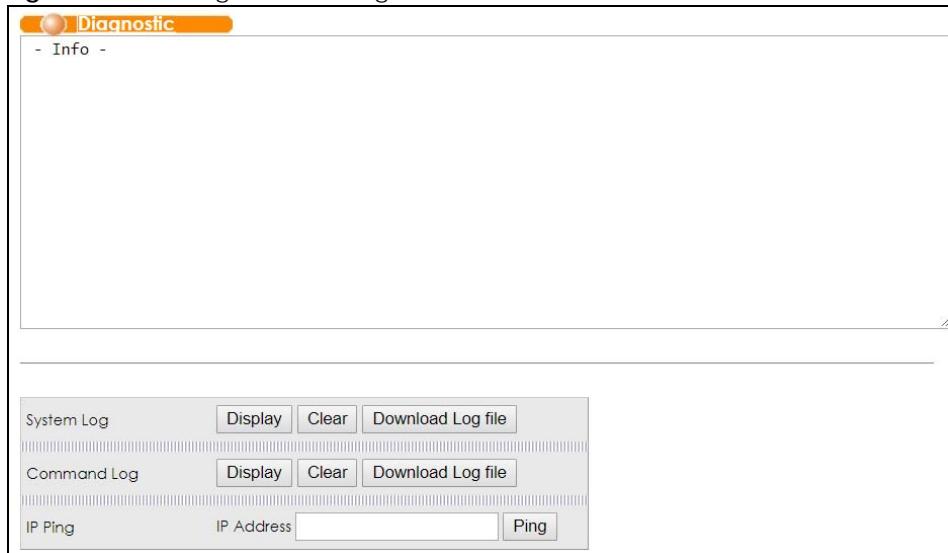
39.1 Overview

This chapter explains the **Diagnostic** screen. You can use this screen to help you identify problems.

39.2 Diagnostic

Click **Management > Diagnostic** in the navigation panel to open this screen. Use this screen to ping IP addresses. You can also use this screen to show/clear/download the OLT's system logs/command logs.

Figure 207 Management > Diagnostic



The following table describes the labels in this screen.

Table 149 Management > Diagnostic

LABEL	DESCRIPTION
System Log	Click Display to display a log of events that happened when you managed the OLT via the web configurator. Click Clear to empty the text box and reset the syslog entry. Click Download Log file to download the log file to your computer. This log file includes the events that happened when you managed the OLT via the web configurator.
Command Log	Click Display to display the commands that were executed via the console port or Telnet. Click Clear to empty the text box and reset the command log entry. Click Download Log file to download the log file to your computer. This log file includes the commands that were executed via the console port or Telnet.
IP Ping	Type the IP address of a device and then click Ping to have the OLT ping the IP address.

CHAPTER 40

Syslog Setup

40.1 Syslog Overview

This chapter explains the syslog screens.

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. The following table describes the syslog severity levels.

Table 150 Syslog Severity Levels

CODE	SEVERITY
0	Emergency: The system is unusable.
1	Alert: Action must be taken immediately.
2	Critical: The system condition is critical.
3	Error: There is an error condition on the system.
4	Warning: There is a warning condition on the system.
5	Notice: There is a normal but significant condition on the system.
6	Informational: The syslog contains an informational message.
7	Debug: The message is intended for debug-level purposes.

40.1.1 What You Can Do

- Use the **Syslog Setup** screen ([Section 40.2 on page 334](#)) to configure the device's system logging settings.
- Use the **Syslog Server Setup** screen ([Section 40.3 on page 335](#)) to configure a list of external syslog servers.
- Use the **Syslog Upload Setup** screen ([Section 40.4 on page 336](#)) to configure the settings for uploading log messages.

40.2 Syslog Setup

The syslog feature sends logs to an external syslog server. Use this screen to configure the device's system logging settings.

Click **Management > Syslog** in the navigation panel to display this screen.

Figure 208 Management > Syslog Setup

The screenshot shows the 'Syslog Setup' screen with the following interface details:

- Top Navigation:** Shows tabs for 'Syslog Setup' (highlighted in orange), 'Syslog Server Setup', and 'Syslog Upload Setup'.
- Buttons:** 'Syslog' and 'Active' (checkbox).
- Table:** A grid for configuring logging types. It has columns for 'Logging type', 'Active' (checkbox), 'Facility' (dropdown), and 'Level' (dropdown). The rows include:

Logging type	Active	Facility	Level
System	<input checked="" type="checkbox"/>	local use 0 ▾	Level 0-7 ▾
Interface	<input checked="" type="checkbox"/>	local use 0 ▾	Level 0-7 ▾
Switch	<input checked="" type="checkbox"/>	local use 0 ▾	Level 0-7 ▾
AAA	<input checked="" type="checkbox"/>	local use 0 ▾	Level 0-7 ▾
IP	<input checked="" type="checkbox"/>	local use 0 ▾	Level 0-7 ▾
Command	<input checked="" type="checkbox"/>	local use 0 ▾	Level 0-7 ▾
- Buttons at bottom:** 'Apply' and 'Cancel'.

The following table describes the labels in this screen.

Table 151 Management > Syslog Setup

LABEL	DESCRIPTION
Syslog	Select Active to turn on syslog (system logging) and then configure the syslog setting
Logging Type	This column displays the names of the categories of logs that the device can generate.
Active	Select this option to set the device to generate logs for the corresponding category.
Facility	The log facility allows you to send logs to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Level	Select the severity level(s) of the logs that you want the device to send to this syslog server. The lower the number, the more critical the logs are.
Apply	Click Apply to save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

40.3 Syslog Server Setup

Click **Management > Syslog > Syslog Server Setup** to view the screen as shown next. Use this screen to configure a list of external syslog servers.

Figure 209 Management > Syslog > Syslog Server Setup

The following table describes the labels in this screen.

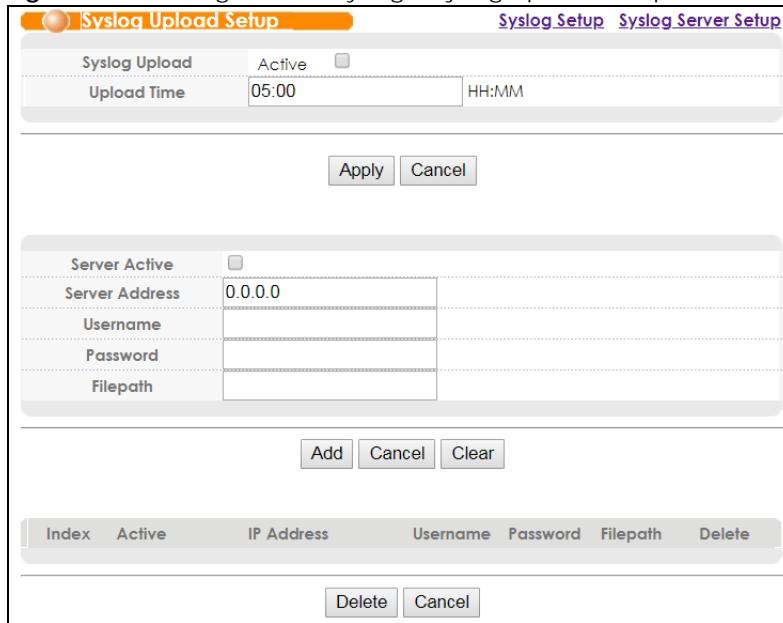
Table 152 Management > Syslog > Syslog Server Setup

LABEL	DESCRIPTION
Syslog Server Setup	
Active	Select this check box to have the OLT send logs to this syslog server immediately when these logs are generated. Clear the check box if you want to create a syslog server entry but not have the device send logs to it (you can edit the entry later).
Server Address	Enter the IPv4 address of the syslog server.
Log Level	Select the severity level(s) of the logs that you want the device to send to this syslog server. The lower the number, the more critical the logs are.
Add	Click Add to save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Clear	Click Clear to return the fields to the factory defaults.
Index	This is the index number of a syslog server entry. Click this number to edit the entry.
Active	This field displays Yes if the device is to send logs to the syslog server. No displays if the device is not to send logs to the syslog server.
IP Address	This field displays the IP address of the syslog server.
Log Level	This field displays the severity level of the logs that the device is to send to this syslog server.
Delete	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Click Delete to remove the selected entry(ies).
Cancel	Click Cancel to begin configuring this screen afresh.

40.4 Syslog Upload Setup

Click **Management > Syslog > Syslog Upload Setup** in the navigation panel to display this screen. Use this screen to set up the time when the file with log messages will be uploaded to an external syslog server. You can also set up the login information on an external syslog server.

Figure 210 Management > Syslog > Syslog Upload Setup



The following table describes the labels in this screen.

Table 153 Management > Syslog > Syslog Upload Setup

LABEL	DESCRIPTION
Syslog Upload Setup	
Syslog Upload	Select Active to upload the file with log messages to the external syslog server configured below.
Upload Time	Enter the time that you want the OLT to upload the file with log messages.
Apply	Click Apply to save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Clear	Click Clear to return the fields to the factory defaults.
Server Active	Select this to activate the syslog server.
Server Address	Enter the IPv4 address of the syslog server.
Username	Enter the username of the syslog server.
Password	Enter the password of the syslog server.
Filepath	Enter the location of the syslog server that you want the file with log messages to be uploaded to.
Add	Click Add to save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Clear	Click Clear to return the fields to the factory defaults.
Index	This field displays the index number.
Active	This displays whether the entry of the syslog server settings is active or not.
IP Address	This displays the IP address of the syslog server.
Username	This displays the username of the syslog server.
Password	This displays the password of the syslog server.
Filepath	This displays the location of the syslog server that you want the file with log messages to be uploaded to.

Table 153 Management > Syslog > Syslog Upload Setup

LABEL	DESCRIPTION
Delete	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Click Delete to remove the selected entry(ies).
Cancel	Click Cancel to begin configuring this screen afresh.

CHAPTER 41

MAC Table

41.1 MAC Table Overview

This chapter introduces the **MAC Table** screen.

The **MAC Table** screen (a MAC table is also known as a filtering database) shows how frames are forwarded or filtered across the OLT's ports. It shows what device MAC address, belonging to what VLAN group (if any) is forwarded to which port(s) and whether the MAC address is dynamic (learned by the OLT) or static (manually entered in the **Static MAC Forwarding** screen).

41.1.1 What You Can Do

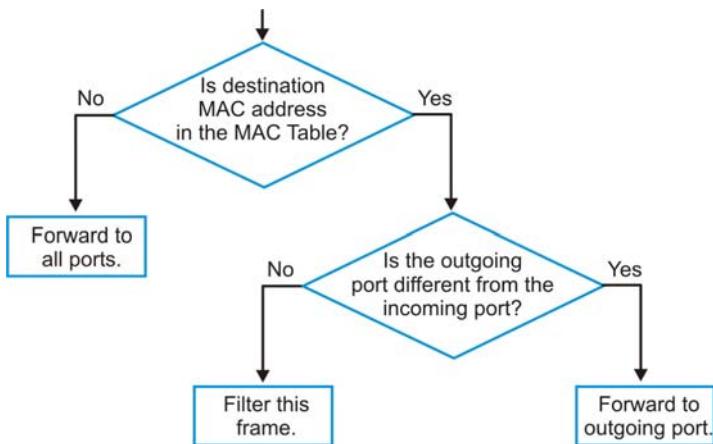
Use the **MAC Table** screen ([Section 41.2 on page 340](#)) to check whether the MAC address is dynamic or static.

41.1.2 What You Need to Know

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

- 1 The OLT examines a received frame and learns the port on which this source MAC address came.
- 2 The OLT checks to see if the frame's destination MAC address matches a source MAC address already learned in the MAC table.
 - If the OLT has already learned the port for this MAC address, then it forwards the frame to that port.
 - If the OLT 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 OLT 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 211 MAC Table Flowchart



41.2 Viewing the MAC Table

Use this screen to check whether the MAC address is dynamic or static.

Click **Management > MAC Table** in the navigation panel to display the following screen.

Figure 212 Management > MAC Table

The screenshot shows the "Management > MAC Table" configuration screen. At the top, there is a title bar with a back arrow and the text "MAC table". Below the title bar, there are several filter options:

- Condition:** Radio buttons for "All", "Static", "MAC" (with a text input field showing a MAC address), "VID" (with a dropdown menu), and "Port" (with a dropdown menu).
- Sort by:** A dropdown menu set to "MAC".
- Transfer Type:** Radio buttons for "Dynamic to MAC forwarding" (selected) and "Dynamic to MAC filtering".

At the bottom of the configuration area are four buttons: "Search", "Transfer", "Flush", and "Cancel".

Below the configuration area is a table header row with columns labeled "Index", "MAC Address", "VID", "Port", and "Type".

The following table describes the labels in this screen.

Table 154 Management > MAC Table

LABEL	DESCRIPTION
Condition	Select one of the buttons and click Search to only display the data which matches the criteria you specified. Select All to display any entry in the MAC table of the OLT. Select Static to display the MAC entries manually configured on the OLT. Select MAC and enter a MAC address in the field provided to display a specified MAC entry. Select VID and enter a VLAN ID in the field provided to display the MAC entries belonging to the specified VLAN. Select Port and enter a port number in the field provided to display the MAC addresses which are forwarded on the specified port.
Sort by	Define how the OLT displays and arranges the data in the summary table below. Select MAC to display and arrange the data according to MAC address. Select VID to display and arrange the data according to VLAN group. Select PORT to display and arrange the data according to port number.
Transfer Type	Select Dynamic to MAC forwarding and click the Transfer button to change all dynamically learned MAC address entries in the summary table below into static entries. They also display in the Static MAC Forwarding screen. Select Dynamic to MAC filtering and click the Transfer button to change all dynamically learned MAC address entries in the summary table below into MAC filtering entries. These entries will then display only in the Filtering screen and the default filtering action is Discard source .
Search	Click this to search data in the MAC table according to your input criteria.
Transfer	Click this to perform the MAC address transferring you selected in the Transfer Type field.
Flush	Select a port or all ports and click this button to clear the MAC address table to remove all learned MAC addresses on the port(s).
Cancel	Click Cancel to change the fields back to their last saved values.
Index	This is the incoming frame index number.
MAC Address	This is the MAC address of the device from which this incoming frame came.
VID	This is the VLAN group to which this frame belongs.
Port	This is the port where the above MAC address is forwarded.
Type	This shows whether the MAC address is dynamic (learned by the OLT) or static (manually entered in the Static MAC Forwarding screen).

CHAPTER 42

IP Table

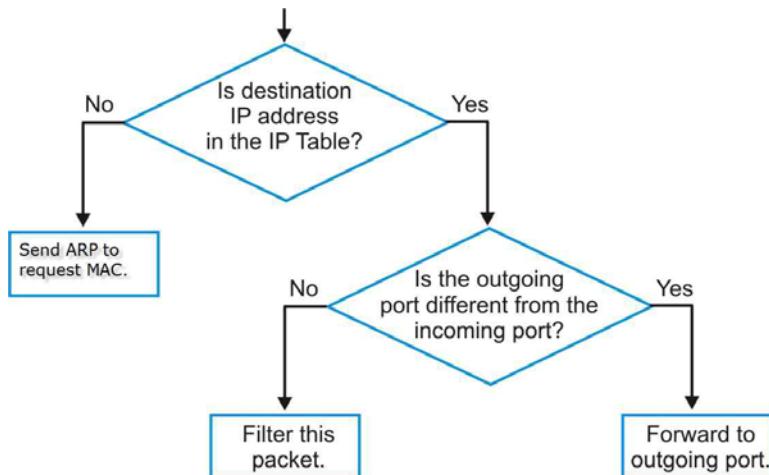
42.1 IP Table Overview

The **IP Table** screen shows how packets are forwarded or filtered across the OLT's ports. When a device (which may belong to a VLAN group) sends a packet which is forwarded to a port on the OLT, the IP address of the device is shown on the OLT's **IP Table**. The **IP Table** also shows whether the IP address is dynamic (learned by the OLT) or static (belonging to the OLT).

The OLT uses the **IP Table** to determine how to forward packets. See the following figure.

- 1 The OLT examines a received packet and learns the port from which this source IP address came.
- 2 The OLT checks to see if the packet's destination IP address matches a source IP address already learned in the **IP Table**.
 - If the OLT has already learned the port for this IP address, then it forwards the packet to that port.
 - If the OLT has not already learned the port for this IP address, then the packet is flooded to all ports. Too much port flooding leads to network congestion then the OLT sends an ARP to request the MAC address. The OLT then learns the port that replies with the MAC address.
 - If the OLT has already learned the port for this IP address, but the destination port is the same as the port it came in on, then it filters the packet.

Figure 213 IP Table Flowchart



42.2 Viewing the IP Table

Click **Management > IP Table** in the navigation panel to display the following screen.

Figure 214 Management > IP Table



The following table describes the labels in this screen.

Table 155 Management > IP Table

LABEL	DESCRIPTION
Sort by	Click one of the following buttons to display and arrange the data according to that button type. The information is then displayed in the summary table below.
IP	Click this button to display and arrange the data according to IP address.
VID	Click this button to display and arrange the data according to VLAN group.
Port	Click this button to display and arrange the data according to port number.
Index	This field displays the index number.
IP Address	This is the IP address of the device from which the incoming packets came.
VID	This is the VLAN group to which the packet belongs.
Port	This is the port from which the above IP address was learned. This field displays CPU to indicate the IP address belongs to the OLT.
Type	This shows whether the IP address is dynamic (learned by the OLT) or static (belonging to the OLT).

CHAPTER 43

ARP Table

43.1 ARP Table Overview

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.

43.1.1 What You Can Do

Use the **ARP Table** screen ([Section 43.2 on page 344](#)) to view IP-to-MAC address mapping(s).

43.1.2 What You Need to Know

When an incoming packet destined for a host device on a local area network arrives at the OLT, the OLT's ARP program looks in the ARP Table and if it finds the address, it 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 OLT 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 OLT puts all ones in the target MAC field (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.

43.2 Viewing the ARP Table

Use the ARP table to view IP-to-MAC address mapping(s) and remove specific dynamic ARP entries.

Click **Management > ARP Table** in the navigation panel to open the following screen.

Figure 215 Management > ARP Table

Index	IP Address	MAC Address	VID	Port	Type
1	1.0.0.1	5c:f4:ab:9c:e7:58	2	CPU	static
2	10.214.80.33	dc:4a:3e:40:ec:67	1	6	dynamic
3	10.214.80.37	dc:4a:3e:40:ec:5f	1	10	dynamic
4	10.214.80.211	5c:f4:ab:9c:e7:58	1	CPU	static
5	192.168.1.1	5c:f4:ab:9c:e7:58	1	CPU	static

The following table describes the labels in this screen.

Table 156 Management > ARP Table

LABEL	DESCRIPTION
Condition	Specify how you want the OLT to remove ARP entries when you click Flush . Select All to remove all of the dynamic entries from the ARP table. Select IP Address and enter an IP address to remove the dynamic entries learned with the specified IP address. Select Port and enter a port number to remove the dynamic entries learned on the specified port.
Flush	Click Flush to remove the ARP entries according to the condition you specified.
Cancel	Click Cancel to return the fields to the factory defaults.
Index	This is the ARP table entry number.
IP Address	This is the IP address of a device connected to a OLT port with the corresponding MAC address below.
MAC Address	This is the MAC address of the device with the corresponding IP address above.
VID	This field displays the VLAN to which the device belongs.
Port	This field displays the port to which the device connects. CPU means this IP address is the OLT's management IP address.
Type	This shows whether the IP address is dynamic (learned by the OLT) or static (manually configured in the Basic Setting > IP Setup screen).

CHAPTER 44

Routing Table

44.1 Overview

The routing table contains the route information to the network(s) that the OLT can reach.

44.2 Viewing the Routing Table Status

Use this screen to view routing table information. Click **Management > Routing Table** in the navigation panel to display the screen as shown.

Figure 216 Management > Routing Table

Routing Table Status					
Index	Destination	Gateway	Interface	Metric	Type
1	192.168.1.0/24	192.168.1.1	192.168.1.1	1	STATIC
2	10.214.80.0/24	10.214.80.211	10.214.80.211	1	STATIC
3	1.0.0.0/16	1.0.0.1	1.0.0.1	1	STATIC

The following table describes the labels in this screen.

Table 157 Management > Routing Table

LABEL	DESCRIPTION
Index	This field displays the index number.
Destination	This field displays the destination IP routing domain.
Gateway	This field displays the IP address of the gateway device.
Interface	This field displays the IP address of the Interface.
Metric	This field displays the cost of the route.
Type	This field displays the method used to learn the route. STATIC - added as a static entry. LOCAL - added as a local entry.

CHAPTER 45

Battery

45.1 Overview

Use this screen to set up the OLT battery capacity and temperature threshold, and view its status.

45.2 The Battery Setup Screen

Use this screen to set up the OLT battery capacity and temperature threshold, and view its status.

Click **Management > Battery** in the navigation panel to display the screen as shown.

Figure 217 Management > Battery

Type Threshold	Current	High Alarm	Low Alarm
Temperature	No thermal sensor	40	0 (50 ~ -15 C)

Power Information	
Power Source	AC
System Power Consumption	36134 (mW)
Battery Charging Power	- (mW)

Battery Information	
Battery Absent	Absent
Battery Temperature	- (C)
Battery Voltage	- (mV)
Battery Status	-
Battery Information Validation	-

Charger Information	
Charger Status	OFF
Charge Current	- (mA)
Charge Voltage	- (mV)
Charge Time	- (sec)
Trickle Charge	-

The following table describes the labels in this screen.

Table 158 Management > Battery

LABEL	DESCRIPTION
Capacity	<p>Enter a value in the range of 7-18 Ah (ampere hour) for the battery capacity. This determines the amount of electric current that can be provided for a period of time.</p> <p>Please pay attention to the following notes:</p> <ul style="list-style-type: none"> • A value must be entered here to charge the connected battery. • The value entered here must be within the range of 7-18 Ah to charge the connected battery correctly. • If the entered value here is smaller than the real capacity, the connected battery will not be fully charged. • If the entered value here is larger than the real capacity, the connected battery will be damaged. The battery life could be shortened.
Apply	Click Apply to save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Reset	Click Reset to reset the fields back to their default values.
Type Threshold	This displays the type of device operating parameter.
Current	This shows the current value of each parameter measured by the installed sensor. If there is no sensor connected, it displays No thermal sensor .
High Alarm	Enter the upper limit for each parameter. The OLT sends an alarm when the parameter values goes over this limit.
Low Alarm	Enter the lowest limit for each parameter. The OLT sends an alarm when the parameter value is below this limit. This value should be smaller than the High Alarm .
Apply	Click Apply to save your changes to the OLT's run-time memory. The OLT loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Reset	Click Reset to reset the fields back to their default values.
Battery Status	
Power Information	
The following fields display the current values and status of the OLT battery.	
Power Source	<p>This displays AC when the input power source detected is via an AC power line.</p> <p>This displays DC when the input power source detected is via an DC power line.</p> <p>This displays Battery when the input power source detected is a battery.</p>
System Power Consumption	This field displays the current power consumption (in mW) of the OLT, and it varies depending on the items currently connected to the OLT' ports.
Battery Charging Power	This field displays how much (in mW) the battery has charged.
Battery Information	
Battery Absent	<p>This displays Absent if there is no battery connection detected by the OLT.</p> <p>This displays Not Absent when there is a battery connection detected by the OLT.</p>
Battery Temperature	This displays the current battery temperature detected by the sensor.
Battery Voltage	This displays the current battery voltage detected by the sensor.
Battery Status	<p>This displays Healthy when the battery is working normally.</p> <p>This displays Unhealthy when the battery voltage is under the alarm threshold.</p>

Table 158 Management > Battery

LABEL	DESCRIPTION
Battery Information Validation	This displays Invalid when there is no battery connection detected or the battery is over the voltage and temperature threshold.
Charger Information	
Charger Status	This displays ON when the charger is currently charging the battery. This displays OFF when the charger is off.
Charge Current	This displays the charger's present current value (in mA).
Charge Voltage	This displays the charger's current voltage value (in mV).
Charge Time	This is the time (in seconds) remaining for the battery to be completely charged.
Trickle Charge	This displays ON when the trickle charge is activated. This means that when the battery charge reaches 95% of its capacity, it will enter float mode. In float mode the OLT lowers the battery's charge voltage to protect the battery. This displays OFF when trickle charge is disabled.

PART III

CLI Commands

About This CLI Reference Guide

Intended Audience

This manual is intended for people who want to configure the OLT via Command Line Interface (CLI).

How To Use This Guide

- Use this guide for command syntax, description and examples. Each chapter describes commands related to a feature.

Document Conventions

Syntax Conventions

This manual follows these general conventions:

- Units of measurement may denote the “metric” value or the “scientific” value. For example, “k” for kilo may denote “1000” or “1024”, “M” for mega may denote “1000000” or “1048576” and so on.

Command descriptions follow these conventions:

- Commands are in `courier new font`.
- Required input values are in angle brackets `<>`; for example, `ping <ip>` means that you must specify an IP address for this command.
- Optional fields are in square brackets `[]`; for instance `show logins [name]`, the name field is optional. The following is an example of a required field within an optional field: `snmp-server [contact <system contact>]`, the contact field is optional. However, if you use contact, then you must provide the `system contact` information.
- 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.
- The `|` (bar) symbol means “or”.
- italic* terms represent user-defined input values; for example, in `snmp-server [contact <system contact>]`, `system contact` can be replaced by the administrator’s name.
- A key stroke is denoted by square brackets and uppercase text, for example, `[ENTER]` means the “Enter” or “Return” key on your keyboard.
- `<cr>` means press the `[ENTER]` key.
- An arrow (`-->`) indicates that this line is a continuation of the previous line.

Command summary tables are organized as follows:

Table 159 Example: Command Summary Table

COMMAND	DESCRIPTION	M	P
<code>show vlan</code>	Displays the status of all VLANs.	E	3
<code>vlan <1-4094></code>	Enters config-vlan mode for the specified VLAN. Creates the VLAN, if necessary.	C	13
<code> inactive</code>	Disables the specified VLAN.	C	13
<code> no inactive</code>	Enables the specified VLAN.	C	13
<code>no vlan <1-4094></code>	Deletes a VLAN.	C	13

The **Table** title identifies commands or the specific feature that the commands configure.

The **COMMAND** column shows the syntax of the command.

- If a command is not indented, you run it in the enable or config mode. See [Chapter 49 on page 359](#) for more information on command modes.
- If a command is indented, you run it in a sub-command mode.

The **DESCRIPTION** column explains what the command does. It also identifies legal input values, if necessary.

The **M** column identifies the mode in which you run the command.

- **E:** The command is available in enable mode. It is also available in user mode if the privilege level (**P**) is less than 13.
- **C:** The command is available in config (not indented) or one of the sub-command modes (indented).

The **P** column identifies the privilege level of the command. If you don't have a high enough privilege level you may not be able to view or execute some of the commands. See [Chapter 49 on page 359](#) for more information on privilege levels.

CHAPTER 46

How to Access and Use the

CLI

This chapter introduces the command line interface (CLI).

46.1 Accessing the CLI

Use any of the following methods to access the CLI.

46.1.1 Console Port

- 1 Connect your computer to the console port on the OLT using the appropriate cable. (See [Section 3.1.4 on page 47](#) for console cable details).
- 2 Use terminal emulation software with the settings listed in [Section 3.1.4 on page 47](#).
- 3 Press [ENTER] to open the login screen.

46.1.2 Local Telnet

- 1 Connect your computer to one of the **MGMT** port.
- 2 Open a Telnet session to the OLT's out-of-band **MGMT** port IP address. If this is your first login, use the default values.

Table 160 Default Management IP Address

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 OLT through one or more routers.

46.1.3 Remote Telnet

- 1 Connect to the OLT through an uplink or GE port.
- 2 Open a Telnet session to the OLT's in-band management IP address.

Table 161 Default In-band Management IP Address

SETTING	DEFAULT VALUE
IP Address	192.168.1.1
Subnet Mask	255.255.255.0

Make sure your computer IP address is in the same subnet, unless you are accessing the OLT through one or more routers.

46.1.4 SSH

- 1 Connect your computer to one of the Ethernet ports.
- 2 Use an SSH client program to access the OLT. If this is your first login, use the default values in [Table 161 on page 355](#) and the user name and password on the cover of this document. Make sure your computer IP address is in the same subnet, unless you are accessing the OLT through one or more routers.

46.2 Logging in

Use the user name and password on the cover of this document for the first login.

Note: The OLT automatically logs you out of the management interface after five minutes of inactivity. If this happens to you, simply log back in again.

46.3 Using Shortcuts and Getting Help

This table identifies some shortcuts in the CLI, as well as how to get help.

Table 162 CLI Shortcuts and Help

COMMAND / KEY(S)	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]+U	Clears the current command.
[CTRL]+Z	Returns to the previous mode.
[TAB]	Auto-completes the keyword you are typing if possible. For example, type config, and press [TAB]. The OLT finishes the word configure.
?	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 help.

46.4 Dual Image Files

The OLT supports dual firmware images.

Use the `show version [flash]` command to display the version of the running firmware on the OLT. Optionally, display the version of the currently installed firmware on the flash memory.

Use `boot image <1|2>` to have the OLT update firmware image 1 or 2 when you upload firmware.

46.5 Dual Configuration Files

The OLT has a start-up configuration file and a passive configuration file. The running configuration is based on the start-up configuration file. These two configuration files are different from the “default” configuration (the system’s built-in configuration included with the firmware). The OLT starts with the default configuration and customizes it with the start-up configuration file’s settings to build the running configuration.

Use `reload config <1|2>` to load configuration file 1 or configuration file 2 into running configuration without restarting.

Use `boot config [1|2]` to restart the OLT (cold reboot) with the specified configuration file.

See [Chapter 77 on page 543](#) and [Chapter 84 on page 572](#) for more on managing the running configuration file.

46.6 Saving Your Configuration

When you run a command, the OLT saves any changes to its run-time memory. The OLT 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.

```
sysname# write memory
```

Note: You should save your changes after each CLI session. All unsaved configuration changes are lost once you restart the OLT.

46.7 Logging Out

Enter `logout` to log out of the CLI. You have to be in user, enable, or config mode. See [Chapter 47 on page 357](#) for more information about modes.

CHAPTER 47

Privilege Level and Command Mode

This chapter introduces the CLI privilege levels and command modes.

- The privilege level determines whether or not a user can run a particular command.
- If a user can run a particular command, the user has to run it in the correct mode.

47.1 Privilege Levels

Every command has a privilege level (0-14). Users can run a command if the session's privilege level is greater than or equal to the command's privilege level. The session's privilege level initially comes from the login account's privilege level, though it is possible to change the session's privilege level after logging in.

47.1.1 Privilege Levels for Commands

At the time of writing, commands have a privilege level of 0, 3, 13, or 14. The following table summarizes the types of commands at each of these privilege levels.

Table 163 Types of Commands at Different Privilege Levels

PRIVILEGE LEVEL	TYPES OF COMMANDS AT THIS PRIVILEGE LEVEL
0	Display basic system information.
3	Display configuration or status.
13	Configure features except for login accounts, SNMP user accounts, the authentication method sequence and authorization settings, multiple logins, administrator and enable passwords, and configuration information display.
14	Configure login accounts, SNMP user accounts, the authentication method sequence and authorization settings, multiple logins, and administrator and enable passwords, and display configuration information.

47.1.2 Privilege Levels for Login Accounts

You can manage the privilege levels for login accounts in the following ways:

- Using commands. Login accounts can be configured by the **admin** account or any login account with a privilege level of 14. See [Chapter 78 on page 552](#).
- Using vendor-specific attributes in an external authentication server. See the User's Guide for more information.

The **admin** account has a privilege level of 14, so the administrator can run every command. You cannot change the privilege level of the **admin** account.

47.1.3 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 OLT. After logging in, the user can use the following commands to change the session's privilege level.

47.1.3.1 enable Command

This command raises the session's privilege level to 14. It also changes the session to enable mode (if not already in enable mode). This command is available in user mode or enable mode, and users have to know the enable password.

In the following example, the login account **user0** has a privilege level of 0 but knows that the enable password is **123456**. Afterwards, the session's privilege level is 14, instead of 0, and the session changes to enable mode.

```
sysname> enable  
Password: 123456  
sysname#
```

The default enable password is **1234**. Use this command to set the enable password.

```
password <password>
```

<password> consists of 1-32 alphanumeric characters. For example, the following command sets the enable password to **123456**. See [Chapter 78 on page 553](#) for more information about this command.

```
sysname(config)# password 123456
```

The password is sent in plain text and stored in the OLT's buffers. Use this command to set the cipher password for password encryption.

```
password cipher <password>
```

<password> consists of 32 alphanumeric characters. For example, the following command encrypts the enable password with a 32-character cipher password. See [Chapter 78 on page 553](#) for more information about this command.

```
sysname(config)# password cipher qwertyuiopasdfghjklzxcvbnm123456
```

47.1.3.2 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 account **user0** 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.

```
sysname> enable 13  
Password: pswd13  
sysname#
```

Users cannot use this command until you create passwords for specific privilege levels. Use the following command to create passwords for specific privilege levels.

```
logins username <name> password <password> privilege <0-14>
```

<password> consists of 1-32 alphanumeric characters. For example, the following command sets the password for privilege level 13 to **pswd13**. See [Chapter 78 on page 552](#) for more information about this command.

```
sysname(config)# logins username admin password pswd13 privilege 13
```

47.1.3.3 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.

47.1.3.4 show privilege command

This command displays the session's current privilege level. This command is available in user mode or enable mode.

```
sysname# show privilege  
Current privilege level : 14
```

47.2 Command Modes

The CLI is divided into several modes. If a user has enough privilege to run a particular command, the user has to run the command in the correct mode. The modes that are available depend on the session's privilege level.

47.2.1 Command Modes for Privilege Levels 0-12

If the session's privilege level is 0-12, the user and all of the allowed commands are in user mode. Users do not have to change modes to run any allowed commands.

47.2.2 Command Modes for Privilege Levels 13-14

If the session's privilege level is 13-14, the allowed commands are in one of several modes.

Table 164 Command Modes for Privilege Levels 13-14 and the Types of Commands in Each One

MODE	PROMPT	COMMAND FUNCTIONS IN THIS MODE
enable	sysname#	Display current configuration, diagnostics, maintenance.
config	sysname(config)#	Configure features other than those below.
config-interface	sysname(config-interface)#	Configure ports.
config-route-domain	sysname(config-if)#	Enable and enter configuration mode for an IPv4 or IPv6 routing domain.
config-ospf	sysname(config-ospf)#	Configure Open Shortest Path First (OSPF) protocol.
config-rip	sysname(config-rip)#	Configure Routing Information Protocol (RIP).
config-vlan	sysname(config-vlan)#	Configure the VLAN settings on a port
config-olt	sysname(config-olt)#	Configure settings on the OLT.
config-uniport	sysname(config-uniport)#	Configure UNI port settings.
config-transceiver	sysname(config-transceiver)#	Configure the interface transceiver threshold settings.
config-ont	sysname(config-ont)#	Configure remote ONT settings.
config-remote-uniport	sysname(config-remote-uniport)#	Configure remote UNI port settings.
config-remote-giga-uniport	sysname(config-remote-giga-uniport)#	Configure card 1 settings of the remote UNI port.
config-remote-veip-uniport	sysname(config-remote-veip-uniport)#	Configure card 2 settings of the remote UNI port.
config-remote-pots-uniport	sysname(config-remote-pots-uniport)#	Configure card 3 settings of the remote UNI port.
config-remote-video-uniport	sysname(config-remote-video-uniport)#	Configure card 4 settings of the remote UNI port.
config-remote-ether-uniport	sysname(config-remote-ether-uniport)#	Configure card 5 settings of the remote UNI port.

Each command is usually in one and only one mode. If a user wants to run a particular command, the user has to change to the appropriate mode. The command modes are organized like a tree, and users start in enable mode. The following table explains how to change from one mode to another.

Table 165 Changing Between Command Modes for Privilege Levels 13-14

MODE	ENTER MODE	LEAVE MODE
enable	--	--
config	configure	exit
config-interface	interface port-channel <port-list>	exit
config-vlan	vlan <1-4094>	exit
config-ospf	router ospf <router-id>	exit
config-rip	router rip	exit
config-olt	interface olt <aid>	exit

Table 165 Changing Between Command Modes for Privilege Levels 13-14 (continued)

MODE	ENTER MODE	LEAVE MODE
config-uniport	interface uni-port <aid>	exit
config-transceiver	interface transceiver-ddmi <aid>	exit
config-ont	remote ont <aid>	exit
config-remote-uniport	remote uniport <aid>	exit
config-remote-giga-uniport	remote uniport uniport <aid> aid: uniport-<pon>-<ont>-<1>-<port> Note: You need to configure remote ONTs' settings first, so you can set up a remote uniport.	exit
config-remote-veip-uniport	remote uniport uniport <aid> aid: uniport-<pon>-<ont>-<2>-<port> Note: You need to set the OLT PON port's register method first.	exit
config-remote-pots-uniport	remote uniport uniport <aid> aid: uniport-<pon>-<ont>-<3>-<port> Note: You need to set the OLT PON port's register method first.	exit
config-remote-video-uniport	remote uniport uniport <aid> aid: uniport-<pon>-<ont>-<4>-<port> Note: You need to set the OLT PON port's register method first.	exit
config-remote-ether-uniport	remote uniport uniport <aid> aid: uniport-<pon>-<ont>-<5>-<port> Note: You need to set the OLT PON port's register method first.	exit

47.3 Listing Available Commands

Use the `help` command to view the executable commands on the OLT. You must have the highest privilege level in order to view all the commands. Follow these steps to create a list of supported commands:

- 1 Log into the CLI. This takes you to the enable mode.
- 2 Type `help` and press [ENTER]. A list comes up which shows all the commands available in enable mode. The example shown next has been edited for brevity's sake.

```
sysname# help
Commands available:

help
exit
history
enable <0-14>
enable <cr>
disable
configure
mgmt-ont-img
fan <0-100>
fan auto
renew dhcp snooping database <tftp://host/filename>
renew dhcp snooping database <cr>
clear loopguard <cr>
clear logging <cr>
clear cmd-logging <cr>
clear arp inspection filter
clear arp inspection log
clear arp inspection statistics <cr>
clear arp inspection statistics vlan <vlan-list>
clear interface <aid>
clear ip arp <cr>
clear ip arp interface port-channel <port-list>
clear ip arp ip <ip-address>
-- more --, next page: Space, continue: c, quit: ESC
```

- 3 Copy and paste the results into a text editor of your choice. This creates a list of all the executable commands in the user and enable modes.
- 4 Type `configure` and press [ENTER]. This takes you to the config mode.
- 5 Type `help` and press [ENTER]. A list is displayed which shows all the commands available in config mode and all the sub-commands. The sub-commands are preceded by the command necessary to enter that sub-command mode. For example, the command name `<name-str>` as shown next, is preceded by the command used to enter the config-vlan sub-mode: `vlan <1-4094>`.

```
sysname# help
.
.
help
history
exit
no ip inband address <ip> <mask> <gateway> <vlan> <cr>
no ip <cr>
no ip route <ip> <mask> <cr>
no ip route <ip> <mask> inactive
no ip route <ip> <mask> <next-hop-ip> <cr>
no ip route <ip> <mask> <next-hop-ip> inactive
no ip source binding <mac-addr> vlan <vlan-id>
no ip load-sharing <cr>
no mac-forward mac <mac-addr> vlan <vlan-id> interface <interface-id>
<cr>
no mac-forward mac <mac-addr> vlan <vlan-id> interface <interface-id>
inactive
no mac-filter mac <mac-addr> vlan <vlan-id> <cr>
no mac-filter mac <mac-addr> vlan <vlan-id> inactive
no mirror-port
no lacp
no trunk <T1|T2|T3|T4|T5|T6|T7|T8|T9|T10|T11|T12> <cr>
no trunk <T1|T2|T3|T4|T5|T6|T7|T8|T9|T10|T11|T12> lacp <cr>
no trunk <T1|T2|T3|T4|T5|T6|T7|T8|T9|T10|T11|T12> interface <aid>
no trunk <T1|T2|T3|T4|T5|T6|T7|T8|T9|T10|T11|T12> criteria <cr>
no bcp-transparency
no storm-control
-- more --, next page: Space, continue: c, quit: ESC
```

- 6 Copy and paste the results into a text editor of your choice. This creates a list of all the executable commands in config and the other submodes, for example, the config-vlan mode.

CHAPTER 48

Provisioning User Interfaces

This chapter gives basic examples of provisioning subscriber data interfaces on an ONT or MDU. See [Section 73.8 on page 519](#) for an example of provisioning a ONT subscriber VoIP port. See [Chapter 87 on page 580](#) for more details on configuring remote ONTs.

48.1 ONT Subscriber Port Provisioning Example Overview

Here is an outline of how to provision a subscriber port on an ONT.

- 1 Configure the PON port with the correct transceiver type.
- 2 Register the ONT on the OLT.
- 3 Configure the QoS ingress profile and bandwidth profiles.
- 4 Associate the bandwidth profiles with the ONT.
- 5 Configure and enable a subscriber port on the ONT.
- 6 Configure a VLAN with the PON port and uplink port as fixed members.
- 7 Configure the subscriber port's QoS and VLAN settings.

See [Section 104.1 on page 660](#) for GPON port status troubleshooting.

After you have a subscriber port configured and working properly, you can use FTP to get the configuration file (See [Chapter 77 on page 543](#)) and configure other subscriber ports in a text editor.

48.2 ONT Subscriber Port Provisioning Example

This example configures **PON1** on the OLT.

- 1 Set the method (A, C, C-autolock, D, or E) the OLT registers ONTs connected to the port.
 - A: (Used in this example) requires the serial number and password the ONT sends to match the ones you configure on the OLT.
 - C: The ONT must match either the serial number or the password configured on the OLT.
 - C-autolock: Requires the serial number the ONT sends to match the one you configure on the OLT.

- D: Automatically registers the ONT and brings it into service without checking the serial number or password. The ONT may receive a different ONT ID when it reconnects.
- E: Automatically registers the ONT and brings it into service without checking the serial number or password. The OLT records the SN/ONT ID mapping and uses the same ONT ID for the ONT when it reconnects.

If you select method D or E, create a template with a number between 121 and 128, and enable the PON port.

```
sysname# config
sysname(config)# interface olt pon-1
sysname(config-olt)# register-method e
sysname(config-olt)# register-method template-option 121
sysname(config-olt)# no
sysname(config-olt)# no inactive
sysname(config-olt)# exit
sysname(config)# exit
```

Check the PON port's status.

2 Configure the QoS ingress profile and bandwidth profiles and then check the configuration.

```
sysname(config-olt)# register-method e
sysname(config-olt)# no inactive
sysname(config-olt)# exit
sysname(config)# exit
sysname# show interface pon-1
AID          | Link      Status     LACP    TxPkts   RxPkts   Errors    Tx_KBs/s
Rx_KBs/s Up_Time
-----
pon-1        | 2500M/F   FORWARDING  None      0         0         0         0.0
0.0          0:05:42
-----
| Details
-----
| TX Packet   Unicast : 0           RX Packet   Unicast : 0
|             Multicast : 0          Multicast : 0
|             Broadcast : 0         Broadcast : 0
|             Pause    : 0           Pause    : 0
|             Tagged   : 0           Control   : 0
|             Octets   : 0           Octets   : 0
| TX Collision Single  : 0          Distribution 64 : 0
|                 Multiple : 0        65-127   : 0
|                 Excessive : 0       128-255  : 0
|                 Late    : 0          256-511   : 0
| Error Packet RX CRC  : 0          512-1023 : 0
|                 Length   : 0        1024-1518 : 0
|                 Runt    : 0          Giant    : 0
-----
```

- **ingprof:** The QoS ingress profile maps IEEE 802.1p priority tags to traffic classes. This example's "voip" QoS ingress profile maps IEEE 802.1p tags 0 to 7 to traffic class 1.

- bwprof: Bandwidth profiles have Sustained Information Rate (SIR), Access Information Rate (AIR), and Peak Information Rate (PIR) settings for limiting bandwidth.
 - This example creates a “1G” QoS bandwidth profile which sets the SIR to 1024 kbps and limits the AIR to 2048 kbps and the PIR to 1000000 kbps. In this step’s final output you can see some other bandwidth profiles are already configured.
 - QoS queues use bandwidth profiles to manage the bandwidth of individual traffic classes within the bandwidth groups. This example creates a “voice” QoS bandwidth profile which sets the SIR to 128 kbps and limits the AIR and PIR both to 256 kbps. You could configure other bandwidth profiles for traffic like Movies on Demand (MoD) and data.

```

sysname# config
sysname(config)# qos ingprof voip dot1p0tc 1 dot1p1tc 1 dot1p2tc 1 dot1p3tc 1
dot1p4tc 1 dot1p5tc 1 dot1p6tc 1 dot1p7tc 1
sysname(config)# qos bwprof 1G sir 1024 air 2048 pir 1000000
sysname(config)# qos bwprof voice sir 128 air 256 pir 256
sysname(config)# exit
sysname# show qos ingprof
Index Active Name                               Value
      1 Yes    DEFVAL                         DOT1P0TC=1, DOT1P1TC=1, DOT1P2TC=1,
DOT1P3TC=1, DOT1P4TC=1, DOT1P5TC=1, DOT1P6TC=1, DOT1P7TC=1

      2 Yes    voip                           DOT1P0TC=1, DOT1P1TC=1, DOT1P2TC=1,
DOT1P3TC=1, DOT1P4TC=1, DOT1P5TC=1, DOT1P6TC=1, DOT1P7TC=1

sysname# show qos Bwprof
Index Active Name     SIR     AIR     PIR
-----  -----  -----  -----  -----
      1 Yes      1G    1024   2048  1000000
      2 Yes    DEFVAL   1024    1024   2048
      3 Yes    voice     128     256     256

```

- 3 Configure the remote ONT’s provisioning and bandwidth group settings. (When you configure “remote ONT” settings, the OLT configures the ONT with those settings.) This example uses:
 - **PON1**, ONT 101.
 - sn: serial number, 5A59584549007102 in this example.
 - pa: password, 10 ASCII characters (Or 20 hexadecimal characters), 44454641554C54000000 in this example.
 - bwgroup: Number 1-40 of the bandwidth group on this ONT you are creating to specify upstream and downstream bandwidth profiles to limit the ONT’s bandwidth. This example uses 1 because it is the first bandwidth group the example configures for the ONT.
 - type: Bandwidth group type from the following table. Use the one that matches your bandwidth profile’s settings. This example uses type 5 which applies the SIR and AIR and uses a PIR greater than the SIR and AIR added together.

Table 166 Bandwidth Group Types

TYPE 1	TYPE 2	TYPE 3	TYPE 4	TYPE 5
SIR				SIR
	AIR	AIR		AIR
PIR=SIR	PIR=AIR	PIR>AIR	PIR	PIR>=SIR+AIR

- usbwprofname: Bandwidth profile this bandwidth group applies to upstream traffic, 1G. Note, the total SIR bandwidth reserved for the ONTs on a PON cannot exceed the PON’s bandwidth.

- dsbwprofilename: Bandwidth profile this bandwidth group applies to downstream traffic, 1G. Note, the total SIR bandwidth reserved for the ONTs on a PON cannot exceed the PON's bandwidth.

Then enable the ONT and check the ONT's registration status and bandwidth group information.

```
sysname# config
sysname(config)# remote ont ont-1-101
sysname(config-ont)# sn 5A59584549007102
sysname(config-ont)# pa 44454641554C54000000
sysname(config-ont)# bwgroup 1 type 5 usbwprofilename 1G dsbwprofilename 1G
sysname(config-ont)# no inactive
sysname(config-ont)# exit
sysname(config)# exit
sysname# show remote ont ont-1-101

-----+-----+-----+-----+-----+-----+-----+-----+-----+
AID | Type SN Password Status Image Active Version Vendor/Model
-----+-----+-----+-----+-----+-----+-----+-----+-----+
--- ont-1-101 | Config 5A59584549007102 | DEFAULT Active | 1 V V100AALJ1b1 | ZYXE
| Actual 5A59584549007102 | DEFAULT IS | 2 V100AALJ1b1 | PMG1006-B20A
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
--- | Details
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
--- | Status : IS
| Estimated distance : 0 m
| OMCI GEM port : 125
| Model : 1
| Full bridge : disable
| Alarm profile : DEFVAL
| Anti MAC Spoofing : disable
| Planned Version :
| Description :
| Template Description :
| Management IP Address : N/A
| PPPoE status : N/A
| IP address : 0.0.0.0
-----+-----+-----+-----+-----+-----+-----+-----+-----+
---
```

```

sysname# show interfaces olt pon-6-1 status
AID | State Key_Exchange SN_Acq Rogue_Detect Rogue_Destruct Proc_Interval Proc_Interval_Sec LOS
-----+-----+-----+-----+-----+-----+-----+-----+-----+
pon-1-101 | ACTIVE Enable Enable Disable Disable 8000 86400 ON
-----+-----+-----+-----+-----+-----+-----+-----+-----+
--- | Details
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| (Optical Statistics) Last 8 (bytes): 4
| (Optical Statistics) End of burst offset: 15
| Protocol Configuration:
| Min round trip propagation delay(ms) : 0 Min ONU response time (ms) : 9
| Number of EqB measurement cycles : 5 Power level mode(0=0db,1=3db,2=6db) : 0
| Drift control interval : 1000 Drift control limit : 4
| Number of guard bits : 64 SR DBA reporting block size : 48
| Multicast port encryption conf : enable US BER interval : 5000
| DS BER interval : 5000 BER SF threshold : 7
| BER SD threshold : 8 ACK timeout : 2000
| PLS max allocation size : 120 Number of tx preamble : 0x00001810
| Type 3 preamble pattern : 0xaa PON link include US FEC : disable
| Key exchange : enable Password request : enable
| Disable onu after discovery : false Transmission control limit : 8
| Protection switch timeout : 0 LOS GPIO Pin : 65535
| Deactivate When Password Auth Fail : enable Key exchange for encrypted ports : disable
| los initial value : off :
| Link Configuration:
| Max round trip propagation delay(ms) : 200 Max onu response time(ms) : 50
| Preassigned EqD (0-up) : 0 LOS alpha : 4
| LOF alpha : 4 LOAM alpha : 3
| Delimiter min ED threshold(0x0-0x28) : 0x0 Delimiter max ED threshold(0x0-0x28) : 0x29
| Delimiter window size(0x0-0x7F) : 0x45 ED pattern : 0xaa
| ED size (0-2) : 0 ED window size(0x0-0x80) : 0x80
| BCDR resync pattern size(0x0-0x1F) : 0x3 BCDR ranging pattern size(0x0-0x1F) : 0x8
| BCDR Resync location(0x6-0xA0) : 0x28 BCDR Resync polarity(low|high) : low
| BCDR Ranging polarity(low|high) : low LA resync pattern size (0x0-0x7F) : 0x8
| LA ranging pattern size (0x0-0x7F) : 0x10 LA Resync location (0x6-0xA0) : 0x25
| LA Resync polarity(low|high) : high LA Ranging polarity(low|high) : high
| Wait window size (0x0-0x7F) : 0x0 Ranging access window size(0x0-0x7F) : 0xf
| ED inversion(true|false) : false LA Medial Value(enable|disable) : disable
| LA Pin Select(ttl|pecl) : ttl DS FEC mode(enable|disable) : disable
| Delimiter length by bits(8,16,20,24) : 20 Idle Port Id : 0
| Idle Port Status : disable Delimiter ED source : BCDR
| Ranging ED source : BCDR
| BCDR resync pattern in HEX : 0xFFFF000000000000
| LA resync pattern in HEX : 0xFFFFFFFFFFFFFF00000000
| BCDR ranging pattern : 0xFFFF000000000000
| LA ranging pattern in HEX : 0xFFFFFFFFFFFFFF00000000
| Delimiter pattern : 0xB5983
| Link type : LUMINENT A
| Link status : 2 Link mode : 0
| Anti Mac Spoofing : disable
-----+-----+-----+-----+-----+-----+-----+-----+-----+
--- | Details
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
sysname# show remote ont ont-1-101 bwgroup
-----+-----+-----+-----+-----+-----+-----+-----+
AID | ID | Status | | Upstream | Downstream
-----+-----+-----+-----+-----+-----+-----+-----+
ont-1-101 | 1 | IS | Bandwidth profile | 1G | 1G
| | | | SIR | 1024 kbps | 1024 kbps
| | | | AIR | 2048 kbps | 2048 kbps
| | | | AIR | 102400 kbps | 102400 kbps
| | | | AllocId | 256 |
| | | +-----+-----+-----+-----+-----+-----+
| | | GEM port | 260 261 262 263
-----+-----+-----+-----+-----+-----+-----+-----+
--- | Details
+-----+-----+-----+-----+-----+-----+-----+-----+-----+

```

- 4 Configure a VLAN (10 in this example) with the PON port (**PON1** in this example) and uplink port (port 1) as fixed members.

Note: The OLT will always configure the ONT to send out US packets with VLAN tag. The PON port must always be configured as egress tagged.

```

sysname# config
sysname(config)# vlan 10
sysname(config-vlan)# fixed pon-1
sysname(config-vlan)# fixed eth-1
sysname(config-vlan)# exit

```

- 5** Configure VLAN flow settings for the subscriber port on the remote ONT and check the settings.
- The subscriber User Network Interface (UNI) port at **PON1**, ONT 101, card 1, card port 1.
 - QoS queue: configure QoS settings to apply to a specific traffic class.
 - tc: traffic class 0-7 to which to apply this queue, 1 in this example.
 - priority: 0-7 to apply to the traffic class, 1 in this example.
 - weight 0-255 to use for the traffic class, 0 in this example.
 - usbwprofilename: upstream bandwidth profile to use for the traffic class, voice in this example.
 - dsbwprofilename: downstream bandwidth profile to use for the traffic class, voice in this example.
 - dsoption: Set whether to apply the downstream rate limit function to the OLT (olt) or the ONT (ont).
 - bwsharegroupid: bandwidth group ID 1-40 on this ONT to put the QoS queues into. This example uses the 1, the bandwidth group you configured in step 3 on [page 366](#).
 - VLAN settings:
 - VLAN: UNI VLAN of traffic (10 in this example) to which to apply this command's QoS ingress profile and AES encryption settings.
 - Network: the Network Node Interface (NNI) VID, 10 in this example. Use a number different from the UNI VLAN to apply VLAN translation.
 - ingprof: the QoS ingress profile to apply to the VLAN's traffic, voip in this example.
 - AES encryption: enabled or disabled (Disabled in this example).
 - Active: on or off (On in this example).

```

sysname# config
sysname(config)# remote uniport uniport-1-101-1-1
sysname(config-remote-uniport)# queue tc 1 priority 1 weight 0 usbwprofilename voice
dsbwprofilename voice dsoption olt bwsharegroupid 1
sysname(config-remote-uniport)# vlan 10 network 10 ingprof voip aesencrypt disable
active on
sysname(config-remote-uniport)# exit
sysname(config)# exit
sysname# show remote uniport uniport-1-101-1-1 queue
-----+-----+-----+-----+-----+
Uniport   TC Pri Wt UsBwProfileName          DsBwProfileName          DsOpt BwGrpShrId DsGrpShrId
-----+-----+-----+-----+-----+
uniport-1-101-1-1  1  1  0  voice           voice                  olt  1        1
-----+-----+-----+-----+-----+
sysname# show remote uniport uniport-1-101-1-1 vlan 10
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|AID          | UNI-VID Status    NNI-VID     Tag      PBit_Prof DSCP_to_PBIT      Ing_Prof TC  GemP AES_Ept  SP  MN
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
v|uniport-1-101-1-1 |      10     IS       10     tag          inactive      voip 1  260 disable of  1
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+

```

CHAPTER 49

Basic Settings

This chapter introduces the basic setting commands of the OLT.

49.1 System Command

Use this command to configure the OLT's system commands.

Table 167 System Commands

COMMAND	DESCRIPTION	M	P
hostname <name_string>	Sets the system's name for identification purposes. <i>name_string</i> : 1-64 printable characters. Spaces are allowed if you enclose the string in double quotation marks ("").	C	13
show logging	Displays the system's logs.	E	3
clear logging	Clears the system logs.	E	13
show cmd-logging	Displays the logs of commands that were used.	E	3
clear cmd-logging	Clears the logs of commands that were used.	E	3

49.2 Multi-login Command

Use the command to display information for multiple administrator logins on the OLT.

Table 168 Multi-login Command

COMMAND	DESCRIPTION	M	P
show multi-login	Displays multi-login information.	E	3
multi-login	Enables multi-login.	C	14
no multi-login	Disables another administrator from logging into Telnet or SSH.	C	14

49.3 Date and Time Commands

Use these commands to configure the date and time on the OLT.

Table 169 Time and Date Commands

COMMAND	DESCRIPTION	M	P
show time	Displays current system time and date.	E	3
time help	Displays the parameters' format for the following commands: <ul style="list-style-type: none">• time <hour:min:sec>• time date <month/day/year>• time timezone <-1200 ... 1200>	C	13
time <hour:min:sec>	Sets the current time on the OLT. <i>hour</i> : 0-23 <i>min</i> : 0-59 <i>sec</i> : 0-59 Note: If you configure Daylight Saving Time after you configure the time, the OLT will apply Daylight Saving Time.	C	13
time date <month/day/year>	Sets the current date on the OLT. <i>month</i> : 1-12 <i>day</i> : 1-31 <i>year</i> : 1970-2037	C	13
time timezone <-1200 ... 1200>	Selects the time difference between UTC (formerly known as GMT) and your time zone.	C	13
time daylight-saving-time	Enables daylight saving time. The current time is updated if daylight saving time has started.	C	13
time daylight-saving-time start-date <week> <day> <month> <o'clock>	Sets the day and time when Daylight Saving Time starts. <i>week</i> : first, second, third, fourth, last. <i>day</i> : Sunday, Monday, Tuesday, <i>month</i> : January, February, March, <i>o'clock</i> : 0-23 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 <i>o'clock</i> 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 <i>o'clock</i> field depends on your time zone.	C	13

Table 169 Time and Date Commands (continued)

COMMAND	DESCRIPTION	M	P
no time daylight-saving-time	Disables daylight saving on the OLT.	C	13
time daylight-saving-time help	Provides more information about the specified command.	C	13

Table 170 Time Sync Commands

COMMAND	DESCRIPTION	M	P
show timesync	Displays time server information.	E	3
timesync server <ip>	Sets the IP address of your time server. The OLT synchronizes with the time server in the following situations: <ul style="list-style-type: none"> When the OLT starts up. Every 24 hours after the OLT starts up. When the time server IP address or protocol is updated. 	C	13
timesync <daytime time ntp>	Sets the time server protocol. You have to configure a time server before you can specify the protocol.	C	13

This example sets the current date, current time, time zone, and daylight savings time.

```
sysname# configure
sysname(config)# time date 06/04/2007
sysname(config)# time timezone -600
sysname(config)# time daylight-saving-time
sysname(config)# time daylight-saving-time start-date second Sunday
--> March 2
sysname(config)# time daylight-saving-time end-date first Sunday
--> November 2
sysname(config)# time 13:24:00
sysname(config)# exit
sysname# show time
Current Time 13:24:03 (UTC-05:00 DST)
Current Date 2007-06-04
```

This example looks at the current time server settings.

```
sysname# show timesync

Time Configuration
-----
Time Zone :UTC -600
Time Sync Mode :USE_DAYTIME
Time Server IP Address :172.16.37.10

Time Server Sync Status:CONNECTING
```

The following table describes the labels in this display.

Table 171 show timesync

LABEL	DESCRIPTION
Time Zone	Displays the time zone.
Time Sync Mode	Displays the time server protocol the OLT uses. It displays NO_TIMESERVICE if the time server is disabled.
Time Server IP Address	Displays the IP address of the time server.
Time Server Sync Status	<p>Displays the status of the connection with the time server.</p> <p>NONE: The time server is disabled.</p> <p>CONNECTING: The OLT is trying to connect with the specified time server.</p> <p>OK: Synchronize with time server done.</p> <p>FAIL: Synchronize with time server fail.</p>

49.4 Hardware Monitor Commands

Use these commands to set the speeds for individual fans, and thresholds on the power modules.

Table 172 Hardware Monitor Commands

COMMAND	DESCRIPTION	M	P
fan <0-100>	<p>Specifies the fan module on which you want to configure the fan speed.</p> <p>Sets the fan's duty cycle percentage from 0~100%.</p>	E	
fan auto	Sets the fan speed to automatic. The fan speed is adjusted automatically according to temperatures sensed by the hardware monitor IC.	E	
hw-monitor fan-speed-threshold <index> <threshold>	<p>Sets the fans speed of a fan in the fan module.</p> <p>index: 1 ~ 4</p> <p>threshold: 0 ~ 15000 in RPM</p>	C	13
no hw-monitor fan-speed-threshold <index>	Sets the fans speed of a fan in the fan module to the default value.	C	13
no hw-monitor fan-speed-threshold all	Sets the fans speed of the fans in the fan module to the default value.	C	13
hw-monitor temperature-threshold <index> <high> <low>	<p>Sets the high and low temperature limits for raising an alarm on the specified module.</p> <p>index: 1-3 (1 is for CPU, 2 is for PON_MAC, and 3 is for SWITCH.)</p> <p>high: -50-106 in degree Celsius</p> <p>low: -50-106 in degree Celsius</p>	C	13

Table 172 Hardware Monitor Commands (continued)

COMMAND	DESCRIPTION	M	P
no hw-monitor temperature-threshold <index>	Clears the temperature limits for raising an alarm to the default value on the specified module. index: 1-3 (1 is for CPU , 2 is for PON_MAC , and 3 is for SWITCH .)	C	13
no hw-monitor temperature-threshold all	Clears the temperature limits for raising an alarm to the default values on all modules.	C	13
hw-monitor voltage-threshold <index> <high> <low>	Sets the high and low voltage limits for raising an alarm on the specified module. index: 1-5 (1 is for +1V , 2 is for +1V_PON , 3 is for +1.8V , 4 is for +3.3V , and 5 is for +15V .) high: 0-25000 in mV low: 0-25000 in mV	C	13
no hw-monitor voltage-threshold <index>	Sets the high and low voltage limits for raising an alarm to the default values on the specified module. index: 1-5 (1 is for +1V , 2 is for +1V_PON , 3 is for +1.8V , 4 is for +3.3V , and 5 is for +15V .)	C	13
no hw-monitor voltage-threshold all	Sets the high and low voltage limits for raising an alarm to the default values on all modules .	C	13

49.5 External Alarm Commands

Use these commands to configure the external alarm features on the OLT.

Table 173 External Alarm Commands

COMMAND	DESCRIPTION	M	P
external-alarm <index> name <name_string>	Sets the name of the specified external alarm. <i>index</i> : 1 ~ 4 <i>name_string</i> : Enters a name of up to 32 ASCII characters.	C	13
no external-alarm <index>	Removes the name of the specified external alarm input.	C	13
no external-alarm all	Removes the name of all external alarms.	C	13
show external-alarm	Displays external alarm settings and status.	E	3

49.6 Switch Setup

Use these commands to configure OLT switch setup.

Table 174 Switch Setup Commands

COMMAND	DESCRIPTION	M	P
<code>bcp-transparency</code>	Enables Bridge Control Protocol (BCP) transparency on the OLT. This allows the OLT to handle bridging control protocols (STP, for example).	C	13
<code>no bcp-transparency</code>	Disables BCP transparency on the OLT.	C	13
<code>mac-aging-time <30-86400></code>	Sets learned MAC aging time in seconds. MAC address learning reduces outgoing traffic broadcasts. For MAC address learning to occur on a port, the port must be active.	C	13
<code>queue priority <0-7> level <0-7></code>	<p>Sets the IEEE 802.1p priority level-to-physical queue mapping.</p> <p>Priority <0-7>: IEEE 802.1p defines up to eight 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.</p> <p>Level <0-7>: The OLT has eight physical queues that you can map to the 8 priority levels. On the OLT, traffic assigned to higher index queues gets through faster while traffic in lower index queues is dropped if the network is congested.</p>	C	13

49.7 IP Setup

This section covers how to configure the default gateway device, the default domain name server and add IP domains.

The OLT needs an IP address for it to be managed over the network. The factory default IP address is 192.168.1.1. The subnet mask specifies the network number portion of an IP address. The factory default subnet mask is 255.255.255.0.

On the OLT, as a layer-3 device, an IP address is not bound to any physical ports. Since each IP address on the OLT must be in a separate subnet, the configured IP address is also known as IP interface (or routing domain). In addition, this allows routing between subnets based on the IP address without additional routers.

You can configure multiple routing domains on the same VLAN as long as the IP address ranges for the domains do not overlap. To change the IP address of the OLT in a routing domain, simply add a new routing domain entry with a different IP address in the same subnet.

The following table describes the related commands.

Table 175 IP Commands

COMMAND	DESCRIPTION	M	P
show ip	Displays current IP interfaces.	E	0
show ip iptable all	Displays the IP address table.	E	3
show ip iptable all <sort>	Displays the IP address table according to the IP address, VLAN ID or the port number.	E	3
show ip iptable count	Displays the number of IP interfaces configured on the OLT.	E	3
show ip iptable static	Displays the static IP address table.	E	3
ip address <ip> <mask>	Sets the IP address of the MGMT port (for out-of-band management) on the OLT.	C	13
ip inband address <ip> <mask> <gateway> <vlan>	Sets the inband management (MGMT port) interface's IP address, subnet mask bit, gateway IP address, and VLAN group . Disables the DHCP client function if it is enabled.	C	13
ip address default-gateway <ip>	Sets the default gateway for the out-of-band management interface on the OLT.	C	13
ip name-server <ip>	Sets the IPv4 address(es) of the domain name server(s).	C	13
ip route <ip> <mask> <next-hop-ip>	Configures a static route. ip: 0.0.0 ~ 223.255.255.255 mask: 0 ~ 32 next-hop-ip: 0.0.0 ~ 223.255.255.255	C	13
no ip	Sets the management IP address, subnet mask bit, and gateway IP address for the out-of-band management port to the default values. The default value is 192.168.0.1.	C	13
no ip inband address <ip> <mask> <gateway> <vlan>	Removes the inabnd management IP address, subnet mask bit, gateway IP address , and VLAN group.	C	13

49.7.1 Configure the Out-of-band Management IP Address Settings

This example changes the out-of-band management IP address to 192.168.0.2 with subnet mask 255.255.255.0.

```
sysname# configure
sysname(config)# ip address 192.168.0.2 255.255.255.0
```

49.7.2 Set the Out-of-band Management Default Gateway IP Address

This example sets the out-of-band management default gateway from 0.0.0.0 to 192.168.0.254.

```
sysname# configure
sysname(config)# ip address default-gateway 192.168.0.254
```

49.7.3 Display IP Settings

This example displays the in-band and out-of-band IP address, subnet mask, and VID.

```
sysname# show ip
Management IP Address
    IP[192.168.0.2], Netmask[255.255.255.0], VID[0]
IP Interface
    IP[192.168.1.1], Netmask[255.255.255.0], VID[1]
```

49.8 Port Setup

The following table describes the commands for configuring the OLT **PON** ports.

Table 176 Port Setup Commands

COMMAND	DESCRIPTION	M	P
interface port-channel <aid>	Selects a port to configure. aid: <pon eth>-<port>	C	13
name <port-name-string>	Sets the interface name.	C	13
speed-duplex <auto 100-half 100-full 1000-full 2500-full 10000-full ...>	Sets the interface speed (in Mbps) and duplex mode. auto: (auto-negotiation) allows one port to negotiate with a peer port automatically to obtain the connection speed and duplex mode that both ends support. When auto-negotiation is turned on, a port on the OLT negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer port does not support auto-negotiation or turns off this feature, the OLT determines the connection speed by detecting the signal on the cable and using half duplex mode. When the OLT's auto-negotiation is turned off, a port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer port are the same in order to connect. 100-full is supported for a 1000Base-T connection. 1000-full is supported by both 1000Base-T and 1000Base-X connections. 2500-full is supported by the SC optical transceiver connections. 10000-full is supported by the 10 Gigabit Ethernet uplink connections.	C	13

Table 176 Port Setup Commands (continued)

COMMAND	DESCRIPTION	M	P
bpd़u-control <peer tunnel discard network>	Sets how Bridge Protocol Data Units (BPDUs) are used in STP port states. Configure the way to treat BPDUs received on this port. You must activate bridging control protocol transparency first. peer: process any BPDU (Bridge Protocol Data Units) received on this port. tunnel: forward BPDUs received on this port. discard: drop any BPDU received on this port. network: process a BPDU with no VLAN tag and forward a tagged BPDU.	C	13
no inactive	Enables the port.	C	13
inactive	Disables the port.	C	13
exit	Leaves the slot configuration sub-commands.	C	13
no interface olt <aid>	Removes the configuration of the specified port. aid: pon-<port>	C	13
no interface olt all	Removes all port configuration.	C	13
show interfaces <aid>	Displays the status of the specified interface. aid: <pon eth>-<port>	E	3
show interfaces config <aid>	Displays port settings. aid: <pon eth>-<port>	E	3

49.8.1 Port Setup Commands Examples

The following commands set up configurations **PON1**.

```
sysname# config
sysname(config)# interface port-channel pon-1
```

Enable the port.

```
sysname(config-interface)# no inactive
```

Exit from the slot configuration .

```
sysname(config-interface)# exit
```

After the **PON** port is installed and activated, use the following commands to display the status of the specified interface.

The following command displays the interface status of **PON1** of the OLT.

```
sysname# show interface pon-1
AID | Link Status LACP TxPkts RxPkts Errors Tx_KBs/s Rx_KBs/s Up_Time
-----
pon-1| 2500M/F FORWARDING None 0 0 0.0 0.0 3:35:28
-----
| Details
-----
| TX Packet   Unicast : 0          RX Packet   Unicast : 0
|             Multicast : 0        Multicast : 0
|             Broadcast : 0       Broadcast : 0
|             Pause    : 0          Pause    : 0
|             Tagged   : 0          Control   : 0
|             Octets   : 0          Octets   : 0
| TX Collision Single  : 0          Distribution 64 : 0
|                  Multiple : 0      65-127    : 0
|                  Excessive : 0     128-255   : 0
|                  Late     : 0      256-511   : 0
| Error Packet  RX CRC  : 0          512-1023  : 0
|                  Length   : 0      1024-1518 : 0
|                  Runt    : 0          Giant    : 0
-----
```

The following commands configure **PON1**.

Select **PON1** and name the port 2406.

```
sysname# configure
sysname(config)# interface port-channel pon-1
sysname(config-interface)# name 2406
```

Set the port to 1 Gb and full duplex.

```
sysname(config-interface)# speed-duplex 1000-full
```

Set the port to forward BPDUs it receives.

```
sysname(config-interface)# bpdu-control tunnel
```

Display the port's settings.

```
sysname(config-interface)# exit
sysname(config)# exit
sysname# show interfaces config pon-1
Port Configurations:

  Port No      :gpon-1
  Active       :Yes
  Name         :2406
  PVID         :1           Flow Control   :Yes
  Type         :1000M        Speed/Duplex  :1000-full
  BPDU         :tunnel      802.1p Priority :0
  max-frame-size :2590
```

CHAPTER 50

IPv6

This chapter introduces the IPv6 commands of the OLT.

50.1 IPv6 Overview

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. At the time of writing, the OLT supports the following features.

- Static address assignment (see [Section 50.1.1 on page 381](#)) and stateless autoconfiguration (see [Stateless Autoconfiguration on page 384](#))
- Neighbor Discovery Protocol (see [Neighbor Discovery Protocol \(NDP\) on page 385](#))
- Remote Management using SNMP, Telnet, and FTP services (see [Chapter 78 on page 546](#))
- ICMPv6 (see [ICMPv6 on page 385](#))
- IPv4/IPv6 dual stack; the OLT can run IPv4 and IPv6 at the same time.
- DHCPv6 client and relay (see [DHCPv6 on page 384](#))
- Multicast Listener Discovery (MLD) snooping and proxy (see [Multicast Listener Discovery on page 386](#))

For more information on IPv6 addresses, refer to RFC 2460 and RFC 4291.

50.1.1 IPv6 Addressing

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 or 2001:0db8:0000:0000:1a2f::0015.

50.1.2 IPv6 Terms

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.

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 fe80::/10. The link-local unicast address format is as follows.

Table 177 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. The global address format as follows.

Table 178 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 ff00::/8. The following table describes some of the predefined multicast addresses.

Table 179 Predefined Multicast Address

MULTICAST ADDRESS	DESCRIPTION
FF01:0:0:0:0:0:0:1	All hosts on a local node.
FF01:0:0:0:0:0:0:2	All routers on a local node.
FF02:0:0:0:0:0:0:1	All hosts on a local connected link.
FF02:0:0:0:0:0:0:2	All routers on a local connected link.
FF05:0:0:0:0:0:0:2	All routers on a local site.
FF05:0:0:0:0:0:1:3	All DHCP servers on a local site.

The following table describes the multicast addresses which are reserved and can not be assigned to a multicast group.

Table 180 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 181

MAC	00	:	13	:	49	:	12	:	34	:	56
-----	----	---	----	---	----	---	----	---	----	---	----

Table 182

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 OLT, 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.

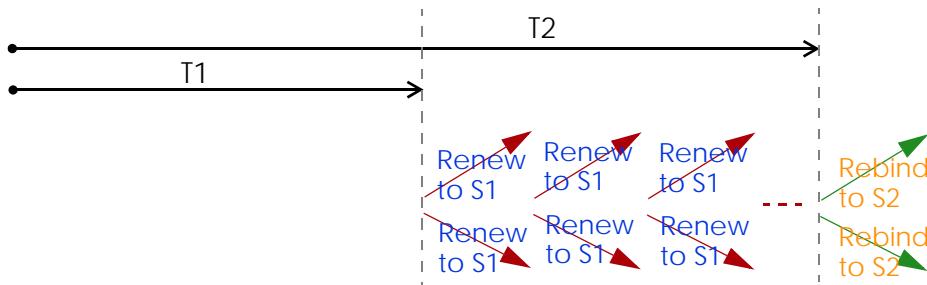
Each DHCP client and server has a unique DHCP Unique IDentifier (DUID), which is used for identification when they are exchanging DHCPv6 messages. The DUID is generated from the MAC address, time, vendor assigned ID and/or the vendor's private enterprise number registered with the IANA. It should not 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

2. In IPv6, all network interfaces can be associated with several addresses.

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.



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.

An IPv6 device uses the following ICMPv6 messages types:

- Neighbor solicitation: A request from a host to determine a neighbor's link-layer address (MAC address) and detect if the neighbor is still reachable. A neighbor being "reachable" means it responds to a neighbor solicitation message (from the host) with a neighbor advertisement message.
- Neighbor advertisement: A response from a node to announce its link-layer address.
- Router solicitation: A request from a host to locate a router that can act as the default router and forward packets.
- Router advertisement: A response to a router solicitation or a periodical multicast advertisement from a router to advertise its presence and other parameters.

IPv6 Cache

An IPv6 host is required to have a neighbor cache, destination cache, prefix list and default router list. The OLT maintains and updates its IPv6 caches constantly using the information from response messages. In IPv6, the OLT configures a link-local address automatically, and then sends a neighbor solicitation message to check if the address is unique. If there is an address to be resolved or verified, the OLT also sends out a neighbor solicitation message. When the OLT receives a neighbor advertisement in response, it stores the neighbor's link-layer address in the neighbor cache. When the OLT uses a router solicitation message to query for a router and receives a router advertisement message, it adds the router's information to the neighbor cache, prefix list and destination cache. The OLT creates an entry in the default router list cache if the router can be used as a default router.

When the OLT needs to send a packet, it first consults the destination cache to determine the next hop. If there is no matching entry in the destination cache, the OLT uses the prefix list to determine whether the destination address is on-link and can be reached directly without passing through a router. If the address is onlink, the address is considered as the next hop. Otherwise, the OLT determines the next-hop from the default router list or routing table. Once the next hop IP address is known, the OLT looks into the neighbor cache to get the link-layer address and sends the packet when the neighbor is reachable. If the OLT cannot find an entry in the neighbor cache or the state for the neighbor is not reachable, it starts the address resolution process. This helps reduce the number of IPv6 solicitation and advertisement messages.

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 listeners 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.

MLD Messages

A multicast router or switch periodically sends general queries to MLD hosts to update the multicast forwarding table. When an MLD host wants to join a multicast group, it sends an MLD Report message for that address.

50.2 IPv6 Commands

The following section lists the commands for this feature.

Table 183 ipv6 address Commands

COMMAND	DESCRIPTION	M	P
<code>ipv6</code>	Creates an IPv6 out-of-band management interface and enables it. The OLT then creates a link-local address automatically. Use "show ipv6" to see the generated address.	C	13
<code>no ipv6</code>	Removes the IPv6 out-of-band management interface.	C	13
<code>ipv6 disable</code>	Disables the IPv6 out-of-band management interface.	C	13
<code>no ipv6 disable</code>	Enables the IPv6 out-of-band management interface.	C	13
<code>ipv6 address <ipv6-address>/<prefix-length></code>	Manually configures a static IPv6 global address on the IPv6 out-of-band management interface.	C	13
<code>ipv6 address <ipv6-address>/<prefix-length> eui-64</code>	Manually configures a static IPv6 global address on the IPv6 out-of-band management interface and has the interface ID be generated automatically using the EUI-64 format.	C	13
<code>ipv6 address <ipv6-address>/<prefix-length> link-local</code>	Manually configures a static IPv6 link-local address on the IPv6 out-of-band management interface.	C	13
<code>ipv6 address autoconfig</code>	Sets the OLT to generate an IPv6 global address automatically on the IPv6 out-of-band management interface after the OLT obtains the VLAN network information from a router. Note: Make sure an IPv6 router is available in the network to which the out-of-band management interface is connected before using this command on the OLT.	C	13
<code>ipv6 address default-gateway <ipv6-address></code>	Sets the default gateway for the IPv6 out-of-band management interface. When the interface cannot find a routing information for a frame's destination, it forwards the packet to the default gateway.	C	13
<code>ipv6 global default-management <ipv6-interface-name></code>	Sets through which IPv6 interface (the IPv6 out-of-band management or a VLAN interface on which IPv6 is enabled) the OLT sends IPv6 packets originating from itself (such as SNMP traps) or IPv6 packets with unknown source.	C	13
<code>no ipv6 global default-mgmt</code>	Resets the global IPv6 management interface to the default settings.	C	13
<code>no ipv6 address <ipv6-address>/<prefix-length></code>	Removes a specified static global address for the IPv6 out-of-band management interface.	C	13
<code>no ipv6 address <ipv6-address>/<prefix-length> eui-64</code>	Removes a specified static global address whose interface ID was generated using the EUI-64 format for the IPv6 out-of-band management interface.	C	13

Table 183 ipv6 address Commands (continued)

COMMAND	DESCRIPTION	M	P
no ipv6 address <ipv6-address>/<prefix-length> link-local	Removes a static IPv6 link-local address for the IPv6 out-of-band management interface.	C	13
no ipv6 address autoconfig	Disables IPv6 address auto configuration on the IPv6 out-of-band management interface.	C	13
no ipv6 address default-gateway	Removes the default gateway address for the IPv6 out-of-band management interface.	C	13
no ipv6 global hop-limit	Resets the maximum number of hops in router advertisements to the default setting.	C	13
vlan <1-4094>	Enters config-vlan mode for the specified VLAN. Creates the VLAN, if necessary.	C	13
ipv6	Globally enables IPv6 in this VLAN. The OLT then creates a link-local address automatically. Use "show ipv6" to see the generated address.	C	13
ipv6 address <ipv6-address>/<prefix-length>	Manually configures a static IPv6 global address for the VLAN.	C	13
ipv6 address <ipv6-address>/<prefix-length> eui-64	Manually configures a static IPv6 global address for the VLAN and has the interface ID be generated automatically using the EUI-64 format.	C	13
ipv6 address <ipv6-address>/<prefix-length> link-local	Manually configures a static IPv6 link-local address for the VLAN.	C	13
ipv6 address autoconfig	Use the command to have the OLT generate an IPv6 global address automatically in this VLAN after the OLT obtains the VLAN network information from a router. Note: Make sure an IPv6 router is available in the VLAN network before using this command on the OLT.	C	13
ipv6 address default-gateway <ipv6-gateway-address>	Sets the default gateway for the VLAN. When an interface cannot find a routing information for a frame's destination, it forwards the packet to the default gateway.	C	13
ipv6 disable	Disables IPv6 in this VLAN.	C	13
no ipv6	Removes this IPv6 VLAN interface.	C	13
no ipv6 address <ipv6-address>/<prefix-length>	Removes a specified static IPv6 global address for this VLAN.	C	13
no ipv6 address <ipv6-address>/<prefix-length> eui-64	Removes a specified static IPv6 global address whose interface ID was generated using the EUI-64 format.	C	13
no ipv6 address <ipv6-address>/<prefix-length> link-local	Removes a static IPv6 link-local address for the VLAN.	C	13
no ipv6 address autoconfig	Disables IPv6 address autoconfiguration in this VLAN.	C	13
no ipv6 address default-gateway	Removes the default gateway address for this VLAN.	C	13
no ipv6 address dhcp client	Disables the DHCP client feature in this VLAN.	C	13

Table 183 ipv6 address Commands (continued)

COMMAND	DESCRIPTION	M	P
no ipv6 address dhcp client [rapid-commit]	sets the OLT to not include a Rapid Commit option in its DHCPv6 Solicit message for this VLAN.	C	13
no ipv6 address dhcp client option	Sets the OLT to not obtain the DNS server information from the DHCP server.	C	13
no ipv6 address dhcp client option <[dns][domain-list]>	Sets the OLT to not obtain DNS server IPv6 addresses or a list of domain names from the DHCP server.	C	13
exit	Leaves the VLAN configuration sub-commands.	C	13
help	Provides more information about the specified command.	C	13
show ipv6	Displays IPv6 settings in all VLANs on the OLT.	E	0
show ipv6 <vlan mgmt> <1-4094 0>	Displays whether IPv6 is enabled in the specified in-band VLAN interface or the IPv6 settings for the out-of-band management interface.	E	3
show ipv6 router	Displays all IPv6 router advertisement information on the OLT.	E	3
show ipv6 router <vlan mgmt> <vlan-id mgmt-id>	Displays IPv6 router advertisement information for the specified inband VLAN or the MGMT (out-of-band) interface.	E	3
default-management <in-band out-of-band>	Sets through which traffic flow (in-band or out-of-band) the OLT sends packets originating from itself (such as SNMP traps) or packets with unknown source. in-band: IP interfaces that can be accessed through GE-1 ~ GE-6 uplink port or OLT PON, GE ports in GE line card. These are the ports for regular customer services. out-of-band: IP interfaces that can be accessed through the management port. The port is not used for regular customer service.	C	13
restart ipv6 dhcp client vlan <1-4094>	Sets the OLT to send a release message for the assigned IPv6 address to the DHCP server and start the DHCP message exchange again.	E	13

Table 184 IPv6 dhcp relay command summary

COMMAND	DESCRIPTION	M	P
ipv6 dhcp relay vlan <1-4094> helper-address <remote-dhcp-server>	Enables DHCPv6 relay agent and configures the remote DHCP server address for the specified VLAN.	C	13
ipv6 dhcp relay vlan <1-4094> option interface-id	Sets the OLT to add the interface-ID option in the DHCPv6 requests from the clients in the specified VLAN before the OLT forwards them to a DHCP server.	C	13
ipv6 dhcp relay vlan <1-4094> option remote-id <remote-id>	Sets the OLT to add the remote-ID option in the DHCPv6 requests from the clients in the specified VLAN before the OLT forwards them to a DHCP server. This also specifies a string (up to 64 printable ASCII characters) to be carried in the remote-ID option.	C	13

Table 184 IPv6 dhcp relay command summary (continued)

COMMAND	DESCRIPTION	M	P
no ipv6 dhcp relay vlan <1-4094> <cr>	Disables DHCPv6 relay agent in the specified VLAN.	C	13
no ipv6 dhcp relay vlan <1-4094> option interface-id	Sets the OLT to not add the interface-ID option in the DHCPv6 requests from the clients in the specified VLAN before the OLT forwards them to a DHCP server.	C	13
no ipv6 dhcp relay vlan <1-4094> option remote-id	Sets the OLT to not add the remote-ID option in the DHCPv6 requests from the clients in the specified VLAN before the OLT forwards them to a DHCP server.	C	13

Table 185 ipv6 icmp and ping6 Commands

COMMAND	DESCRIPTION	M	P
ipv6 global icmp error-interval <0-2147483647> [bucket-size <1-200>]	<p>Sets the average transmission rate of ICMPv6 error messages the OLT generates, such as Destination Unreachable message, Packet Too Big message, Time Exceeded message and Parameter Problem message.</p> <p>error-interval: specifies a time period (in milliseconds) during which packets of up to the bucket size (10 by default) can be transmitted. 0 means no limit.</p> <p>Note: The OLT applies the time interval in increments of 10. For example, if you set a time interval from 1280 to 1289 milliseconds, the OLT uses the time interval of 1280 milliseconds.</p> <p>bucket-size: Defines the maximum number of packets which are allowed to transmit in a given time interval. If the bucket is full, subsequent error messages are suppressed.</p>	C	13

Table 185 ipv6 icmp and ping6 Commands (continued)

COMMAND	DESCRIPTION	M	P
<code>ping6 <ipv6-address> <[-i <interface-type> <interface-number>] [-t] [-l <1-1452>] [-n <1-65535>] [-s <ipv6-address>]</code>	<p>Sends IPv6 ping packets to the specified Ethernet device.</p> <p><i>interface-type</i>: the OLT supports only the VLAN interface type at the time of writing.</p> <p><i>interface-number</i>: The VLAN ID to which the Ethernet device belongs.</p> <p><i>-l <1-1452></i>: Specifies the size of the ping packet.</p> <p><i>-t</i>: Sends ping packets to the Ethernet device indefinitely. Press [CTRL]+C to terminate the Ping process.</p> <p><i>-n <1-65535></i>: Specifies how many times the OLT sends the ping packets.</p> <p><i>-s <ipv6-address></i>: Specifies the source IPv6 address of the ping packets.</p>	E	0
<code>show ipv6 mtu</code>	<p>Displays IPv6 path MTU information on the OLT.</p> <p>The OLT uses Path MTU Discovery to discover Path MTU (PMTU), that is, the minimum link MTU of all the links in a path to the destination. If the OLT receives an ICMPv6 Packet Too Big error message after sending a packet, it adjusts the next packet size according to the suggested MTU in the error message.</p>	E	3

Table 186 ipv6 nd Commands

COMMAND	DESCRIPTION	M	P
<code>ipv6 nd dad-attempts <0-600></code>	Sets the number of consecutive neighbor solicitations the OLT sends for the IPv6 out-of-band management interface.	C	13
<code>ipv6 nd ns-interval <1000-3600000></code>	Specifies the time interval (in milliseconds) at which neighbor solicitations are re-sent for the IPv6 out-of-band management interface.	C	13
<code>ipv6 nd reachable-time <1000-2147483647></code>	Specifies how long (in milliseconds) a neighbor is considered reachable for the IPv6 out-of-band management interface.	C	13
<code>no ipv6 nd dad-attempts</code>	Resets the number of the DAD attempts for the IPv6 out-of-band management interface to the default settings (3).	C	13
<code>no ipv6 nd managed-config-flag</code>	Configures the OLT to set the "managed address configuration" flag (the M flag) to 0 in IPv6 router advertisements for the IPv6 out-of-band management interface, which means hosts do not use DHCPv6 to obtain IPv6 stateful addresses.	C	13
<code>no ipv6 nd ns-interval</code>	Resets the time interval between retransmissions of neighbor solicitations for the IPv6 out-of-band management interface to the default setting (3000 milliseconds).	C	13

Table 186 ipv6 nd Commands (continued)

COMMAND	DESCRIPTION	M	P
no ipv6 nd other-config-flag	Configures the OLT to set the “Other stateful configuration” flag (the O flag) to 0 in IPv6 router advertisements for the IPv6 out-of-band management interface, which means hosts do not use DHCPv6 to obtain additional configuration settings, such as DNS information.	C	13
no ipv6 nd prefix <ipv6-prefix>/<prefix-length>	Sets the OLT to not include the specified IPv6 prefix and prefix length in router advertisements for the IPv6 out-of-band management interface.	C	13
no ipv6 nd ra interval	Resets the minimum and maximum time intervals between retransmissions of router advertisements for the IPv6 out-of-band management interface to the default settings.	C	13
no ipv6 nd ra lifetime	Resets the lifetime of a router in router advertisements for the IPv6 out-of-band management interface to the default setting (9000 seconds).	C	13
no ipv6 nd ra suppress	Enables the sending of router advertisements and responses to router solicitations on the IPv6 out-of-band management interface.	C	13
no ipv6 nd reachable-time	Resets the reachable time of a neighbor on the IPv6 out-of-band management interface to the default setting (60000 milliseconds).	C	13
vlan <1-4094>	Enters config-route-domain mode for the specified VLAN. Creates the VLAN, if necessary.	C	13
ipv6 nd dad-attempts <0-600>	Sets the number of consecutive neighbor solicitations the OLT sends for this VLAN. The OLT uses Duplicate Address Detection (DAD) with neighbor solicitation and advertisement messages to check whether an IPv6 address is already in use before assigning it to an interface, such as the link-local address it creates through stateless address autoconfiguration for this VLAN. To turn off the DAD for this VLAN, set the number of DAD attempts to 0.	C	13
ipv6 nd managed-config-flag	Configures the OLT to set the “managed address configuration” flag (the M flag) to 1 in IPv6 router advertisements, which means hosts use DHCPv6 to obtain IPv6 stateful addresses.	C	13
ipv6 nd ns-interval <1000-3600000>	Specifies the time interval (in milliseconds) at which neighbor solicitations are re-sent for this VLAN.	C	13
ipv6 nd other-config-flag	Configures the OLT to set the “Other stateful configuration” flag (the O flag) to 1 in IPv6 router advertisements, which means hosts use DHCPv6 to obtain additional configuration settings, such as DNS information.	C	13

Table 186 ipv6 nd Commands (continued)

COMMAND	DESCRIPTION	M	P
<code>ipv6 nd prefix <ipv6-prefix>/<prefix-length> [valid-lifetime <0-4294967295>] [preferred-lifetime <0-4294967295>] [no-autoconfig] [no-onlink] [no-advertise]</code>	<p>Sets the OLT to include the specified IPv6 prefix, prefix length and optional parameters in router advertisements for this VLAN.</p> <p>valid-lifetime: sets how long in seconds the prefix is valid for on-link determination.</p> <p>preferred-lifetime: sets how long (in seconds) that addresses generated from the prefix via stateless address autoconfiguration remain preferred.</p> <p>no-autoconfig: indicates the hosts can not use this prefix for stateless address autoconfiguration.</p> <p>no-onlink: indicates this prefix can not be used for on-link determination.</p> <p>no-advertise: sets the OLT to not include the specified IPv6 prefix, prefix length and optional parameters in router advertisements for this VLAN.</p>	C	13
<code>ipv6 nd prefix <ipv6-prefix>/<prefix-length></code>	Sets the OLT to include the specified IPv6 prefix and prefix length in router advertisements for this VLAN.	C	13
<code>ipv6 nd ra interval minimum <3-1350> maximum <4-1800></code>	Specifies the minimum and maximum time intervals at which the OLT sends router advertisements for this VLAN.	C	13
<code>ipv6 nd ra lifetime <0-9000></code>	Sets how long (in seconds) the router in router advertisements can be used as a default router for this VLAN.	C	13
<code>ipv6 nd ra suppress</code>	Sets the OLT to not send router advertisements and responses to router solicitations for this VLAN.	C	13
<code>ipv6 nd reachable-time <1000-2147483647></code>	Specifies how long (in milliseconds) a neighbor is considered reachable for this VLAN.	C	13
<code>no ipv6 nd dad-attempts</code>	Resets the number of the DAD attempts to the default settings (3).	C	13
<code>no ipv6 nd managed-config-flag</code>	Configures the OLT to set the "managed address configuration" flag (the M flag) to 0 in IPv6 router advertisements, which means hosts do not use DHCPv6 to obtain IPv6 stateful addresses.	C	13
<code>no ipv6 nd ns-interval</code>	Resets the time interval between retransmissions of neighbor solicitations to the default setting (3000 milliseconds).	C	13
<code>no ipv6 nd other-config-flag</code>	Configures the OLT to set the "Other stateful configuration" flag (the O flag) to 0 in IPv6 router advertisements, which means hosts do not use DHCPv6 to obtain additional configuration settings, such as DNS information.	C	13
<code>no ipv6 nd prefix <ipv6-prefix>/<prefix-length></code>	Sets the OLT to not include the specified IPv6 prefix and prefix length in router advertisements for this VLAN.	C	13

Table 186 ipv6 nd Commands (continued)

COMMAND	DESCRIPTION	M	P
no ipv6 nd ra interval	Resets the minimum and maximum time intervals between retransmissions of router advertisements for this VLAN to the default settings.	C	13
no ipv6 nd ra lifetime	Resets the lifetime of a router in router advertisements to the default setting (9000 seconds).	C	13
no ipv6 nd ra suppress	Enables the sending of router advertisements and responses to router solicitations on this interface.	C	13
no ipv6 nd reachable-time	Resets the reachable time of a neighbor to the default setting (60000 milliseconds).	C	13
show ipv6 prefix	Displays all IPv6 prefix information on the OLT.	E	3
show ipv6 prefix <interface-type> <interface-number>	Displays IPv6 prefix information for the specified interface (VLAN).	E	3

Table 187 ipv6 neighbor Commands

COMMAND	DESCRIPTION	M	P
clear ipv6 neighbor	Removes all IPv6 neighbor information on the OLT.	E	13
clear ipv6 neighbor <interface-type> <interface-number>	Removes IPv6 neighbor information for a specified interface on the OLT.	E	13
ipv6 neighbor <interface-type> <interface-number> <ipv6-address> <mac-address>	Creates a static IPv6 neighbor entry in the IPv6 cache.	C	13
no ipv6 neighbor <interface-type> <interface-number> <ipv6-address>	Removes a static IPv6 neighbor entry from the IPv6 cache.	C	13
show ipv6 neighbor	Displays IPv6 neighbor devices for all interfaces on the OLT.	E	3
show ipv6 neighbor <interface-type> <interface-number>	Displays IPv6 neighbor devices for a specified interface on the OLT.	E	3

50.3 IPv6 Command Examples

This example shows how to enable IPv6 in VLAN 1 and display the link-local address the OLT automatically generated and other IPv6 information for the VLAN.

```
sysname# config
sysname(config)# vlan 1
sysname(config-vlan)# ipv6
sysname(config-vlan)# exit
sysname(config)# exit
sysname# show ipv6 vlan 1
VLAN : 1 (VLAN1)
    IPv6 is enabled.
    MTU is 1500 bytes.
    ICMP error messages limited to 10 every 100 milliseconds.
    Stateless Address Autoconfiguration is disabled.
    Link-Local address is fe80::219:cbff:fe6f:9159 [preferred]
    Global unicast address(es):
        Joined group address(es):
            ff02::2
            ff01::1
            ff02::1
            ff02::1:ff6f:9159
        ND DAD is enabled, number of DAD attempts: 1
        ND NS-interval is 1000 milliseconds
        ND reachable time is 30000 milliseconds
        ND router advertised managed config flag is disable
        ND router advertised other config flag is disable
        ND router advertisements are sent every 200 to 600 seconds
        ND router advertisements lifetime 1800 seconds
```

This example shows how to manually configure two IPv6 addresses (one uses the EUI-64 format, one doesn't) in VLAN 1, and then display the result. Before using `ipv6 address` commands, you have to enable IPv6 in the VLAN and this has the OLT generate a link-local address for the interface.

There are three addresses created in total for VLAN 1. The address "2001:db8:c18:1:219:cbff:fe00:1/64" is created with the interface ID "219:cbff:fe00:1" generated using the EUI-64 format. The address "2001:db8:c18:1::12b/64" is created exactly the same as what you entered in the command.

```

sysname# config
sysname(config)# vlan 1
sysname(config-vlan)# ipv6
sysname(config-vlan)# ipv6 address 2001:db8:c18:1::127/64 eui-64
sysname(config-vlan)# ipv6 address 2001:db8:c18:1::12b/64
sysname(config-vlan)# exit
sysname(config)# exit
sysname# show ipv6
VLAN : 1 (VLAN1)
    IPv6 is enabled.
    MTU is 1500 bytes.
    ICMP error messages limited to 10 every 100 milliseconds.
    Stateless Address Autoconfiguration is disabled.
    Link-Local address is fe80::219:cbff:fe00:1 [preferred]
    Global unicast address(es):
        2001:db8:c18:1::12b/64 [preferred]
        2001:db8:c18:1:219:cbff:fe00:1/64 [preferred]
    Joined group address(es):
        ff02::1:ff00:12b
        ff02::2
        ff01::1
        ff02::1
        ff02::1:ff6f:9159
    ND DAD is enabled, number of DAD attempts: 1
    ND NS-interval is 1000 milliseconds
    ND reachable time is 30000 milliseconds
    ND router advertised managed config flag is disable
    ND router advertised other config flag is disable
    ND router advertisements are sent every 200 to 600 seconds
    ND router advertisements lifetime 1800 seconds

```

This example shows the OLT owns (L displays in the T field) two manually configured (permanent) IP addresses, 2001::1234 and fe80::219:cbff:fe00:1. It also displays a neighbor fe80::2d0:59ff:feb8:103c in VLAN 1 is reachable from the OLT.

```

sysname# show ipv6 neighbor
Address                               MAC           S   T Interface
-----+-----+-----+-----+-----+
2001::1234                           00:19:cb:0:0:0:1 R   L  vlan 1
fe80::219:cbff:fe00:1                00:19:cb:0:0:0:1 R   L  vlan 1
fe80::2d0:59ff:feb8:103c             00:d0:59:b8:10:3c R   D  vlan 1

S:
reachable(R),stale(S),delay(D),probe(P),invalid(IV),incomplete(I),unknown(?)
)
T: local(L),dynamic(D),static(S),other(O)

```

The following table describes the labels in this display.

Table 188 show ipv6 neighbor

LABEL	DESCRIPTION
Address	This is the IPv6 address of the OLT or a neighboring device.
MAC	This is the MAC address of the neighboring device or itself.

Table 188 show ipv6 neighbor (continued)

LABEL	DESCRIPTION
S	This displays whether the neighbor IPv6 interface is reachable. In IPv6, "reachable" means an IPv6 packet can be correctly forwarded to a neighbor node (host or router) and the neighbor can successfully receive and handle the packet. The available options in this field are: <ul style="list-style-type: none"> • reachable (R): The interface of the neighboring device is reachable. (The OLT has received a response to the initial request.) • stale (S): The last reachable time has expired and the OLT is waiting for a response to another initial request. The field displays this also when the OLT receives an un-requested response from the neighbor's interface. • delay (D): The neighboring interface is no longer known to be reachable, and traffic has been sent to the neighbor recently. The OLT delays sending request packets for a short to give upper-layer protocols a chance to determine reachability. • probe (P): The OLT is sending request packets and waiting for the neighbor's response. • invalid (IV): The neighbor address is with an invalid IPv6 address. • unknown (?): The status of the neighboring interface can not be determined for some reason. • incomplete (I): Address resolution is in progress and the link-layer address of the neighbor has not yet been determined (see RFC 2461). The interface of the neighboring device did not give a complete response.
T	This displays the type of an address mapping to a neighbor interface. The available options in this field are: <ul style="list-style-type: none"> • other (O): none of the following type. • dynamic (D): The IP address to MAC address can be successfully resolved using IPv6 Neighbor Discovery protocol (See Neighbor Discovery Protocol (NDP)). Is it similar as IPv4 ARP (Address Resolution protocol). • static (S): The interface address is statically configured. • local (L): A OLT interface is using the address.
Interface	This displays the VLAN the IPv6 interface is on.
Expire	This displays how long (<i>hhmmss</i>) an address can be used before it expires. If an address is manually configured, it displays permanent (never expires).

This example sends ping requests to an Ethernet device with IPv6 address fe80::2d0:59ff:feb8:103c in VLAN 1. The device also responds the pings.

```
sysname# ping6 ffe80::2d0:59ff:feb8:103c -i vlan 1
PING6(56=40+8+8 bytes) fe80::219:cbff:fe00:1 --> fe80::2d0:59ff:feb8:103c
16 bytes from fe80::2d0:59ff:feb8:103c, icmp_seq=0 hlim=64 time=1.0 ms
16 bytes from fe80::2d0:59ff:feb8:103c, icmp_seq=1 hlim=64 time=1.0 ms
16 bytes from fe80::2d0:59ff:feb8:103c, icmp_seq=2 hlim=64 time=1.0 ms

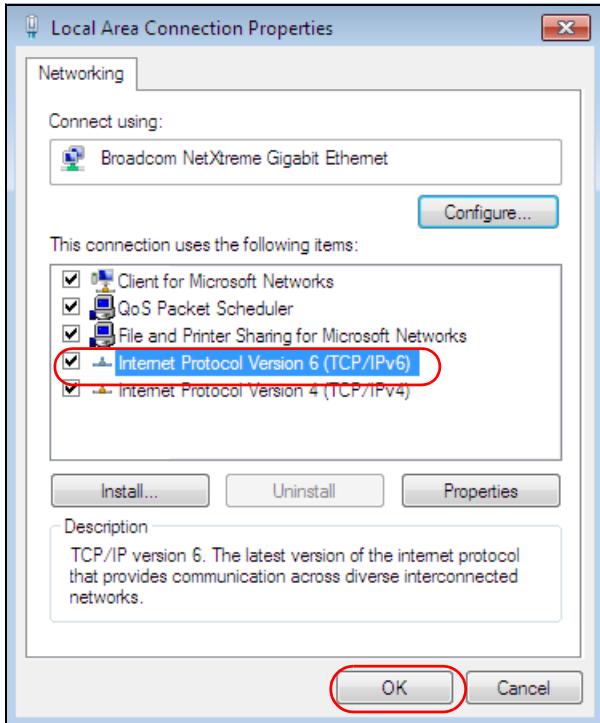
--- fe80::2d0:59ff:feb8:103c ping6 statistics ---
3 packets transmitted, 3 packets received, 0.0 % packet loss
round-trip min/avg/max = 1.0 /1.0 /1.0 ms
sysname#
```

50.4 Example - Enabling IPv6 on Windows 7/10

By default, IPv6 is enabled on Windows 7/10. This example shows you how to enable IPv6 on Windows 7/10. This also displays how to use the ipconfig command to see auto-generated IP addresses.

- 1 Select Control Panel > Network and Sharing Center > Change adapter settings.

- 2 Right-click on **Local Area Connection**, and select **Properties**.
- 3 Select the **Internet Protocol Version 6 (TCP/IPv6)** checkbox to enable it.
- 4 Click **OK** to save the change.



- 5 Click **Close** to exit the **Local Area Connection Status** screen.
- 6 Select **Start > All Programs > Accessories > Command Prompt**.
- 7 Use the **ipconfig** command to check your dynamic IPv6 address. This example shows a global address (2001:b021:2d::1000) obtained from a DHCP server.

```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

  Connection-specific DNS Suffix . :
  IPv6 Address . . . . . : 2001:b021:2d::1000
  Link-local IPv6 Address . . . . . : fe80::25d8:dcab:c80a:5189%11
  IPv4 Address . . . . . : 172.16.100.61
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : fe80::213:49ff:fea:7125%11
                                         172.16.100.254
```

IPv6 is installed and enabled by default in Windows Vista. Use the “ipconfig” command to check your automatic configured IPv6 address as well. You should see at least one IPv6 address available for the interface on your computer.

CHAPTER 51

VLAN

This chapter introduces the VLAN commands of the OLT.

51.1 Introduction to VLANs

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(s); 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 on the same network.

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.

Note: VLAN is unidirectional; it only governs outgoing traffic.

51.2 Introduction to IEEE 802.1Q Tagged VLANs

A 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 for the TPID (Tag Protocol Identifier, residing within the type/length field of the Ethernet frame) and two bytes for the TCI (Tag Control Information, starting 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 the value 4095 (FFF) is reserved, so the maximum possible number of VLAN configurations is 4,094.

TPID	User Priority	CFI	VLAN ID
2 Bytes	3 Bits	1 Bit	12 bits

51.2.1 Forwarding Tagged and Untagged Frames

Each port on the OLT 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 OLT 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 OLT 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.

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.

51.3 Static VLAN

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 outgoing frames (that were previously untagged) from a port with the specified VID.

51.4 VLAN Configuration Overview

- 1 Use the `vlan <vlan-id>` command to configure or create a VLAN on the OLT. The OLT automatically enters config-vlan mode. Use the `exit` command when you are finished configuring the VLAN.
- 2 Use the `interface port-channel <aid>` command to set the VLAN settings on a port. The OLT automatically enters config-interface mode. Use the `pvid <vlan-id>` command to set the VLAN ID you created for the port-list in the PVID table. Use the `exit` command when you are finished configuring the ports.

Note: The OLT will always configure the ONT to send out US packets with VLAN tag. The PON port must always be configured as egress tagged.

```

sysname (config)# vlan 2000
sysname (config-vlan)# name up1
sysname (config-vlan)# fixed eth-1
sysname (config-vlan)# no untagged eth-1
sysname (config-vlan)# exit
sysname (config)# interface port-channel eth-1
sysname (config-interface)# pvid 2000
sysname (config-interface)# exit

```

51.5 VLAN Commands

The following section lists the commands for this feature.

Table 189 VLAN Commands

COMMAND	DESCRIPTION	M	P
show vlan	Displays the status of all VLANs.	E	3
show vlan <vlan-id>	Displays the status of the specified VLAN.	E	3
vlan <1-4094>	Enters config-vlan mode for the specified VLAN. Creates the VLAN, if necessary.	C	13
fixed <aid>	Specifies the port(s) to be a permanent member of this VLAN group. aid: <pon eth>-<port> port list	C	13
no fixed <aid>	Sets fixed port(s) to normal port(s). aid: <pon eth>-<port> port list	C	13
forbidden <aid>	Specifies the port(s) you want to prohibit from joining this VLAN group. aid: <pon eth>-<port> port list	C	13
no forbidden <aid>	Sets forbidden port(s) to normal port(s). aid: <pon eth>-<port> port list	C	13
inactive	Disables the specified VLAN.	C	13
no inactive	Enables the specified VLAN.	C	13
name <name-str>	Specifies a name for identification purposes. <i>name-str</i> : 1-64 English keyboard characters	C	13
untagged <aid>	Specifies the port(s) you don't want to tag all outgoing frames transmitted with this VLAN Group ID. aid: <pon eth>-<port> port list	C	13
no untagged <aid>	Specifies the port(s) you want to tag all outgoing frames transmitted with this VLAN Group ID. aid: <pon eth>-<port> port list	C	13
ip address <ip-address> <mask>	Sets the IP address and subnet mask of the OLT in the specified VLAN.	C	13
no ip address <ip-address> <mask>	Deletes the IP address and subnet mask from this VLAN.	C	13

Table 189 VLAN Commands (continued)

COMMAND	DESCRIPTION	M	P
ip address <ip-address> <mask> manageable	Sets the IP address and subnet mask of the OLT in the specified VLAN. Some switch models require that you execute this command to ensure that remote management via HTTP, Telnet or SNMP is activated.	C	13
ip address default-gateway <ip-address>	Sets a default gateway IP address for this VLAN.	C	13
no ip address default-gateway	Deletes the default gateway from this VLAN.	C	13
no vlan <vlan-id>	Deletes a VLAN.	C	13

The following section lists the commands for the ingress checking feature. Enable or disable VLAN ingress checking on each port individually via the `ingress-check` command in the config-interface mode.

Table 190 Ingress Check Commands

COMMAND	DESCRIPTION	M	P
interface port-channel <aid>	Enters config-interface mode for the specified port(s). <code>aid: <pon eth>-<port></code>	C	13
ingress-check	Enables ingress checking on the specified ports. The OLT discards incoming frames for VLANs that do not include this port in its member set.	C	13
no ingress-check	Disables ingress checking on the specified ports.	C	13

Use these commands to configure VLAN port isolation on the OLT. VLAN port isolation allows each port to communicate only with the CPU management port and the uplink ports, but not to communicate with each other.

Table 191 `vlan1q port-isolation` Command Summary

COMMAND	DESCRIPTION	M	P
<code>vlan1q port-isolation</code>	Enables VLAN port isolation.	C	13
<code>no vlan1q port-isolation</code>	Disables VLAN port isolation.	C	13
<code>show vlan1q port-isolation</code>	Displays port isolation settings.	E	3

The following section lists the commands for the VLAN monitor counter feature. You can display the monitor counter for all or a specified VLAN.

Table 192 Monitor Counter Commands

COMMAND	DESCRIPTION		
<code>show monitor-counter vlan <vlan-id></code>	Displays the VLAN monitor counter for the specified VLAN or all VLANs. <code><vlan-id>: <vid> <all></code>	E	3
<code>clear interface <aid></code>	Clears all statistics from the interface status. <code>aid: <pon eth>-<port></code>	E	13

51.5.1 VLAN Command Examples

This example configures ports 10 to 15 as fixed and untagged ports in VLAN 2000.

```
sysname (config)# vlan 2000
sysname (config-vlan)# fixed 10-15
sysname (config-vlan)# untagged 10-15
```

This example deletes entry 4 in the static VLAN table.

```
sysname (config)# no vlan 4
```

This example shows the VLAN table.

```
sysname# show vlan
The Number of VLAN :      3
Idx.   VID    Status     Elap-Time
----  ----  -----
1      1      Static      2:41:38
TagCtl Tagged  :
TagCtl Untagged  :
pon-1,pon-2,pon-3,pon-4
eth-1,eth-2,eth-3,eth-4,eth-5,eth-6,eth-7,eth-8,eth-9,eth-10,eth-
11,eth-12,eth-13,eth-14,eth-15,eth-16,eth-17,eth-18,eth-19,et
h-20

2      2      Static      2:41:38
TagCtl Tagged  :
pon-1,pon-2,pon-3,pon-4
TagCtl Untagged  :

3  2000      Static      0:01:15
TagCtl Tagged  :
TagCtl Untagged  :
eth-6,eth-7,eth-8,eth-9,eth-10,eth-11
```

The following table describes the labels in this display.

Table 193 show vlan

LABEL	DESCRIPTION
The Number of VLAN	Displays the number of VLANs on the OLT.
Idx.	Displays an entry number for each VLAN.
VID	Displays the VLAN identification number.
Status	Displays how this VLAN was added to the OLT. Dynamic: The VLAN was added via GVRP. Static: The VLAN was added as a permanent entry Other: The VLAN was added in another way, such as Multicast VLAN Registration (MVR).

Table 193 show vlan (continued)

LABEL	DESCRIPTION
Elap-Time	Displays how long it has been since a dynamic VLAN was registered or a static VLAN was set up.
TagCtl	Displays untagged and tagged ports. Untagged: These ports do not tag outgoing frames with the VLAN ID. Tagged: These ports tag outgoing frames with the VLAN ID.

This example enables ingress checking on port 1.

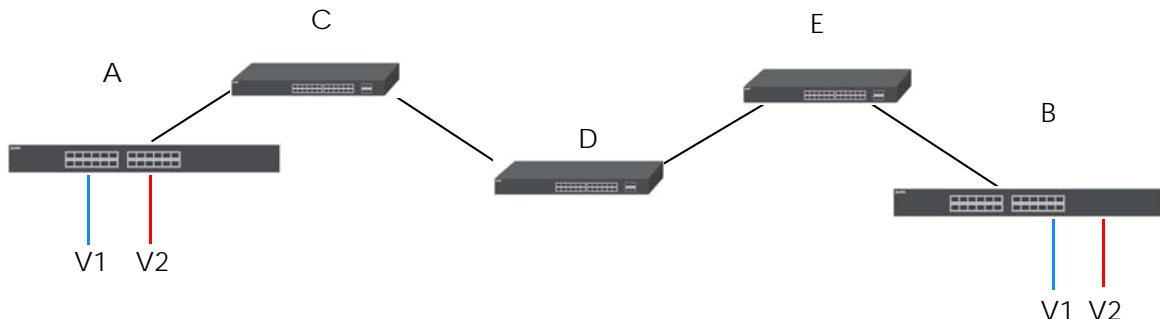
```
sysname(config)# interface port-channel eth-1
sysname(config-interface)# ingress-check
```

51.6 Port VLAN Trunking

Enable VLAN trunking on a port to allow frames belonging to unknown VLAN groups to pass through that port. This is useful if you want to set up VLAN groups on end devices without having to configure the same VLAN groups on intermediary devices.

The following figure describes VLAN trunking. Suppose you want to create VLAN groups 1 and 2 (V1 and V2) on devices A and B. Without VLAN trunking, you must configure VLAN groups 1 and 2 on all intermediary switches C, D and E; otherwise they will drop frames with unknown VLAN group tags. However, with VLAN trunking enabled on a port(s) in each intermediary switch you only need to create VLAN groups in the end devices (A and B). C, D and E automatically allow frames with VLAN group tags 1 and 2 (VLAN groups that are unknown to those switches) to pass through their VLAN trunking port(s).

Figure 218 Port VLAN Trunking



The following section lists the commands for this feature.

Table 194 Port VLAN Trunking Commands

COMMAND	DESCRIPTION	M	P
interface port-channel <aid>	Enters config-interface mode for the specified port(s). <i>aid: <pon eth>-<port></i>	C	13
vlan-trunking	Enables VLAN trunking on ports connected to other switches or routers (but not ports directly connected to end users). This allows frames belonging to unknown VLAN groups to go out via the VLAN-trunking port.	C	13
no vlan-trunking	Disables VLAN trunking on the port(s).	C	13

51.6.1 VLAN Trunking Setup Commands Example

This example enables VLAN trunking on port 1.

```
sysname# config
sysname(config)# interface port-channel eth-1
sysname(config-interface)# vlan-trunking
```

This example disables VLAN trunking on port 1.

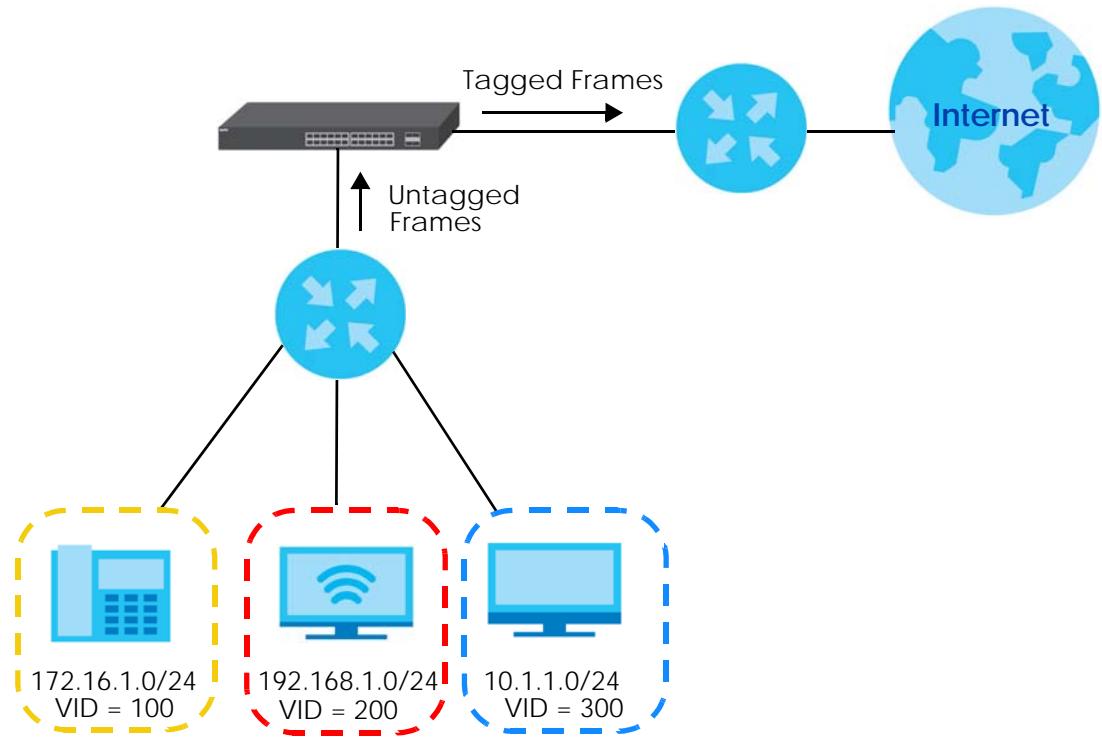
```
sysname# config
sysname(config)# interface port-channel pon-1
sysname(config-interface)# no vlan-trunking
```

51.7 Subnet Based VLANs

Subnet based VLANs allow you to group traffic into logical VLANs based on the source IP subnet you specify. When a frame is received on a port, the OLT checks if a tag is added already and the IP subnet it came from. The untagged packets from the same IP subnet are then placed in the same subnet based VLAN. One advantage of using subnet based VLANs is that priority can be assigned to traffic from the same IP subnet.

For example, an ISP (Internet Service Provider) may divide different types of services it provides to customers into different IP subnets. Traffic for voice services is designated for IP subnet 172.16.1.0/24, video for 192.168.1.0/24 and data for 10.1.1.0/24. The OLT can then be configured to group incoming traffic based on the source IP subnet of incoming frames.

You can then configure a subnet based VLAN with priority 6 and VID of 100 for traffic received from IP subnet 172.16.1.0/24 (voice services). You can also have a subnet based VLAN with priority 5 and VID of 200 for traffic received from IP subnet 192.168.1.0/24 (video services). Lastly, you can configure VLAN with priority 3 and VID of 300 for traffic received from IP subnet 10.1.1.0/24 (data services). All untagged incoming frames will be classified based on their source IP subnet and prioritized accordingly. That is, video services receive the highest priority and data the lowest.

Figure 219 Subnet Based VLAN Application Example

Note: Subnet based VLAN applies to un-tagged packets and is applicable only when you use IEEE 802.1Q tagged VLAN.

51.8 Subnet Based VLAN Commands

The following section lists the commands for this feature.

Table 195 Subnet Based VLAN Commands

COMMAND	DESCRIPTION	M	P
show subnet-vlan	Displays subnet based VLAN settings on the OLT.	E	3
subnet-based-vlan	Enables subnet based VLAN on the OLT.	C	13
subnet-based-vlan dhcp-vlan-override	Sets the OLT to force the DHCP clients to obtain their IP addresses through the DHCP VLAN.	C	13
subnet-based-vlan name <name> source-ip <ip> mask-bits <mask-bits> vlan <vid> priority <0-7>	Specifies the name, IP address, subnet mask, VLAN ID of the subnet based VLAN you want to configure along with the priority you want to assign to the outgoing frames for this VLAN.	C	13
subnet-based-vlan name <name> source-ip <ip> mask-bits <mask-bits> vlan <vlan-id> priority <0-7> inactive	Disables the specified subnet-based VLAN.	C	13
no subnet-based-vlan	Disables subnet-based VLAN on the OLT.	C	13

Table 195 Subnet Based VLAN Commands (continued)

COMMAND	DESCRIPTION	M	P
no subnet-based-vlan source-ip <ip> mask-bits <mask-bits>	Removes the specified subnet from the subnet-based VLAN configuration.	C	13
no subnet-based-vlan dhcp-vlan-override	Disables the DHCP VLAN override setting for subnet-based VLAN(s).	C	13

51.8.1 Subnet-based VLAN Command Examples

This example configures a subnet-based VLAN (**subnet1VLAN**) with priority **6** and a VID of **200** for traffic received from IP subnet **172.16.37.1/24**.

```
sysname# subnet-based-vlan name subnet1VLAN source-ip 172.16.37.1 mask-bits
--> 24 vlan 200 priority 6
sysname(config)# exit
sysname# show subnet-vlan

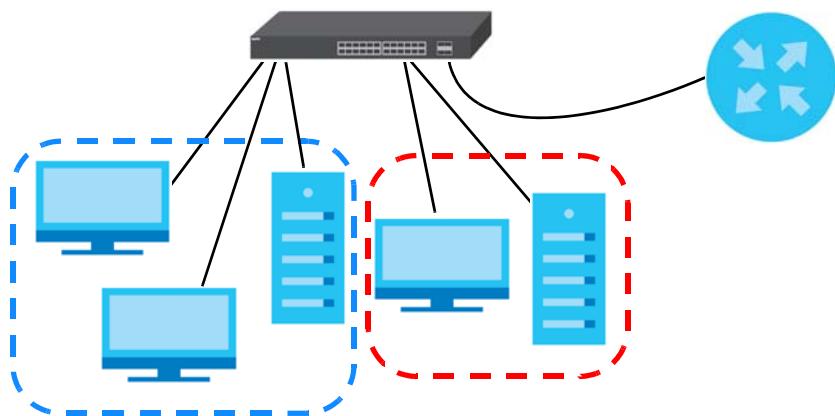
Global Active :Yes
      Name      Src IP   Mask-Bits   Vlan   Priority   Entry Active
-----  -----  -----  -----  -----  -----
subnet1VLAN  172.16.37.1        24     200        6           1
```

51.9 Protocol Based VLANs

Protocol based VLANs allow you to group traffic into logical VLANs based on the protocol you specify. When an upstream frame is received on a port (configured for a protocol based VLAN), the OLT checks if a tag is added already and its protocol. The untagged packets of the same protocol are then placed in the same protocol based VLAN. One advantage of using protocol based VLANs is that priority can be assigned to traffic of the same protocol.

Note: Protocol based VLAN applies to un-tagged packets and is applicable only when you use IEEE 802.1Q tagged VLAN.

For example, ports 1, 2, 3, and 4 belong to static VLAN 100, and ports 4, 5, 6, 7 belong to static VLAN 120. You can configure a protocol based VLAN A with priority 3 for ARP traffic received on port 1, 2 and 3. You can also have a protocol based VLAN B with priority 2 for Apple Talk traffic received on port 6 and 7. All upstream ARP traffic from ports 1, 2, and 3 will be grouped together, and all upstream Apple Talk traffic from ports 6 and 7 will be in another group and have higher priority than ARP traffic when they go through the uplink port to a backbone switch C.

Figure 220 Protocol Based VLAN Application Example

51.9.1 Protocol Based VLAN Commands

The following section lists the commands for this feature.

Table 196 Protocol Based VLAN Commands

COMMAND	DESCRIPTION	M	P
<code>show interfaces config <aid> protocol-based-vlan</code>	Displays the protocol based VLAN settings for the specified port(s). <code>aid: <pon eth>-<port></code>	E	3
<code>interface port-channel <aid></code>	Enters sub-command mode for configuring the specified ports. <code>aid: <pon eth>-<port></code>	C	13

Table 196 Protocol Based VLAN Commands (continued)

COMMAND	DESCRIPTION	M	P
<code>protocol-based-vlan name <name> ethernet-type <ether-num ip ipx arp rarp appletalk decnet> vlan <vid> priority <0-7></code>	<p>Creates a protocol based VLAN with the specified parameters.</p> <p><i>name</i>: Use up to 32 alphanumeric characters.</p> <p><i>ether-num</i>: If you don't select a predefined Ethernet protocol (ip, ipx, arp, rarp, appletalk or decnet), type the protocol number in hexadecimal notation with a prefix, "0x". For example, type "0x0800" for the IP protocol and type "0x8137" for the Novell IPX protocol.</p> <p>Note: Protocols in the hexadecimal number range 0x0000 to 0x05ff are not allowed.</p> <p><i>priority</i>: Specify the IEEE 802.1p priority that the OLT assigns to frames belonging to this VLAN.</p>	C	13
<code>protocol-based-vlan name <name> ethernet-type <ether-num ip ipx arp rarp appletalk decnet> vlan <vid> priority <0-7> inactive</code>	<p>Creates a disabled protocol based VLAN with the specified parameters.</p> <p><i>name</i>: Use up to 32 alphanumeric characters.</p> <p><i>ether-num</i>: If you don't select a predefined Ethernet protocol (ip, ipx, arp, rarp, appletalk or decnet), type the protocol number in hexadecimal notation with a prefix, "0x". For example, type 0x0800 for the IP protocol and type 0x8137 for the Novell IPX protocol.</p> <p>Note: Protocols in the hexadecimal number range 0x0000 to 0x05ff are not allowed.</p> <p><i>priority</i>: Specify the IEEE 802.1p priority that the OLT assigns to frames belonging to this VLAN.</p>	C	13

51.9.2 Protocol Based VLAN Command Examples

This example creates a VLAN rule based on the IP Ethernet protocol and named IP_VLAN on port 1 with a VLAN ID of 200 and a priority 6.

```

sysname(config)# interface port-channel eth-1
sysname(config-interface)# protocol-based-vlan name IP_VLAN ethernet-type ip
--> vlan 200 priority 6
sysname(config-interface)# exit
sysname(config)# exit
sysname# show interfaces config ge-5-1&&-4 protocol-based-vlan
      Name  Port  Packet type  Ethernet type  Vlan  Priority  Active
      -----  ----  -----  -----  -----  -----  -----
IP_VLAN    9    EtherII        ip    200       6    Yes
IP_VLAN   10    EtherII        ip    200       6    Yes
IP_VLAN   11    EtherII        ip    200       6    Yes
IP_VLAN   12    EtherII        ip    200       6    Yes

```

CHAPTER 52

Static MAC Forwarding

Use this chapter to configure static MAC address forwarding rules based on MAC addresses of devices on your network.

52.1 Static MAC Forwarding Overview

A static MAC address is an address that has been manually entered in the MAC address table. Static MAC addresses do not age out. When you set up static MAC address rules, you are setting static MAC addresses for a port. This may reduce the need for broadcasting.

Static MAC address forwarding together with port security allows only computers in the MAC address table on a port to access the OLT. See [Chapter 65 on page 453](#) for more information on port security.

52.2 Static MAC Forwarding Commands

Use these commands to configure static MAC address forwarding.

Note: Use the `mac` commands to look at the current `mac-forward` settings. See [Chapter 81 on page 565](#).

Table 197 Static MAC Forwarding Commands

COMMAND	DESCRIPTION	M	P
<code>mac-forward name <name> mac <mac-addr> vlan <vlan-id> interface <pon eth>-<port></code>	Configures a static MAC address forwarding rule. The name can be 1-32 alphanumeric characters.	C	13
<code>no mac-forward mac <mac-addr> vlan <vlan-id> interface <interface-id></code>	Removes the specified MAC forwarding entry, belonging to a VLAN group forwarded through an interface.	C	13
<code>mac-forward name <name> mac <mac-addr> vlan <vlan-id> interface <pon eth>-<port> inactive</code>	Disables a static MAC address forwarding rule.	C	13
<code>no mac-forward mac <mac-addr> vlan <vlan-id> interface <interface-id> inactive</code>	Enables the specified MAC address, belonging to a VLAN group forwarded through an interface.	C	13

This example configures unicast address 10:11:11:11:11:11 as a static MAC address on VLAN 3 belonging to **PON1**.

```
sysname# mac-forward name mcfw mac 10:11:11:11:11:11 vlan 3 interface  
pon-1
```

CHAPTER 53

Static Multicast Forwarding

Use these commands to configure static multicast address forwarding.

53.1 Static Multicast Forwarding Overview

A multicast MAC address is the MAC address of a member of a multicast group. A static multicast address is a multicast MAC address that has been manually entered in the multicast table. Static multicast addresses do not age out. Static multicast forwarding allows you (the administrator) to forward multicast frames to a member without the member having to join the group first.

If a multicast group has no members, then the switch will either flood the multicast frames to all ports or drop them. You can configure this using the `igmp-snooping unknown-multicast-frame <drop|flooding>` command. [Figure 221](#) shows such unknown multicast frames flooded to all ports. With static multicast forwarding, you can forward these multicasts to port(s) within a VLAN group. [Figure 222](#) shows frames being forwarded to devices connected to port 3. [Figure 223](#) shows frames being forwarded to ports 2 and 3 within VLAN group 4.

Figure 221 No Static Multicast Forwarding

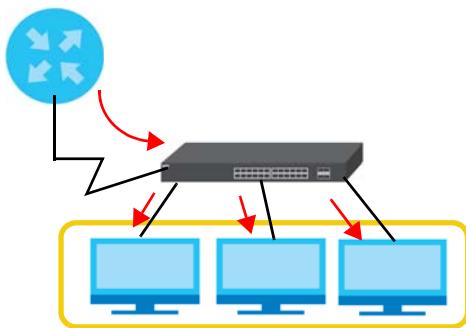


Figure 222 Static Multicast Forwarding to A Single Port

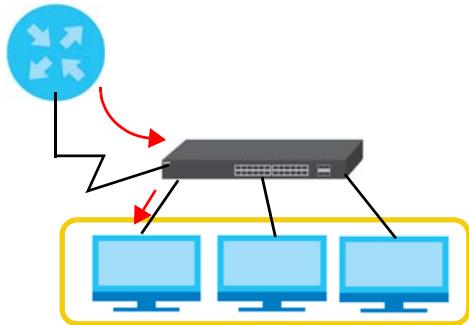
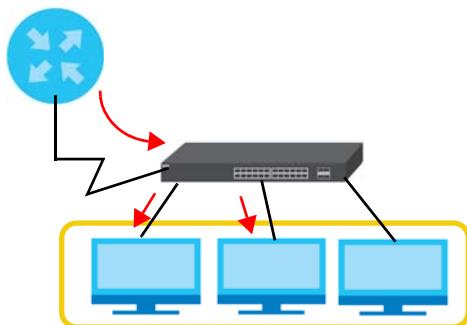


Figure 223 Static Multicast Forwarding to Multiple Ports



53.2 Static Multicast Forwarding Commands

Use the `multicast-forward` command to configure rules to forward specific multicast frames, such as streaming or control frames, to specific port(s).

The following section lists the commands for this feature.

Table 198 Static Multicast Forwarding Commands

COMMAND	DESCRIPTION	M	P
show mac address-table multicast	Displays the multicast MAC address table.	E	3
multicast-forward name <name> mac <mac-addr> vlan <vlan> inactive	<p>Deactivates a static multicast forwarding rule. The rule name can be up to 32 printable ASCII characters.</p> <p><i>mac-addr</i>: Enter a multicast MAC address which identifies the multicast group. The last binary bit of the first octet pair in a multicast MAC address must be 1. For example, the first octet pair 00000001 is "01" and 00000011 is "03" in hexadecimal, so 01:00:5e:00:00:0A and 03:00:5e:00:00:27 are valid multicast MAC addresses.</p> <p><i>vlan</i>: A VLAN identification number.</p> <p>Note: Static multicast addresses do not age out.</p>	C	13
multicast-forward name <name> mac <mac-addr> vlan <vlan> interface port-channel <aid>	Associates a static multicast forwarding rule with specified port(s) within a specified VLAN.	C	13
no multicast-forward mac <mac-addr> vlan <vlan-id>	Removes a specified static multicast rule.	C	13
no multicast-forward mac <mac-addr> vlan <vlan-id> inactive	Activates a specified static multicast rule.	C	13

53.3 Static Multicast Forwarding Command Examples

This example shows the current multicast table. The **Type** field displays **User** for rules that were manually added through static multicast forwarding or displays **System** for rules the OLT has automatically learned through IGMP snooping.

```
sysname# show mac address-table multicast
The Number of Multicast-forward : 1
Idx.    MAC Address        VLAN ID      Type
----  -----
1       01:a0:c5:aa:aa:aa   1           Dynamic
Port : cpu
```

This example removes a static multicast forwarding rule with multicast MAC address (01:00:5e:06:01:46) which belongs to VLAN 1.

```
sysname# no multicast-forward mac 01:00:5e:06:01:46 vlan 1
```

This example creates a static multicast forwarding rule. The rule forwards frames with destination MAC address 01:00:5e:00:00:06 to **PON1** in VLAN 1.

```
sysname# configure
sysname(config)# multicast-forward name AAA mac 01:00:5e:00:00:06 vlan 1 interface
port-channel pon-1
```

CHAPTER 54

AAA

Use these commands to configure authentication, authorization and accounting on the OLT.

54.1 AAA Overview

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 OLT, your OLT 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 199 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 OLT and the TACACS+ server is encrypted.

54.2 AAA Commands

The following section lists the commands for this feature.

Table 200 AAA Commands

COMMAND	DESCRIPTION	M	P
aaa accounting commands <privilege> stop-only tacacs+	Enables accounting of command sessions and specifies the minimum privilege level (0-14) for the command sessions that should be recorded.	C	13
aaa accounting commands <privilege> stop-only tacacs+ [broadcast]	Enables accounting of command sessions and specifies the minimum privilege level (0-14) for the command sessions that should be recorded. Sends accounting information for command sessions to all configured accounting servers at the same time.	C	13
aaa accounting dot1x <start-stop stop-only> <radius tacacs+>	Enables accounting of IEEE 802.1x authentication sessions and specifies the mode and protocol method. The OLT 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.	C	13
aaa accounting dot1x <start-stop stop-only> <radius tacacs+> [broadcast]	Enables accounting of IEEE 802.1x authentication sessions and specifies the mode and protocol method. Sends accounting information for IEEE 802.1x authentication sessions to all configured accounting servers at the same time.	C	13
aaa accounting exec <start-stop stop-only> <radius tacacs+>	Enables accounting of administrative sessions via SSH, Telnet and console port and specifies the mode and protocol method.	C	13

Table 200 AAA Commands (continued)

COMMAND	DESCRIPTION	M	P
aaa accounting exec <start-stop stop-only> <radius tacacs+> [broadcast]	Enables accounting of administrative sessions via SSH, Telnet and console port and specifies the mode and protocol method. Sends accounting information for administrative sessions via SSH, Telnet and console port to all configured accounting servers at the same time.	C	13
aaa accounting system <radius tacacs+>	Enables accounting of system events and specifies the protocol method.	C	13
aaa accounting system <radius tacacs+> [broadcast]	Enables accounting of system events and specifies the protocol method. Sends accounting information for system events to all configured accounting servers at the same time.	C	13
aaa accounting update periodic <1-2147483647>	Sets the update period (in minutes) for accounting sessions. This is the time the OLT waits to send an update to an accounting server after a session starts.	C	13
aaa authentication enable <method1> [<method2>...]	Specifies which method should be used first, second, and third for checking privileges. method: enable, radius, or tacacs+.	C	14
aaa authentication login <method1> [<method2>...]	Specifies which method should be used first, second, and third for the authentication of login accounts. method: enable, radius, or tacacs+.	C	14
aaa authorization dot1x radius	Enables authorization for IEEE 802.1x clients using RADIUS.	C	14
aaa authorization exec <radius tacacs+>	Specifies which method (radius or tacacs+) should be used for administrator authorization.	C	14
no aaa accounting commands	Disables accounting of command sessions on the OLT.	C	13
no aaa accounting dot1x	Disables accounting of IEEE 802.1x authentication sessions on the OLT.	C	13
no aaa accounting exec	Disables accounting of administrative sessions via SSH, Telnet or console on the OLT.	C	13
no aaa accounting system	Disables accounting of system events on the OLT.	C	13
no aaa accounting update	Resets the accounting update interval to the default value.	C	13
no aaa authentication enable	Resets the method list for checking privileges to its default value.	C	14
no aaa authentication login	Resets the method list for the authentication of login accounts to its default value.	C	14
no aaa authorization dot1x	Disables authorization of allowing an IEEE 802.1x client to have a different bandwidth limit or VLAN ID assigned via the external server.	C	14
no aaa authorization exec	Disables authorization of allowing an administrator which logs into the OLT through Telnet or SSH to have a different access privilege level assigned via the external server.	C	14
show aaa accounting	Displays accounting settings configured on the OLT.	E	3

Table 200 AAA Commands (continued)

COMMAND	DESCRIPTION	M	P
show aaa accounting commands	Displays accounting settings for recording command events.	E	3
show aaa accounting dot1x	Displays accounting settings for recording IEEE 802.1x session events.	E	3
show aaa accounting exec	Displays accounting settings for recording administrative sessions via SSH, Telnet or the console port.	E	3
show aaa accounting system	Displays accounting settings for recording system events, for example system shut down, start up, accounting enabled or accounting disabled.	E	3
show aaa accounting update	Displays the update period setting on the OLT for accounting sessions.	E	3
show aaa authentication	Displays what methods are used for authentication.	E	3
show aaa authentication enable	Displays the authentication method(s) for checking privilege level of administrators.	E	3
show aaa authentication login	Displays the authentication methods for administrator login accounts.	E	3
show aaa authorization	Displays authorization settings configured on the OLT.	E	3
show aaa authorization dot1x	Displays the authorization method used to allow an IEEE 802.1x client to have a different bandwidth limit or VLAN ID assigned via the external server.	E	3
show aaa authorization exec	Displays the authorization method used to allow an administrator which logs into the OLT through Telnet or SSH to have a different access privilege level assigned via the external server.	E	3

CHAPTER 55

TACACS+

Use these commands to configure external TACACS+ (Terminal Access Controller Access-Control System Plus) servers.

55.1 TACACS+ Commands Summary

The following section lists the commands for this feature.

Table 201 TACACS+ Commands

COMMAND	DESCRIPTION	M	P
show tacacs-accounting	Displays TACACS+ accounting server settings.	E	3
tacacs-accounting host <index> <ip>	Specifies the IP address of the specified TACACS+ accounting server. <i>index</i> : 1 or 2.	C	13
tacacs-accounting host <index> <ip> [acct-port <socket-number>] [key <key-string>]	Specifies the IP address of the specified TACACS+ accounting server. Optionally, sets the port number and key of the external TACACS+ accounting server. <i>index</i> : 1 or 2. <i>key-string</i> : 1-32 alphanumeric characters	C	13
tacacs-accounting timeout <1-1000>	Specifies the TACACS+ accounting server timeout value in seconds.	C	13
no tacacs-accounting <index>	Disables TACACS+ accounting on the specified server.	C	13
tacacs-server host <index> <ip>	Specifies the IP address of the specified TACACS+ server. <i>index</i> : 1 or 2.	C	14
tacacs-server host <index> <ip> [auth-port <socket-number>] [key <key-string>]	Specifies the IP address of the specified TACACS+ server. Optionally, sets the port number and key of the TACACS+ server. <i>index</i> : 1 or 2. <i>key-string</i> : 1-32 alphanumeric characters	C	14
tacacs-server mode <index-priority> round-robin>	Specifies the mode for TACACS+ server selection. <i>index-priority</i> : 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. <i>round-robin</i> : alternate between the TACACS+ servers.	C	14

Table 201 TACACS+ Commands (continued)

COMMAND	DESCRIPTION	M	P
tacacs-server timeout <1-1000>	Specifies the TACACS+ server timeout value.	C	14
no tacacs-server <index>	Disables TACACS+ authentication on the specified server.	C	14
show tacacs-server	Displays TACACS+ server settings.	E	3

CHAPTER 56

Display Commands

Use these commands to display configuration information.

56.1 Display Commands Summary

The following section lists the commands for this feature.

Table 202 Display Commands

COMMAND	DESCRIPTION	M	P
display aaa	Enables all options of displaying AAA configuration.	C	14
display aaa <[authentication][authorization][server]>	Displays all or specific AAA information in the configuration file. authentication: Displays authentication information in the configuration file. authorization: Displays authorization information in the configuration file. server: Displays authentication server information in the configuration file.	C	14
display user	Enables all options of displaying user configuration.	C	14
display user <[system] [snmp]>	Displays all or specific user account information in the configuration file. system: Displays system account information, such as admin, enable or login username and password. snmp: Displays SNMP user account information.	C	14
no display aaa	Disables all options of displaying AAA configuration.	C	14
no display aaa <[authentication][authorization]>	Hides all or specific AAA information in the configuration file.	C	14
no display user	Disables all options of displaying user configuration.	C	14
no display user <[system] [snmp]>	Displays all or specific user account information in the configuration file.	C	14

CHAPTER 57

Filtering

This chapter discusses MAC address port filtering.

57.1 MAC Filtering Overview

Configure the OLT to filter traffic based on the traffic's source, destination MAC addresses and VLAN group (ID).

57.2 MAC Filtering Commands

The following section lists the commands for this feature.

Table 203 MAC Filtering Commands

COMMAND	DESCRIPTION	M	P
no mac-filter mac <mac-addr> vlan <vlan-id>	Deletes the specified MAC filter rule.	C	13
mac-filter name <name> mac <mac-addr> vlan <vlan-id> drop <src dst both>	Specifies the source and or destination filter parameters.	C	13
mac-filter name <name> mac <mac-addr> vlan <vlan-id> drop <src dst both> inactive	Disables a static MAC address port filtering rule. <i>name</i> : 1-32 alphanumeric characters	C	13
no mac-filter mac <mac-addr> vlan <vlan-id> inactive	Enables the specified MAC-filter rule.	C	13

57.3 MAC Filtering Commands Examples

This example creates a MAC filter called "filter1" that drops packets coming from or going to the MAC address 00:12:00:12:00:12 on VLAN 1.

```
sysname(config)# mac-filter name filter1 mac 00:12:00:12:00:12 vlan 1 drop both
```

57.3.1 Command Example: Filter Source

The next example is for OLTs that support the filtering of frames based on the source or destination MAC address only. This example creates a filter “sourcefilter” that drops packets originating from the unicast MAC address 00:12:00:12:00:12 on VLAN 3.

```
sysname(config)# mac-filter name sourcefilter mac 00:12:00:12:00:12 vlan 3  
drop src
```

CHAPTER 58

Spanning Tree Protocol

The OLT supports Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP) as defined in the following standards.

- IEEE 802.1D Spanning Tree Protocol
- IEEE 802.1w Rapid Spanning Tree Protocol
- IEEE 802.1s Multiple Spanning Tree Protocol

The OLT also allows you to set up multiple STP configurations (or trees). Ports can then be assigned to the trees.

58.1 STP/RSTP Overview

(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a OLT to interact with other (R)STP-compliant switches in your network to ensure that only one path exists between any two stations on the network.

The OLT uses IEEE 802.1w RSTP (Rapid Spanning Tree Protocol) that allows faster convergence of the spanning tree than STP (while also being backwards compatible with STP-only aware bridges). In RSTP, topology change information is directly propagated throughout the network from the device that generates the topology change. In STP, a longer delay is required as the device that causes a topology change first notifies the root bridge and then the root bridge notifies the network. Both RSTP and STP flush unwanted learned addresses from the filtering database. In RSTP, the port states are Discarding, Learning, and Forwarding.

Note: In this user's guide, "STP" refers to both STP and RSTP.

58.1.1 STP Terminology

The root bridge is the base of the spanning tree.

Path cost is the cost of transmitting a frame onto a LAN through that port. The recommended cost is assigned according to the speed of the link to which a port is attached. The slower the media, the higher the cost.

Table 204 STP Path Costs

	LINK SPEED	RECOMMENDED VALUE	RECOMMENDED RANGE	ALLOWED RANGE
Path Cost	4 Mbps	250	100 to 1000	1 to 65535
Path Cost	10 Mbps	100	50 to 600	1 to 65535

Table 204 STP Path Costs

	LINK SPEED	RECOMMENDED VALUE	RECOMMENDED RANGE	ALLOWED RANGE
Path Cost	16 Mbps	62	40 to 400	1 to 65535
Path Cost	100 Mbps	19	10 to 60	1 to 65535
Path Cost	1 Gbps	4	3 to 10	1 to 65535
Path Cost	10 Gbps	2	1 to 5	1 to 65535

On each bridge, the bridge communicates with the root through the root port. The root port is the port on this OLT with the lowest path cost to the root (the root path cost). If there is no root port, then this OLT 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.

58.1.2 How STP Works

After a bridge determines the lowest cost-spanning tree with STP, it enables the root port and the ports that are the designated ports for connected LANs, and disables all other ports that participate in STP. Network packets are therefore only forwarded between enabled ports, eliminating any possible network loops.

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

Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the root bridge. If a bridge does not get a Hello BPDU after a predefined interval (Max Age), the bridge assumes that the link to the root bridge is down. This bridge then initiates negotiations with other bridges to reconfigure the network to re-establish a valid network topology.

58.1.3 STP Port States

STP assigns five port states to eliminate packet looping. A bridge port is not allowed to go directly from blocking state to forwarding state so as to eliminate transient loops.

Table 205 STP Port States

PORT STATE	DESCRIPTION
Disabled	STP is disabled (default).
Blocking	Only configuration and management BPDUs are received and processed.
Listening	All BPDUs are received and processed. Note: The listening state does not exist in RSTP.
Learning	All BPDUs are received and processed. Information frames are submitted to the learning process but not forwarded.
Forwarding	All BPDUs are received and processed. All information frames are received and forwarded.

58.1.4 Multiple STP

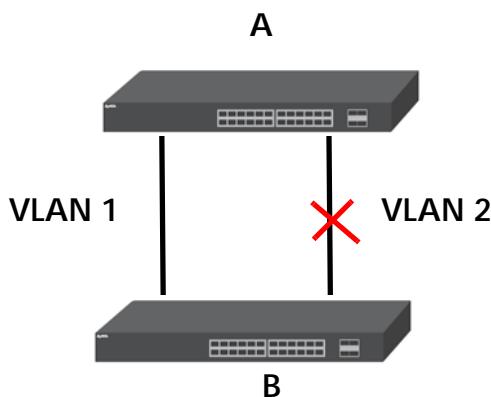
Multiple Spanning Tree Protocol (IEEE 802.1s) is backwards compatible with STP/RSTP and addresses the limitations of existing spanning tree protocols (STP and RSTP) in networks to include the following features:

- One Common and Internal Spanning Tree (CIST) that represents the entire network's connectivity.
- Grouping of multiple bridges (or switching devices) into regions that appear as one single bridge on the network.
- A VLAN can be mapped to a specific Multiple Spanning Tree Instance (MSTI). MSTI allows multiple VLANs to use the same spanning tree.
- Load-balancing is possible as traffic from different VLANs can use distinct paths in a region.

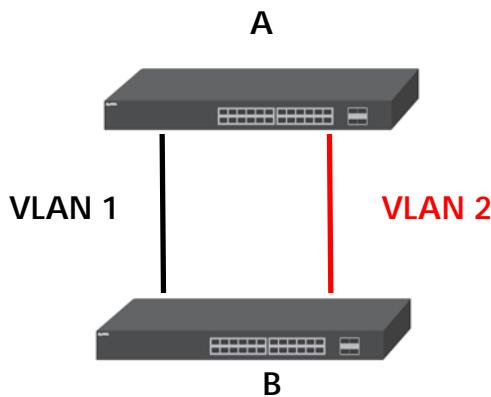
58.1.4.1 MSTP Network Example

The following figure shows a network example where two VLANs are configured on the two switches. If the switches are using STP or RSTP, the link for VLAN 3 will be blocked as STP and RSTP allow only one link in the network and block the redundant link.

Figure 224 STP/RSTP Network Example



With MSTP, VLANs 1 and 3 are mapped to different spanning trees in the network. Thus traffic from the two VLANs travel on different paths. The following figure shows the network example using MSTP.

Figure 225 MSTP Network Example

58.1.4.2 MST Region

An MST region is a logical grouping of multiple network devices that appears as a single device to the rest of the network. Each MSTP-enabled device can only belong to one MST region. When BPDUs enter an MST region, external path cost (of paths outside this region) is increased by one. Internal path cost (of paths within this region) is increased by one when BPDUs traverse the region.

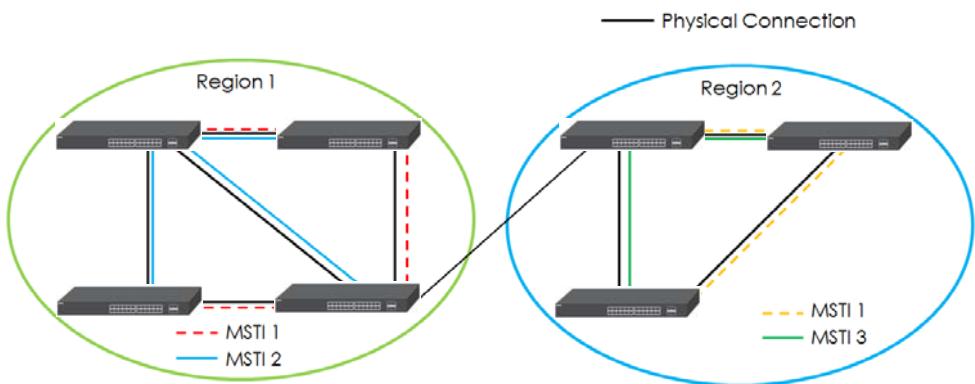
Devices that belong to the same MST region are configured to have the same MSTP configuration identification settings. These include the following parameters:

- Name of the MST region
- Revision level as the unique number for the MST region
- VLAN-to-MST Instance mapping

58.1.4.3 MST Instance

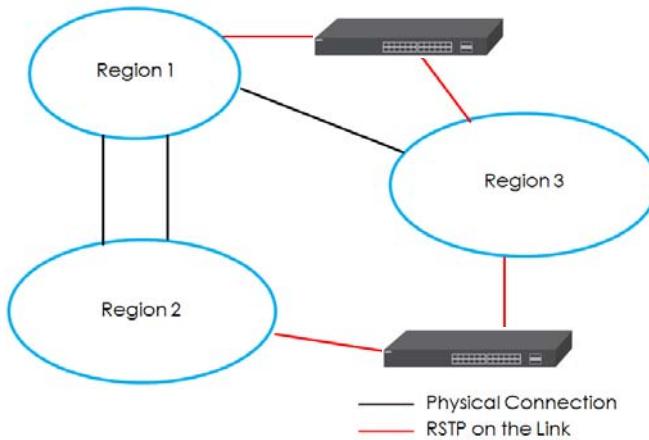
An MST Instance (MSTI) is a spanning tree instance. VLANs can be configured to run on a specific MSTI. Each created MSTI is identified by a unique number (known as an MST ID) known internally to a region. Thus an MSTI does not span across MST regions.

The following figure shows an example where there are two MST regions. Regions 1 and 2 have 2 spanning tree instances.

Figure 226 MSTIs in Different Regions

58.1.4.4 Common and Internal Spanning Tree (CIST)

A CIST represents the connectivity of the entire network and it is equivalent to a spanning tree in an STP/RSTP. The CIST is the default MST instance (MSTID 0). Any VLANs that are not members of an MST instance are members of the CIST. In an MSTP-enabled network, there is only one CIST that runs between MST regions and single spanning tree devices. A network may contain multiple MST regions and other network segments running RSTP.

Figure 227 MSTP and Legacy RSTP Network Example

58.2 STP and RSTP Commands

Use these commands to configure 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

See [Section 58.3 on page 433](#) for more information on MSTP commands. See also [Chapter 74 on page 526](#) for information on loopguard commands.

Table 206 STP and RSTP Commands

COMMAND	DESCRIPTION	M	P
show spanning-tree config	Displays Spanning Tree Protocol (STP) settings.	E	3
spanning-tree mode <RSTP MSTP>	Specifies the STP mode you want to implement on the OLT.	C	13
spanning-tree	Enables STP on the OLT.	C	13
no spanning-tree	Disables STP on the OLT.	C	13
spanning-tree hello-time <1-10> maximum-age <6-40> forward-delay <4-30>	Sets Hello Time, Maximum Age and Forward Delay. <i>hello-time</i> : The time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. <i>maximum-age</i> : The maximum time (in seconds) the OLT can wait without receiving a BPDU before attempting to reconfigure. <i>forward-delay</i> : The maximum time (in seconds) the OLT will wait before changing states.	C	13
spanning-tree priority <0-61440>	Sets the bridge priority of the OLT. The lower the numeric value you assign, the higher the priority for this bridge. <i>priority</i> : Must be a multiple of 4096.	C	13
spanning-tree <aid>	Enables STP on a specified ports. <i>aid</i> : eth-<port>	C	13
no spanning-tree <aid>	Disables STP on listed ports. <i>aid</i> : eth-<port>	C	13
spanning-tree <aid> path-cost <1-65535>	Specifies the cost of transmitting a frame to a LAN through the port(s). It is assigned according to the speed of the bridge. <i>aid</i> : eth-<port>	C	13
spanning-tree <aid> priority <0-255>	Sets the priority for the specified ports. Priority decides which port should be disabled when more than one port forms a loop in a OLT. Ports with a higher priority numeric value are disabled first. <i>aid</i> : eth-<port>	C	13
spanning-tree help	Provides more information about the specified command.	C	13

58.2.1 STP and RSTP Command Examples

This example configures STP in the following ways:

- 1 Enables STP on the OLT.

- 2** Sets the bridge priority of the OLT to 0.
- 3** Sets the Hello Time to 4, Maximum Age to 20 and Forward Delay to 15.
- 4** Enables STP on port 2 with a path cost of 150.
- 5** Sets the priority for port 2 to 20.

```
sysname(config)# spanning-tree
sysname(config)# spanning-tree priority 0
sysname(config)# spanning-tree hello-time 4 maximum-age 20 forward-delay
15
sysname(config)# spanning-tree eth-2 path-cost 150
sysname(config)# spanning-tree eth-2 priority 20
```

This example shows the current STP settings.

```
sysname# show spanning-tree config
Bridge Info:
(a)BridgeID: 8000-001349aefb7a
(b)TimeSinceTopoChange: 9
(c)TopoChangeCount: 0
(d)TopoChange: 0
(e)DesignatedRoot: 8000-001349aefb7a
(f)RootPathCost: 0
(g)RootPort: 0x0000
(h)MaxAge: 20 (seconds)
(i)HelloTime: 4 (seconds)
(j)ForwardDelay: 15 (seconds)
(k)BridgeMaxAge: 20 (seconds)
(l)BridgeHelloTime: 2 (seconds)
(m)BridgeForwardDelay: 15 (seconds)
(n)TransmissionLimit: 3
(o)ForceVersion: 2
```

The following table describes the labels in this display.

Table 207 show spanning-tree config

LABEL	DESCRIPTION
BridgeID	This field displays the unique identifier for this bridge, consisting of bridge priority plus MAC address.
TimeSinceTopoChange	This field displays the time since the spanning tree was last reconfigured.
TopoChangeCount	This field displays the number of times the spanning tree has been reconfigured.
TopoChange	This field indicates whether or not the current topology is stable. 0: The current topology is stable. 1: The current topology is changing.
DesignatedRoot	This field displays the unique identifier for the root bridge, consisting of bridge priority plus MAC address.
RootPathCost	This field displays the path cost from the root port on this OLT to the root switch.
RootPort	This field displays the priority and number of the port on the OLT through which this OLT must communicate with the root of the Spanning Tree.

Table 207 show spanning-tree config (continued)

LABEL	DESCRIPTION
MaxAge	This field displays the maximum time (in seconds) the root switch can wait without receiving a configuration message before attempting to reconfigure.
HelloTime	This field displays the time interval (in seconds) at which the root switch transmits a configuration message.
ForwardDelay	This field displays the time (in seconds) the root switch will wait before changing states (that is, listening to learning to forwarding).
BridgeMaxAge	This field displays the maximum time (in seconds) the OLT can wait without receiving a configuration message before attempting to reconfigure.
BridgeHelloTime	This field displays the time interval (in seconds) at which the OLT transmits a configuration message.
BridgeForwardDelay	This field displays the time (in seconds) the OLT will wait before changing states (that is, listening to learning to forwarding).
TransmissionLimit	This field displays the maximum number of BPDUs that can be transmitted in the interval specified by BridgeHelloTime .
ForceVersion	This field indicates whether BPDUs are RSTP (a value less than 3) or MSTP (a value greater than or equal to 3).

58.3 MSTP Commands

Use these commands to configure Multiple Spanning Tree Protocol (MSTP) as defined in IEEE 802.1s.

Table 208 MSTP Commands

COMMAND	DESCRIPTION	M	P
show mstp	Displays MSTP configuration for the OLT.	E	3
spanning-tree mode <RSTP MSTP>	Specifies the STP mode you want to implement on the OLT.	C	13
mstp	Activates MSTP on the OLT.	C	13
no mstp	Disables MSTP on the OLT.	C	13
mstp configuration-name <name>	Sets a name for an MSTP region. <i>name</i> : 1-32 printable characters	C	13
mstp revision <0-65535>	Sets the revision number for this MST Region configuration.	C	13
mstp hello-time <1-10> maximum-age <6-40> forward-delay <4-30>	Sets Hello Time, Maximum Age and Forward Delay. hello-time: The time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. maximum-age: The maximum time (in seconds) the OLT can wait without receiving a BPDU before attempting to reconfigure. forward-delay: The maximum time (in seconds) the OLT will wait before changing states.	C	13
mstp max-hop <1-255>	Sets the maximum hop value before BPDUs are discarded in the MST Region.	C	13

Table 208 MSTP Commands (continued)

COMMAND	DESCRIPTION	M	P
mstp interface port-channel <aid> edge-port	Sets the specified ports as edge ports. This allows the port to transition to a forwarding state immediately without having to go through the listening and learning states. Note: An edge port becomes a non-edge port as soon as it receives a Bridge Protocol Data Units (BPDU). <i>aid: eth-<port></i>	C	13
no mstp interface port-channel <aid> edge-port	Sets the listed ports as non-edge ports. <i>aid: eth-<port></i>	C	13

Table 209 MSTP Instance Commands

COMMAND	DESCRIPTION	M	P
show mstp instance <0-16>	Displays the specified MSTP instance configuration.	E	3
no mstp instance <0-16>	Disables the specified MST instance on the OLT.	C	13
mstp instance <0-16> priority <0-61440>	Specifies the bridge priority of the instance. <i>priority: Must be a multiple of 4096.</i>	C	13
mstp instance <0-16> vlan <vlan-list>	Specifies the VLANs that belongs to the instance.	C	13
no mstp instance <0-16> vlan <1-4094>	Disables the assignment of specific VLANs from an MST instance.	C	13
mstp instance <0-16> interface port-channel <aid>	Specifies the ports you want to participate in this MST instance. <i>aid: eth-<port></i>	C	13
no mstp instance <0-16> interface port-channel <aid>	Disables the assignment of specific ports from an MST instance. <i>aid: eth-<port></i>	C	13
mstp instance <0-16> interface port-channel <aid> path-cost <1-65535>	Specifies the cost of transmitting a frame to a LAN through the port(s). It is recommended you assign it according to the speed of the bridge. <i>aid: eth-<port></i>	C	13
mstp instance <0-16> interface port-channel <aid> priority <0-255>	Sets the priority for the specified ports. Priority decides which port should be disabled when more than one port forms a loop in a OLT. Ports with a higher priority numeric value are disabled first. <i>aid: eth-<port></i>	C	13

58.3.1 MSTP Command Examples

This example shows the current MSTP configuration.

```
sysname# show mstp
(a)BridgeMaxAge:          20      (seconds)
(b)BridgeHelloTime:        2       (seconds)
(c)BridgeForwardDelay:    15      (seconds)
(d)BridgeMaxHops:          128
(e)TransmissionLimit:     3
(f)ForceVersion:           3
(g)MST Configuration ID
  Format Selector:         0
  Configuration Name:     001349aefb7a
  Revision Number:          0
  Configuration Digest:   0xAC36177F50283CD4B83821D8AB26DE62
  msti          vlans mapped
  -----
  0            1-4094
  -----
```

The following table describes the labels in this display.

Table 210 show mstp

LABEL	DESCRIPTION
BridgeMaxAge	This field displays the maximum time (in seconds) the OLT can wait without receiving a configuration message before attempting to reconfigure.
BridgeHelloTime	This field displays the time interval (in seconds) at which the OLT transmits a configuration message.
BridgeForwardDelay	This field displays the time (in seconds) the OLT will wait before changing states (that is, listening to learning to forwarding).
BridgeMaxHops	This field displays the number of hops (in seconds) in an MSTP region before the BPDU is discarded and the port information is aged.
TransmissionLimit	This field displays the maximum number of BPDUs that can be transmitted in the interval specified by BridgeHelloTime .
ForceVersion	This field indicates whether BPDUs are RSTP (a value less than 3) or MSTP (a value greater than or equal to 3).
MST Configuration ID	
Format Selector	This field displays zero, which indicates the use of the fields below.
Configuration Name	This field displays the configuration name for this MST region.
Revision Number	This field displays the revision number for this MST region.
Configuration Digest	A configuration digest is generated from the VLAN-MSTI mapping information. This field displays the 16-octet signature that is included in an MSTP BPDU. This field displays the digest when MSTP is activated on the system.
msti	This field displays the MSTI ID.
vlans mapped	This field displays which VLANs are mapped to an MSTI.

This example shows the current CIST configuration (MSTP instance 0).

```
sysname# show mstp instance 0
Bridge Info: MSTID: 0
(a)BridgeID: 8000-001349aefb7a
(b)TimeSinceTopoChange: 756003
(c)TopoChangeCount: 0
(d)TopoChange: 0
(e)DesignatedRoot: 8000-001349aefb7a
(f)RootPathCost: 0
(g)RootPort: 0x0000
(h)RootMaxAge: 20 (seconds)
(i)RootHelloTime: 2 (seconds)
(j)RootForwardDelay: 15 (seconds)
(k)BridgeMaxAge: 20 (seconds)
(l)BridgeHelloTime: 2 (seconds)
(m)BridgeForwardDelay: 15 (seconds)
(n)ForceVersion: mstp
(o)TransmissionLimit: 3

(p)CIST_RRootID: 8000-001349aefb7a
(q)CIST_RRootPathCost: 0
```

The following table describes the labels in this display.

Table 211 show mstp instance

LABEL	DESCRIPTION
MSTID	This field displays the MSTI ID.
BridgeID	This field displays the unique identifier for this bridge, consisting of bridge priority plus MAC address.
TimeSinceTopoChange	This field displays the time since the spanning tree was last reconfigured.
TopoChangeCount	This field displays the number of times the spanning tree has been reconfigured.
TopoChange	This field indicates whether or not the current topology is stable. 0: The current topology is stable. 1: The current topology is changing.
DesignatedRoot	This field displays the unique identifier for the root bridge, consisting of bridge priority plus MAC address.
RootPathCost	This field displays the path cost from the root port on this OLT to the root switch.
RootPort	This field displays the priority and number of the port on the OLT through which this OLT must communicate with the root of the Spanning Tree.
RootMaxAge	This field displays the maximum time (in seconds) the root switch can wait without receiving a configuration message before attempting to reconfigure.
RootHelloTime	This field displays the time interval (in seconds) at which the root switch transmits a configuration message.
RootForwardDelay	This field displays the time (in seconds) the root switch will wait before changing states (that is, listening to learning to forwarding).
BridgeMaxAge	This field displays the maximum time (in seconds) the OLT can wait without receiving a configuration message before attempting to reconfigure.
BridgeHelloTime	This field displays the time interval (in seconds) at which the OLT transmits a configuration message.

Table 211 show mstp instance (continued)

LABEL	DESCRIPTION
BridgeForwardDelay	This field displays the time (in seconds) the OLT will wait before changing states (that is, listening to learning to forwarding).
ForceVersion	This field indicates whether BPDUs are RSTP (a value less than 3) or MSTP (a value greater than or equal to 3).
TransmissionLimit	This field displays the maximum number of BPDUs that can be transmitted in the interval specified by BridgeHelloTime .
CIST_RRootID	This field displays the unique identifier for the CIST regional root bridge, consisting of bridge priority plus MAC address.
CIST_RRootPathCost	This field displays the path cost from the root port on this OLT to the CIST regional root switch.

This example adds the OLT to the MST region **MSTRegionNorth**. **MSTRegionNorth** is on revision number 1. In **MSTRegionNorth**, VLAN 3 is in MST instance 1, and VLAN 4 is in MST instance 2.

```
sysname# configure
sysname(config)# mstp
sysname(config)# mstp configuration-name MSTRegionNorth
sysname(config)# mstp revision 1
sysname(config)# mstp instance 1 vlan 3
sysname(config)# mstp instance 2 vlan 4
sysname(config)# exit
```

CHAPTER 59

Bandwidth Control

This chapter shows you how you can cap the maximum bandwidth using the bandwidth control settings.

59.1 Bandwidth Control Commands

Bandwidth control means defining a maximum allowable bandwidth for out-going traffic flows on a port.

The following table describes the related commands.

Table 212 Bandwidth Control Commands

COMMAND	DESCRIPTION	M	P
bandwidth-control	Enables bandwidth control on the OLT.	C	13
no bandwidth-control	Disables bandwidth control on the OLT.	C	13
interface port-channel <aid>	Enters the sub-command mode for configuring the specified ports. aid: <pon eth>-<port>	C	13
bandwidth-limit cir <kbps>	Sets the ports' Committed Information Rate (CIR) bandwidth limit in Kbps.	C	13
bandwidth-limit cir <cr>	Enables the CIR bandwidth limit on the port.	C	13
no bandwidth-limit cir	Disables commit rate limits on the specified port(s).	C	13
bandwidth-limit egress	Enables bandwidth limits for outgoing traffic on the ports.	C	13
no bandwidth-limit egress	Disables egress bandwidth limits on the specified port(s).	C	13
bandwidth-limit egress <kbps>	Sets the maximum bandwidth allowed for outgoing traffic on the ports.	C	13
bandwidth-limit pir <kbps>	Sets the ports' Peak Information Rate (PIR) bandwidth limit in Kbps.	C	13
bandwidth-limit pir <cr>	Enables the PIR bandwidth limit on the ports.	C	13
no bandwidth-limit pir	Disables peak rate limits on the specified port(s).	C	13

Table 212 Bandwidth Control Commands (continued)

COMMAND	DESCRIPTION	M	P
<code>bandwidth-threshold egress <kbps></code>	Sets the interface's bandwidth rate threshold for outgoing traffic. The range of an XE port is from 0 to 10000000 Kbps. The range of a GPON port is from 0 to 2500000 Kbps. The range of a GE port is from 0 to 1000000 Kbps.	C	13
<code>bandwidth-threshold ingress <kbps></code>	Sets the interface's bandwidth rate threshold for incoming traffic. The range of an XE port is from 0 to 10000000 Kbps. The range of a GPON port is from 0 to 2500000 Kbps. The range of a GE port is from 0 to 1000000 Kbps.	C	13
<code>no bandwidth-threshold egress</code>	Removes the interface's bandwidth rate threshold for outgoing traffic.	C	13
<code>no bandwidth-threshold ingress</code>	Removes the interface's bandwidth rate threshold for incoming traffic.	C	13
<code>show interfaces config <aid> bandwidth-threshold</code>	Displays the bandwidth control configuration for the specified port. <i>aid: <pon eth>-<port></i>	E	13
<code>show interfaces config <aid> bandwidth-control</code>	Displays the current settings for bandwidth control on the specified ports. <i>aid: <pon eth>-<port></i>	E	3

CHAPTER 60

MTU

Use these commands to configure the Maximum Transmission Unit (MTU) on specific interfaces.

60.1 MTU Commands

This table describes the commands.

Table 213 MTU Commands

COMMAND	DESCRIPTION	M	P
interface port-channel <aid>	Enters the sub-command mode for configuring the specified ports. <i>aid: <pon eth>-<port></i>	C	13
max-frame-size <frame-size>	Configures the interface's maximum frame size for IP packets. <i>frame-size: 64-2590 bytes (2590 is the default value.)</i>	C	13
no max-frame-size	Sets the interface's maximum frame size for IP packets to the default value of 9216 bytes.	C	13
exit	Leaves the interface configuration sub-command mode.	C	13
show interfaces config <aid> max-frame-size	Displays the specified port's maximum frame size setting. <i>aid: <pon eth>-<port></i>	E	13

CHAPTER 61

Broadcast Storm Control

Use these commands to configure broadcast storm control on the OLT.

61.1 Broadcast Storm Control Overview

Broadcast storm control limits the number of broadcast, multicast and destination lookup failure (DLF) packets the OLT receives per second on the ports. When the maximum number of allowable broadcast, multicast and/or DLF packets is reached per second, the subsequent packets are discarded. Enable this feature to reduce broadcast, multicast and/or DLF packets in your network. You can specify limits for each packet type on each port.

61.2 Broadcast Storm Control Commands

The following table describes the related commands.

Table 214 Broadcast Storm Control Commands

COMMAND	DESCRIPTION	M	P
storm-control	Enables traffic storm control on the OLT.	C	13
no storm-control	Disables traffic storm control on the OLT.	C	13
show interfaces config <aid> bstorm-control	Displays the storm control status on the specified port. <i>aid: <pon eth>-<port></i>	E	3
interface port-channel <aid>	Enters the sub-command mode for configuring the specified ports. <i>aid: <pon eth>-<port></i>	C	13
broadcast-limit	Enables broadcast limits on the port.	C	13
no broadcast-limit	Disables broadcast limits on the port.	C	13
broadcast-limit <pkt/s>	Sets the number of broadcast packets the port receives per second.	C	13
multicast-limit	Enables multicast limits on the port.	C	13
multicast-limit <pkt/s>	Sets the number of multicast packets the port receives per second.	C	13
no multicast-limit	Disables multicast packet limit on the specified port(s).	C	13
dlf-limit	Enables DLF limits on the port.	C	13

Table 214 Broadcast Storm Control Commands (continued)

COMMAND	DESCRIPTION	M	P
dlf-limit <pkt/s>	Sets the number of DLF packets the port receives per second.	C	13
no dlf-limit	Clears the number of DLF packets the port receives per second.	C	13

61.3 Broadcast Storm Control Examples

Enable broadcast storm control on the OLT.

```
sysname# configure
sysname(config)# storm-control
```

Disable broadcast storm control on the OLT.

```
sysname(config)# no storm-control
```

Set broadcast storm control on a port (**PON1**) which is active, to limit its broadcast type traffic with a threshold of 999 packets per second.

```
sysname(config)# interface port-channel pon-1
sysname(config-interface)# broadcast-limit
sysname(config-interface)# broadcast-limit 999
```

Display storm control status and settings. This example displays the settings for **PON1** to **PON4**.

```
sysname# show interfaces config pon-1&&-4 bstorm-control
Broadcast Storm Control Enabled: Yes

Port      Broadcast|Enabled      Multicast|Enabled      DLF-Limit|Enabled
pon-1     999 pkt/s|No          10 pkt/s|No          10 pkt/s|No
pon-2     10 pkt/s|No           10 pkt/s|No          10 pkt/s|No
pon-3     10 pkt/s|No           10 pkt/s|No          10 pkt/s|No
pon-4     10 pkt/s|No           10 pkt/s|No          10 pkt/s|No
```

Table 215 Broadcast Storm Control Port Status

LABEL	DESCRIPTION
Port	This field displays a port number.
Broadcast Enabled	How many broadcast packets the port receives per second and the enable state for broadcast packets.

Table 215 Broadcast Storm Control Port Status (continued)

LABEL	DESCRIPTION
Multicast Enabled	How many multicast packets the port receives per second and the enable state for multicast packets.
DLF-Limit Enabled	How many DLF packets the port receives per second and the enable state for DFL packets.

CHAPTER 62

Port Mirroring

This chapter discusses port mirroring setup.

62.1 Port Mirroring Overview

Port mirroring allows you to copy a traffic flow to a monitor port (the port you copy the traffic to) in order that you can examine the traffic from the monitor port without interference.

Use these commands to copy a traffic flow for one or more ports to a monitor port (the port you copy the traffic to) so that you can examine the traffic on the monitor port without interference.

Note: Use the running configuration commands to look at the current mirror settings. See [Chapter 84 on page 572](#).

62.2 Port Mirroring Commands

The following section lists the commands for this feature.

Table 216 Port Mirroring Commands

COMMAND	DESCRIPTION	M	P
<code>mirror-port</code>	Enables port mirroring on the OLT.	C	13
<code>mirror-port <aid></code>	Specifies the monitor port (the port to which traffic flow is copied) for port mirroring. <i>aid</i> : <pon eth>-<port>	C	13
<code>no mirror-port</code>	Disables port mirroring on the OLT.	C	13
<code>show mirror</code>	Displays mirror settings of the OLT.	E	3
<code>mirror-port vlan <vid all></code>	Sets the mirrored VLAN of the monitored port. <i>vid</i> : 1~4094 <i>all</i> : all VLANs	C	13
<code>interface port-channel <aid></code>	Enters config-interface mode for the specified port(s). <i>aid</i> : <pon eth>-<port>	C	13
<code>mirror</code>	Enables port mirroring in the interface.	C	13

Table 216 Port Mirroring Commands (continued)

COMMAND	DESCRIPTION	M	P
mirror dir <ingress egress both>	Enables port mirroring for incoming (ingress), outgoing (egress) or both incoming and outgoing (both) traffic.	C	13
no mirror	Disables port mirroring on the port(s).	C	13

62.3 Port Mirroring Command Examples

This example enables port mirroring and copies outgoing traffic from port 4 to port 1..

```
sysname(config)# mirror-port
sysname(config)# mirror-port eth-1
sysname(config)# interface port-channel eth-4
sysname(config-interface)# mirror
sysname(config-interface)# mirror dir egress
```

This example displays the mirror settings of the OLT after you configured in the example above.

```
sysname# show mirror

    Mirroring: enable
    Monitor port: eth-1
        Vlan: All

    Mirrored port: eth-3
        Ingress: eth-3
        Egress:
            Both:
```

CHAPTER 63

Link Aggregation

This chapter shows you how to logically aggregate physical links to form one logical, higher-bandwidth link.

63.1 Link Aggregation Overview

Link aggregation (Trunking) is the grouping of physical ports into one logical higher-capacity link. You may want to trunk ports if for example, it is cheaper to use multiple lower-speed links than to under-utilize a high-speed, but more costly, single-port link.

However, the more ports you aggregate then the fewer available ports you have. A trunk group is one logical link containing multiple ports.

The beginning port of each trunk group must be physically connected to form a trunk group.

The OLT supports both static and dynamic link aggregation.

Note: In a properly planned network, it is recommended to implement static link aggregation only. This ensures increased network stability and control over the trunk groups on your OLT.

See [Section 63.4 on page 448](#) for a static port trunking example.

63.2 Dynamic Link Aggregation

The OLT adheres to the IEEE 802.3ad standard for static and dynamic (LACP) port trunking.

The OLT supports the link aggregation IEEE802.3ad standard. This standard describes the Link Aggregation Control Protocol (LACP), which is a protocol that dynamically creates and manages trunk groups.

When you enable LACP link aggregation on a port, the port can automatically negotiate with the ports at the remote end of a link to establish trunk groups. LACP also allows port redundancy, that is, if an operational port fails, then one of the “standby” ports become operational without user intervention. Please note that:

- You must connect all ports point-to-point to the same Ethernet switch and configure the ports for LACP trunking.
- LACP only works on full-duplex links.

- All ports in the same trunk group must have the same media type, speed, duplex mode and flow control settings.

Configure trunk groups or LACP before you connect the Ethernet switch to avoid causing network topology loops.

63.2.1 Link Aggregation ID

LACP aggregation ID consists of the following information³:

Table 217 Link Aggregation ID: Local Switch

SYSTEM PRIORITY	MAC ADDRESS	KEY	PORT PRIORITY	PORT NUMBER
0000	00-00-00-00-00-00	0000	00	0000

Table 218 Link Aggregation ID: Peer Switch

SYSTEM PRIORITY	MAC ADDRESS	KEY	PORT PRIORITY	PORT NUMBER
0000	00-00-00-00-00-00	0000	00	0000

63.3 Link Aggregation Commands

The following table describes the related commands.

Table 219 Trunk Commands

COMMAND	DESCRIPTION	M	P
show trunk	Displays link aggregation information.	E	3
trunk <T1 T2 T3 T4 T5 T6 T7 T8 T9 T10 T11 T12>	Activates a trunk group.	C	13
no trunk <T1 T2 T3 T4 T5 T6 T7 T8 T9 T10 T11 T12>	Disables the specified trunk group.	C	13
trunk <T1 T2 T3 T4 T5 T6 T7 T8 T9 T10 T11 T12> criteria <src-mac dst-mac src-dst-mac src-ip dst-ip src-dst-ip>	Sets the traffic distribution type used for the specified trunk group.	C	13
no trunk <T1 T2 T3 T4 T5 T6 T7 T8 T9 T10 T11 T12> criteria	Returns the traffic distribution type used for the specified trunk group to the default (src-dst-mac).	C	13
trunk <T1 T2 T3 T4 T5 T6 T7 T8 T9 T10 T11 T12> interface <aid>	Adds a port(s) to the specified trunk group. <i>aid: eth-<port></i>	C	13
no trunk <T1 T2 T3 T4 T5 T6 T7 T8 T9 T10 T11 T12> interface <aid>	Removes ports from the specified trunk group. <i>aid: eth-<port></i>	C	13
trunk <T1 T2 T3 T4 T5 T6 T7 T8 T9 T10 T11 T12> lacp	Enables LACP for a trunk group.	C	13

3. Port Priority and Port Number are 0 as it is the aggregator ID for the trunk group, not the individual port.

Table 219 Trunk Commands (continued)

COMMAND	DESCRIPTION	M	P
no trunk <T1 T2 T3 T4 T5 T6 T7 T8 T9 T10 T11 T12> lacp	Disables LACP in the specified trunk group.	C	13
trunk interface <aid> timeout <lACP-timeout>	Defines LACP timeout period (in seconds) for the specified port(s). aid: eth-<port> lACP-timeout: 1 or 30	C	13

Table 220 LACP Commands

COMMAND	DESCRIPTION	M	P
show lacp	Displays LACP (Link Aggregation Control Protocol) settings.	E	3
lacp	Enables Link Aggregation Control Protocol (LACP).	C	13
no lacp	Disables the link aggregation control protocol (Dynamic trunking) on the OLT.	C	13
lacp system-priority <1-65535>	Sets the priority of an active port using LACP.	C	13

63.4 Link Aggregation Commands Examples

This example activates trunk 1 and places port 1 to port 2 in the trunk using static link aggregation.

```
sysname(config)# trunk T1
sysname(config)# trunk T1 interface eth-1&&-2
```

This example disables trunk one (T1) and removes port 3 to port 4 from trunk two (T2).

```
sysname(config)# no trunk T1
sysname(config)# no trunk T2 interface eth-3&&-4
```

This example displays the current trunks.

```
sysname# show trunk
Group ID T1:    inactive
Criteria : src-dst-mac
Status: -
Member number: 0
Group ID T2:    inactive
Criteria : src-dst-mac
Status: -
Member number: 0
```

The following table describes the labels.

Table 221 Show Trunk Labels

LABEL	DESCRIPTION
Group ID	This field displays the trunk ID number and the current status. inactive: This trunk is disabled. active: This trunk is enabled.
Criteria	This shows the outgoing traffic distribution algorithm used in this trunk group. Packets from the same source and/or to the same destination are sent over the same link within the trunk. src-mac means the OLT distributes traffic based on the packet's source MAC address. dst-mac means the OLT distributes traffic based on the packet's destination MAC address. src-dst-mac means the OLT distributes traffic based on a combination of the packet's source and destination MAC addresses. src-ip means the OLT distributes traffic based on the packet's source IP address. dst-ip means the OLT distributes traffic based on the packet's destination IP address. src-dst-ip means the OLT distributes traffic based on a combination of the packet's source and destination IP addresses.
Status	This field displays how the ports were added to the trunk. -: The trunk is disabled. Static: The ports are static members of the trunk. LACP: The ports joined the trunk via LACP.
Member Number	This field shows the number of ports in the trunk.
Member	This field is displayed if there are ports in the trunk. This field displays the member port(s) in the trunk.

This example displays the current LACP settings.

```
sysname# show lacp
AGGREGATOR INFO:
ID: 1
[(0000,00-00-00-00-00-00,0000,00,0000)][(0000,00-00-00-00-00,0000,00,0000)]
LINKS :
SYNCS :

ID: 2
[(0000,00-00-00-00-00-00,0000,00,0000)][(0000,00-00-00-00-00,0000,00,0000)]
LINKS :
SYNCS :
```

The following table describes the labels.

Table 222 Show LACP Labels

LABEL	DESCRIPTION
ID	This field displays the trunk ID to identify a trunk group, that is, one logical link containing multiple ports.
[(0000,00-00-00-00-00,00,0000,00,0000)]	This field displays the system priority, MAC address, key, port priority, and port number.
LINKS	This field displays the ports whose link state are up.
SYNCS	These are the ports that are currently transmitting data as one logical link in this trunk group.

CHAPTER 64

RADIUS

This chapter describes the external RADIUS (Remote Authentication Dial-In User Service) servers configuration methods.

64.1 RADIUS Commands

Use these commands to configure external RADIUS (Remote Authentication Dial-In User Service) servers.

Table 223 RADIUS Server Commands

COMMAND	DESCRIPTION	M	P
<code>show radius-server</code>	Displays RADIUS server settings.	E	3
<code>radius-server host <index> <ip></code>	Specifies the IP address of the RADIUS authentication server.	C	14
<code>radius-server host <index> <ip> [auth-port <socket-number>] [key <key-string>]</code>	Specifies the IP address of the RADIUS authentication server. Optionally, sets the UDP port number and shared secret. <i>index</i> : 1 or 2. <i>key-string</i> : 1-32 alphanumeric characters.	C	14
<code>radius-server mode <index-priority round-robin></code>	Specifies how the OLT decides which RADIUS server to select if you configure multiple servers. <i>index-priority</i> : The OLT tries to authenticate with the first configured RADIUS server. If the RADIUS server does not respond, then the OLT tries to authenticate with the second RADIUS server. <i>round-robin</i> : The OLT alternates between RADIUS servers that it sends authentication requests to.	C	14
<code>radius-server timeout <1-1000></code>	Specifies the amount of time (in seconds) that the OLT waits for an authentication request response from the RADIUS server. In <i>index-priority</i> mode, the timeout is divided by the number of servers you configure. For example, if you configure two servers and the timeout is 30 seconds, then the OLT waits 15 seconds for a response from each server.	C	14
<code>no radius-server <index></code>	Resets the specified RADIUS server to its default values.	C	14
<code>show radius-accounting</code>	Displays the RADIUS accounting settings.	E	3

Table 223 RADIUS Server Commands (continued)

COMMAND	DESCRIPTION	M	P
<code>radius-accounting host <index> <ip></code>	Specifies the IP address of a RADIUS accounting host. <i>index</i> : 1 or 2.	C	13
<code>radius-accounting host <index> <ip> [acct-port <socket-number>] [key <key-string>]</code>	Set s the RADIUS accounting host's optional settings. <i>index</i> : 1 or 2. acct-port <socket-number>, key <key-string>: Optional commands	C	13
<code>radius-accounting timeout <1-1000></code>	Sets the RADIUS accounting server's timeout setting.	C	13
<code>no radius-accounting <index></code>	Removes the specific index of the RADIUS accounting server. <i>index</i> : 1 or 2.	C	13

64.2 RADIUS Command Examples

This example sets up one primary RADIUS server (172.16.10.10) and one secondary RADIUS server (172.16.10.11). The secondary RADIUS server is also the accounting server.

```
sysname# configure
sysname(config)# radius-server mode index-priority
sysname(config)# radius-server host 1 172.16.10.10
sysname(config)# radius-server host 2 172.16.10.11
sysname(config)# radius-accounting host 1 172.16.10.11
sysname(config)# exit
```

CHAPTER 65

Port Security

This chapter shows you how to set up port security.

65.1 Port Security Overview

Port security allows only packets with dynamically learned MAC addresses and/or configured static MAC addresses to pass through a port on the OLT. The OLT can learn up to 32K MAC addresses in total with no limit on individual ports other than the sum cannot exceed 32K.

For maximum port security, enable this feature, disable MAC address learning and configure static MAC address(es) for a port. It is not recommended you disable port security together with MAC address learning as this will result in many broadcasts. By default, MAC address learning is still enabled even though port security is not activated.

With port-security enabled on the OLT, each subscriber port counts the number of newly learnt MAC addresses. Configure the number of MAC addresses a specific port can learn and the OLT drops Source Lookup Failure (SLF) packets on the port that exceed the limit.

Anti-MAC spoofing lets you set whether or not to allow a subscriber device to move between OLT subscriber ports. This means the OLT has learned a subscriber device's source MAC address at one port but receives packets containing the same source MAC address through another subscriber port before the learned MAC address times out from the MAC address table. Disable anti-MAC spoofing to have the OLT allow the port move and learn the source MAC address on the new port. Enable anti-MAC spoofing to have the OLT drop the packets and not learn the source MAC address on the new port. Anti-MAC spoofing applies to the subscriber ports, not the uplink ports.

65.2 Port Security Commands

The following table lists the port security commands.

Table 224 Port Security Commands

COMMAND	DESCRIPTION	M	P
port-security	Enables the port security feature.	C	13
port-security <aid>	Enables port security on the specified port. aid: <pon eth>-<port>	C	13
no port-security	Disables the port security feature.	C	13

Table 224 Port Security Commands (continued)

COMMAND	DESCRIPTION	M	P
no port-security <aid>	Disables port security on the specified port. aid: <pon eth>-<port>	C	13
port-security <aid> address-limit <number>	Limits the number of (dynamic) MAC addresses that may be learned on the specified ports. aid: <pon eth>-<port> number: PON port: 0-1023 Ethernet port: 0-8191	C	13
port-security <aid> learn inactive	Disables MAC address learning for the specified port. aid: <pon eth>-<port>	C	13
no port-security <aid> learn inactive	Enables MAC address learning for specified port. aid: <pon eth>-<port>	C	13
port-security <aid> MAC-freeze	Adds learned MAC addresses to the static table and stops the specified port from learning new MAC addresses. aid: <pon eth>-<port>	C	13
show port-security	Displays the port security settings.	E	3
show port-security <aid>	Displays the port security settings of a specified OLT, MSC, or GE port. aid: <pon eth>-<port>	E	3
show privilege	Displays the current privilege level. It shows the current login level privilege or the privilege changed via an enable command for the current CLI session.	E	0

65.3 Port Security Command Examples

Activate port-security on the OLT and on **PON1**. Then limit the number of (dynamic) MAC addresses subscriber port **PON1** can learn to 100.

```
sysname#config
sysname(config)# port-security
sysname(config)# port-security pon-1
sysname(config)# port-security pon-1 address-limit 100
```

Activate learning mode on **PON1**.

```
sysname#config
sysname(config)# no port-security pon-1 learn inactive
```

Display the port security settings.

Port	Active	Address Learning	Limited Number of Learned MAC Address
pon-1	Y	Y	100
pon-2	N	Y	0
pon-3	N	Y	0
pon-4	N	Y	0
eth-1	N	Y	0
eth-2	N	Y	0
eth-3	N	Y	0
eth-4	N	Y	0
eth-5	N	Y	0
eth-6	N	Y	0
eth-7	N	Y	0
eth-8	N	Y	0
eth-9	N	Y	0
eth-10	N	Y	0
eth-11	N	Y	0
eth-12	N	Y	0
eth-13	N	Y	0
eth-14	N	Y	0
eth-15	N	Y	0
eth-16	N	Y	0
eth-17	N	Y	0
eth-18	N	Y	0
eth-19	N	Y	0
eth-20	N	Y	0

CHAPTER 66

Classifier

This chapter introduces and shows you how to configure the packet classifier on the OLT.

66.1 Classifier and QoS Overview

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 time-critical application such as video-on-demand.

A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming port number. For example, you can configure a classifier to select traffic from the same protocol port (Such as Telnet) to form a flow.

Configure QoS on the OLT to group and prioritize application traffic and fine-tune network performance. Setting up QoS involves two separate steps:

- 1 Configure classifiers to sort traffic into different flows.
- 2 Configure policy rules to define actions to be performed for a classified traffic flow (Refer to [Chapter 68 on page 466](#) to configure policy rules).

66.2 QoS Commands

Use these commands to configure QoS settings.

Table 225 QoS Commands

COMMAND	DESCRIPTION	M	P																				
<code>qos bwprof <bwprofName> ustype <0 ~ 5>[sir<value>][air<value>][pir<value>]</code>	<p>Sets the QoS upstream/downstream bandwidth profile.</p> <p><i>bwprofName</i>: The QoS upstream/downstream bandwidth profile name</p> <p><i>ustype <0 ~ 5></i>: Specify the upstream bandwidth group type the profile uses.</p> <p>See bandwidth group types and how their bandwidth is controlled by SIR, AIR, and PIR parameters respectively in the following figure.</p> <p>Figure 228 ONT Templates</p> <table border="1"> <tr> <td>Type 1</td><td>Type 2</td><td>Type 3</td><td>Type 4</td><td>Type 5</td></tr> <tr> <td>sir > 0</td><td>sir = 0</td><td>sir = 0</td><td>sir = 0</td><td>sir > 0</td></tr> <tr> <td>air = 0</td><td>air > 0</td><td>air > 0</td><td>air = 0</td><td>air > 0</td></tr> <tr> <td>pir = sir</td><td>pir = air</td><td>pir > air</td><td>pir > 0</td><td>pir >= sir + air</td></tr> </table> <p><i>sir<value>, air<value>, pir<value></i>: Sets the SIR, AIR, and PIR values (in Kbps).</p>	Type 1	Type 2	Type 3	Type 4	Type 5	sir > 0	sir = 0	sir = 0	sir = 0	sir > 0	air = 0	air > 0	air > 0	air = 0	air > 0	pir = sir	pir = air	pir > air	pir > 0	pir >= sir + air	C	13
Type 1	Type 2	Type 3	Type 4	Type 5																			
sir > 0	sir = 0	sir = 0	sir = 0	sir > 0																			
air = 0	air > 0	air > 0	air = 0	air > 0																			
pir = sir	pir = air	pir > air	pir > 0	pir >= sir + air																			
<code>qos bwprof help</code>	Displays more information about the QoS bandwidth profile.	C	13																				
<code>no qos bwprof <name> <cr></code>	Removes the specified QoS bandwidth profile.	C	13																				
<code>no qos bwprof all</code>	Removes all QoS bandwidth profiles.	C	13																				
<code>qos ds-meter macro-mode <pir cir></code>	<p>Sets the downstream macro meter rate limit sharing mode.</p> <p><i>pir</i>: the micro meter's Peak Information Rate (PIR) takes bandwidth first.</p> <p><i>cir</i>: the micro meter's Committed Information Rate (CIR) takes bandwidth first.</p>	C	13																				
<code>qos ingprof <ingprofName> [DOT1P0TC<value>],...</code>	<p>Configures a QoS ingress profile to map IEEE 802.1p priority tags to traffic classes.</p> <p><i>ingprofName</i>: The QoS ingress profile name</p> <p><i>DOT1P0TC<value></i>: Sets the traffic class mapping to priority</p>	C	13																				
<code>qos ingprof help</code>	Displays more information about the QoS ingress profile.	C	13																				
<code>no qos ingprof <name> <cr></code>	Removes the specified QoS ingress profile.	C	13																				
<code>no qos ingprof all</code>	Removes all QoS ingress profiles.	C	13																				

Table 225 QoS Commands (continued)

COMMAND	DESCRIPTION	M	P
<code>qos pbitprof <pbitprofName> [p0to<value>],...</code>	Sets the QoS priority bit translation profile. <i>pbitprofName</i> : The QoS priority bit translation profile name <i>p0to<value></i> : Sets the priority bit translation (0–7)	C	13
<code>qos pbitprof help</code>	Displays more information about the QoS priority bit profile.	C	13
<code>no qos pbitprof <name> <cr></code>	Removes the specified QoS priority bit profile.	C	13
<code>no qos pbitprof all</code>	Removes all QoS priority bit profiles.	C	13
<code>qos wred</code>	Enables Weighted Random Early Detection (WRED) on the QoS. Use WRED to help avoid traffic congestion. See Chapter 89 on page 608 for more information on WRED.	C	13
<code>interface port-channel <aid></code>	Enters config-interface mode for the specified port(s). <i>aid</i> : <pon eth>-<port>	C	13
<code>hybrid-spq lowest-queue <q0 q1 ... q7></code>	Enables SPQ starting with the specified queue and subsequent higher queues on the ports.	C	13
<code>no hybrid-spq</code>	Disables SPQ starting with the specified queue and subsequent higher queues on the ports.	C	13
<code>qos priority <0-7></code>	Sets the specified interface's QoS priority.	C	13
<code>exit</code>	Leaves the interface configuration sub-command mode.	C	13

66.2.1 Show QoS Commands

Use these commands to display different types of QoS profile settings.

Table 226 Show QoS Commands

COMMAND	DESCRIPTION	M	P
<code>sh qos Bwprof</code>	Displays the QoS bandwidth profile settings.	E	13
<code>sh qos ds-meter</code>	Displays the QoS downstream meter settings.	E	3
<code>sh qos ingprof</code>	Displays the QoS ingress profile settings.	E	13
<code>sh qos pbitprof</code>	Displays the QoS priority bit profile settings.	E	13
<code>sh qos wred</code>	Displays the QoS Weighted Random Early Detection (WRED) settings. Use WRED to help avoid traffic congestion. See Chapter 89 on page 608 for more information on WRED.	E	3

66.3 Classifier Commands

Use these commands to classify packets into traffic flows. After classifying traffic, policy commands ([Chapter 68 on page 466](#)) can be used to ensure that a traffic flow gets the requested treatment in the network.

Table 227 Classifier Commands

COMMAND	DESCRIPTION	M	P
show classifier	Displays all classifier related information.	E	3
show classifier [<name>]	Displays the specified classifier related information.	E	3
classifier <name> [<packet-format <EtherIIuntag EtherIITag>] [priority <0-7>] [<vlan-id>] [ethernet-type <ether-num> ip ipx arp rarp appletalk decn et ipv6>] [<source-mac <src-mac-addr>>][<source-port <port-num>>][<destination-port <port-num>>] [<destination-mac <dest-mac-addr>>] [dscp <0-63>] [<ipv6-dscp <0-63>>] [<ip-protocol <protocol-num>> tcp udp icmp egp ospf rsvp igmp igp pim ipsec] [<establish-only>]] [<ipv6-next-header <protocol-num>> tcp udp icmv6] [<establish-only>]] [<source-ip <src-ip-addr>>][<mask-bits <mask-bits>>]] [<ipv6-source-ip <src-ipv6-addr>>][<prefix-length <prefix-length>>]] [<source-socket <socket-num>>][<destination-ip <dest-ip-addr>>][<mask-bits <mask-bits>>]] [<ipv6-destination-ip <dest-ipv6-addr>>][<prefix-length <prefix-length>>]] [<destination-socket <socket-num>>]	C	13	
classifier help	Provides more information about the specified command.	C	13
classifier <name> inactive	Disables a classifier.	C	13
no classifier <name>	Deletes the classifier. If you delete a classifier you cannot use policy rule related information.	C	13
no classifier <name> inactive	Enables a classifier.	C	13

The following table shows some other common Ethernet types and the corresponding protocol number.

Table 228 Common Ethernet Types and Protocol Number

ETHERNET TYPE	PROTOCOL NUMBER
IP ETHII	0800
X.75 Internet	0801

Table 228 Common Ethernet Types and Protocol Number

ETHERNET TYPE	PROTOCOL NUMBER
NBS Internet	0802
ECMA Internet	0803
Chaosnet	0804
X.25 Level 3	0805
XNS Compat	0807
Banyan Systems	0BAD
BBN Simnet	5208
IBM SNA	80D5
AppleTalk AARP	80F3

In an IPv4 packet header, the "Protocol" field identifies the next level protocol. The following table shows some common IPv4 protocol types and the corresponding protocol number. Refer to <http://www.iana.org/assignments/protocol-numbers> for a complete list.

Table 229 Common IPv4 Protocol Types and Protocol Numbers

PROTOCOL TYPE	PROTOCOL NUMBER
ICMP	1
TCP	6
UDP	17
EGP	8
L2TP	115

In an IPv6 packet header, the "Next Header" field identifies the next level protocol. The following table shows some common IPv6 Next Header values.

Table 230 Common IPv6 Next Header Values

PROTOCOL TYPE	VALUE
IPv6 Hop-by-Hop Option	0
IPv4	4
TCP	6
UDP	17
IPv6	41
Routing Header for IPv6	43
Fragment Header for IPv6	44
Encapsulation Security Payload	50
Authentication Header	51
ICMP for IPv6	58
No Next Header for IPv6	59
Destination Options for IPv6	60

66.4 Classifier Command Examples

This example creates a classifier for packets with a VLAN ID of 3. The resulting traffic flow is identified by the name **VLAN3**. The **policy** command can use the name **VLAN3** to apply policy rules to this traffic flow. See the policy example in [Section 68.3 on page 468](#).

```
sysname# config
sysname(config)# classifier VLAN3 vlan 3
sysname(config)# exit
sysname# show classifier
Index Active Name                               Rule
      1 Yes     VLAN3                         VLAN = 3;
```

CHAPTER 67

RMON

67.1 RMON Overview

Similar to SNMP, RMON (Remote Network Monitor) allows you to gather and monitor network traffic.

Both SNMP and RMON use an agent, known as a probe, which are software processes running on network devices to collect information about network traffic and store it in a local MIB (Management Information Base). With SNMP, a network manager has to constantly poll the agent to obtain MIB information. The probe on the OLT communicates with the network manager via SNMP.

RMON groups contain detailed information about specific activities. The following table describes the four RMON groups that your OLT supports.

Table 231 Supported RMON Groups

GROUP	DESCRIPTION
Statistics	Records current network traffic information on a specified Ethernet port.
History	Records historical network traffic information on a specified Ethernet port for a certain time period.
Alarm	Provides alerts when configured alarm conditions are met.
Event	Defines event generation and resulting actions to be taken based on an alarm.

67.2 RMON Commands

The following section lists the commands for this feature.

Table 232 RMON Commands

COMMAND	DESCRIPTION	M	P
<pre>rmon alarm alarmtable <1-65535> variable <variable> interval <integer> sample-type <absolute delta> startup-alarm <startup-alarm> rising-threshold <integer> <0-65535> falling- threshold <integer> <0-65535> [owner <string>]</pre>	<p>Sets an alarm that occurs when the sampled data exceeds the specified threshold.</p> <p>1-65535: An alarm's index number in the alarm table.</p> <p>variable: The variable(s) whose data is sampled.</p> <p>variable <variable>: The time interval (in seconds) between data samplings.</p> <p>interval <integer>: This is the time interval (in seconds) between data samplings. 1~3600.</p> <p>sample-type <absolute delta>: The method of obtaining the sample value and calculating the value to be compared against the thresholds.</p> <ul style="list-style-type: none"> • absolute: the sampling value of the selected variable will be compared directly with the thresholds. • delta: the last sampling value of the selected variable will be subtracted from the current sampling value first. Then use the difference to compare with the thresholds. <p>startup-alarm <startup-alarm>: Specifies when the OLT should generate an alarm regarding to the rising and/or falling thresholds.</p> <ul style="list-style-type: none"> • rising: the OLT generates an alarm if the sampling value (or calculated value) is greater than or equal to the rising threshold. • falling: the OLT generates an alarm if the sampling value (or calculated value) is less than or equal to the falling threshold. • risingOrFalling: the OLT generates an alarm either when the sampling value (or calculated value) is greater than or equal to the rising threshold or when the sampling value (or calculated value) is less than or equal to the falling threshold. <p>rising-threshold <integer>: Specify an integer for the rising threshold. When a value is greater or equal to this threshold, the OLT generates an alarm.</p>	C	13

Table 232 RMON Commands (continued)

COMMAND	DESCRIPTION	M	P
	<p>0–65535: Specify an event's index number (0–65535). The OLT will take the corresponding action of the selected event for the rising alarm. Set this to 0 if you do not want to take any action for the alarm.</p> <p>falling-threshold <integer>: Specify an integer for the falling threshold. When a value is smaller or equal to this threshold, the OLT generates an alarm.</p> <p>0–65535: Specify an event's index number (0–65535). The OLT will take the corresponding action of the selected event for the falling alarm. Set this to 0 if you do not want to take any action for the alarm.</p> <p>owner <string>: Specify who should handle this alarm.</p>	C	13
rmon event eventtable <1-65535> [description<string>]	<p>Sets the RMON event table.</p> <p>eventtable <1-65535>: The event's index number in the event table (1–65535).</p> <p>description<string>: owner log trap description</p>	C	13
rmon event eventtable help	Provides more information about the specified command.	C	13
rmon history historycontrol <1-65535> buckets <1-65535> interval <1-3600> port-channel <aid> [owner <string>]	<p>Sets RMON history configuration settings.</p> <p>buckets <1-65535>: The number of data samplings the network manager requests the OLT to store.</p> <p>interval <1-3600>: The time in seconds between data samplings.</p> <p>aid: pon-<port> The port that the OLT will poll for data.</p> <p>owner <string>: Specify who should handle these historical network traffic statistics.</p>	C	13
rmon statistics etherstats <1-65535> port-channel <aid> [owner <string>]	<p>Sets to collect network traffic on the specified port since the last time the OLT was reset.</p> <p>1-65535: The entry's index number in the Ethernet statistics table.</p> <p>aid: pon-<port> The port that the OLT will poll for data.</p> <p>owner <string>: Specify who should handle these Ethernet statistics.</p>	C	13
rmon alarm alarmtable	Provides more information about the specified command.	C	13
no rmon alarm alarmtable <1-65535>	Removes the specified RMON alarm's settings.	C	13
no rmon event eventtable <1-65535>	Removes the RMON event table settings of the specified event.	C	13

Table 232 RMON Commands (continued)

COMMAND	DESCRIPTION	M	P
no rmon history historycontrol <1-65535>	Removes the historical network traffic statistics table settings for the specified event.	C	13
no rmon statistics etherstats <1-65535>	Stops collecting network traffic for the specified event.	C	13
show rmon alarm alarmtable	Displays all RMON alarm settings.	E	3
show rmon alarm alarmtable <1-65535>	Displays the specified RMON alarm settings.	E	3
show rmon event eventtable	Displays all of the RMON event table settings.	E	3
show rmon event eventtable <1-65535>	Displays the specified RMON event table settings.	E	3
show rmon history historycontrol	Displays all historical network traffic statistics table settings.	E	3
show rmon history historycontrol index <1-65535>	Displays the specified historical network traffic statistics table settings.	E	3
show rmon history historycontrol port-channel <aid>	Displays historical network traffic statistics for the specified port. aid: pon-<port>	E	3
show rmon statistics etherstats	Displays all current network traffic statistics.	E	3
show rmon statistics etherstats index <1-65535>	Displays the current network traffic statistics on the specified entry.	E	3
show rmon statistics etherstats port-channel <aid>	Displays the current network traffic statistics for the specified port. aid: pon-<port>	E	3

CHAPTER 68

Policy Rule

This chapter shows you how to configure policy rules.

68.1 Policy Rules Overview

A classifier distinguishes traffic into flows based on the configured criteria (Refer to [Chapter 66 on page 456](#) for more information). A policy rule ensures that a traffic flow gets the requested treatment in the network.

68.2 Policy Commands

Use these commands to configure policies based on the classification of traffic flows. A classifier distinguishes traffic into flows based on the configured criteria. A policy rule defines the treatment of a traffic flow.

Note: Configure classifiers before you configure policies. See [Chapter 66 on page 456](#) for more information on classifiers.

Table 233 Policy Commands

COMMAND	DESCRIPTION	M	P
show policy	Displays all policy related information.	E	3
show policy <name>	Displays the specified policy related information.	E	3

Table 233 Policy Commands (continued)

COMMAND	DESCRIPTION	M	P
<pre>policy <name> classifier <classifier-list> <[vlan <vlan- id>][egress-port <port- num>][mirror-port <port- num>][priority <0-7>][dscp <0- 63>][tos <0-7>][cir <bandwidth>][pir <bandwidth>][out- of-profile-dscp <0-63>][forward- action <drop forward>][queue- action <prio-set prio-queue prio- replace-tos>][diffserv-action <diff-set-dscp>][outgoing- mirror][outgoing-set- vlan][metering][out-of-profile- action <[change- dscp]>[drop][forward][set-drop-prec]>][green-to-cosq <0-7>]</pre>	<p>Configures a policy with the specified name.</p> <p><i>name</i>: 32 alphanumeric characters</p> <p>Specifies which classifiers this policy applies to.</p> <p><i>classifier-list</i>: names of classifiers separated by commas.</p> <p><[vlan <VLAN-ID>>]: Specifies a VLAN ID.</p> <p>Specifies the parameters related to the actions:</p> <ul style="list-style-type: none"> <i>egress-port</i>: an outbound port number <i>mirror-port</i>: mirror port number <i>priority</i>: IEEE 802.1p priority field <i>dscp</i>: Specifies a DSCP (DiffServ Code Point) number between 0 and 63. <i>tos</i>: Specifies the type of service (TOS) priority level. <i>cir</i>: Specifies the Commit Information Rate (CIR). <i>pir</i>: Specifies the Peak Information Rate (PIR). <i>out-of-profile-dscp</i>: Specifies a new DSCP number (between 0 and 63) if you want to replace or remark the DSCP number for out-of-profile traffic. <p>Specifies the actions for this policy:</p> <ul style="list-style-type: none"> <i>queue-action</i>: tells the OLT to: <ul style="list-style-type: none"> - set the IEEE 802.1p priority you specified in the <i>priority</i> parameter (<i>prio-set</i>) - sends the packet to priority queue (<i>prio-queue</i>) - replace the IEEE 802.1p priority field with the <i>tos</i> parameter value (<i>prio-replace-tos</i>). <i>outgoing-mirror</i> - sends the packet to the mirror port. <i>metering</i> - enables bandwidth limitations on the traffic flows. <i>out-of-profile-action</i> - specifies the actions to take for packets that exceed the bandwidth limitations: <ul style="list-style-type: none"> - discards the out of profile packets (<i>drop</i>). - queues the packets that are marked for dropping (<i>forward</i>). - marks the out of profile traffic and drops it when network is congested (<i>set-drop-precedence</i>). <i>green-to-cosq <0-7></i> - Select the CoS queue priority level for the incoming packets marked as green for transmission. 7 has the highest priority and 0 the lowest. It's recommended to assign the incoming packets marked as green via TRICM to the highest CoS queue priority level. 	C	13
policy help	Provides more information about the specified command.	C	13

Table 233 Policy Commands (continued)

COMMAND	DESCRIPTION	M	P
policy <name> inactive	Disables a policy.	C	13
no policy <name>	Deletes the policy.	C	13
no policy <name> inactive	Enables a policy.	C	13

68.3 Policy Command Examples

This example creates a policy (**highPriority**) for the traffic flow identified via classifier **VLAN3** (see the classifier example in [Chapter 66 on page 456](#)). This policy replaces the IEEE 802.1 priority field with the IP ToS priority field (value **7**) for **VLAN3** packets.

```
sysname(config)# policy highPriority classifier VLAN3 tos 7 queue-action
prio-replace-tos
sysname(config)# exit
sysname# show policy highPriority
Policy highPriority:
  Classifiers:
    VLAN3;
  Parameters:
    VLAN = 1; Priority = 0; DSCP = 0; TOS = 7;
    Egress Port = eth-1;
    Mirror Port = eth-1;
    CIR = 0; PIR= 0; Out-of-profile DSCP = 0;
  Action:
    Replace the 802.1 priority field with the IP TOS value;
```

This example creates a policy (**Policy1**) for the traffic flow identified via classifier **Class1** (see the classifier example in [Chapter 66 on page 456](#)). This policy forwards **Class1** packets to port ge-5-4.

```
sysname(config)# policy Policy1 classifier Class1 egress-port eth-4
outgoing-eport
sysname(config)# exit
sysname# show policy Policy1
Policy Policy1:
  Classifiers:
    Class1;
  Parameters:
    VLAN = 1; Priority = 0; DSCP = 0; TOS = 0;
    Egress Port = eth-4;
    Mirror Port = eth-1;
    CIR = 0; PIR= 0; Out-of-profile DSCP = 0;
  Action:
    Send the packet to the egress port;
```

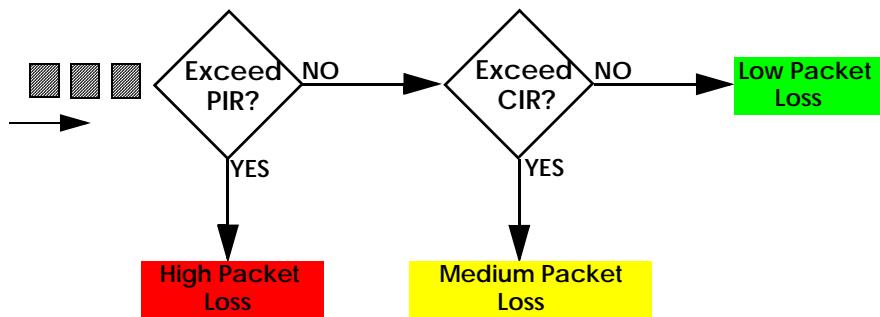
68.4 Two Rate Three Color Marker Traffic Policing

See [Section on page 156](#) for more information about Two Rate Three Color Marker.

68.4.1 TRTCM - Color-blind Mode

All packets are evaluated against the PIR. If a packet exceeds the PIR it is marked red. Otherwise it is evaluated against the CIR. If it exceeds the CIR then it is marked yellow. Finally, if it is below the CIR then it is marked green.

Figure 229 TRTCM - Color-blind Mode

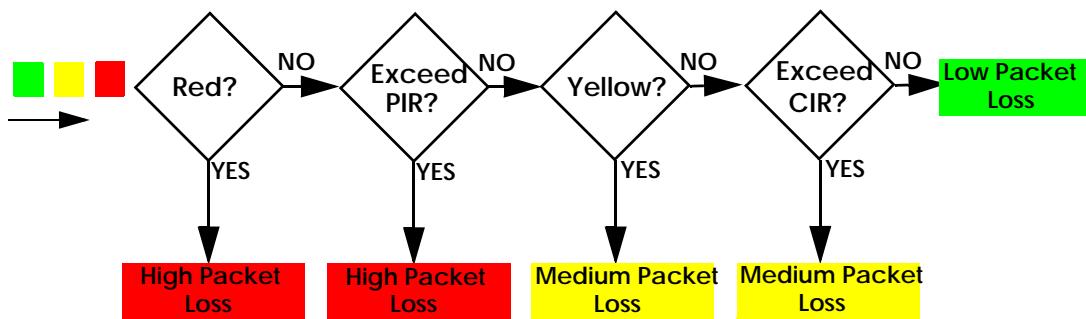


68.4.2 TRTCM - Color-aware Mode

In color-aware mode the evaluation of the packets uses the existing packet loss priority. TRTCM can increase a packet loss priority of a packet but it cannot decrease it. Packets that have been previously marked red or yellow can only be marked with an equal or higher packet loss priority.

Packets marked red (High packet loss priority) continue to be red without evaluation against the PIR or CIR. Packets marked yellow can only be marked red or remain yellow so they are only evaluated against the PIR. Only the packets marked green are first evaluated against the PIR and then if they don't exceed the PIR level, they will be evaluated against the CIR.

Figure 230 TRTCM - Color-aware Mode



68.5 TRTCM Commands

The following table lists the TRTCM commands.

Table 234 TRTCM Commands

COMMAND	DESCRIPTION	M	P
trtcm	Enables TRTCM on the OLT.	C	13
trtcm mode <color-aware color-blind>	Sets the mode for TRTCM on the OLT.	C	13
no trtcm	Disables TRTCM feature on the OLT.	C	13
interface port-channel <aid>	Enters sub-command mode for configuring the specified ports. aid: <pon eth>-<port>	C	13
trtcm	Enables TRTCM on the specified port(s).	C	13
no trtcm	Disables TRTCM on the port(s).	C	13
trtcm cir <kbps>	Sets the Commit Information Rate on the port(s).	C	13
trtcm pir <kbps>	Sets the Peak Information Rate on the port(s).	C	13
trtcm dscp green <0-63>	Specifies the DSCP value to use for packets with low packet loss priority.	C	13
trtcm dscp yellow <0-63>	Specifies the DSCP value to use for packets with medium packet loss priority.	C	13
trtcm dscp red <0-63>	Specifies the DSCP value to use for packets with high packet loss priority.	C	13

68.6 TRTCM Command Examples

This example activates TRTCM on the OLT with the following settings:

- Sets the OLT to inspect the DSCP value of packets (Color-aware mode).
- Enables TRTCM on port 5.
- Sets the Committed Information Rate (CIR) to 4000 Kbps.
- Sets the Peak Information Rate (PIR) to 4500 Kbps.

- Specifies DSCP value 7 for green packets, 22 for yellow packets and 44 for red packets.

```
sysname(config)# trtcn
sysname(config)# trtcn mode color-aware
sysname(config)# interface port-channel eth-5
sysname(config-interface)# trtcn
sysname(config-interface)# trtcn cir 4000
sysname(config-interface)# trtcn pir 4500
sysname(config-interface)# trtcn dscp green 7
sysname(config-interface)# trtcn dscp yellow 22
sysname(config-interface)# trtcn dscp red 44
sysname(config-interface)# exit
sysname(config)# exit
sysname# show running-config interface port-channel eth-5 trtcn
Building configuration...

Current configuration:

interface port-channel eth-5
  trtcn
    trtcn cir 4000
    trtcn pir 4500
    trtcn dscp green 7
    trtcn dscp yellow 22
    trtcn dscp red 44
exit
```

CHAPTER 69

Queuing Method

This chapter introduces the queuing methods supported.

69.1 Queuing Method Overview

Queuing is used to help solve performance degradation when there is network congestion. Queuing algorithms allow switches to maintain separate queues for packets from each individual source or flow and prevent a source from monopolizing the bandwidth.

69.1.1 Strictly Priority

Strictly Priority (SP) services queues based on priority only. As traffic comes into the OLT, 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.

69.1.2 Weighted Fair Queuing

Weighted Fair Queuing (WFQ) is used to guarantee the minimum bandwidth of each queue based on its bandwidth weight (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. By default, the weight for Q0 is 1, for Q1 is 2, for Q2 is 3, and so on.

The weights range from 1 to 15 and the actual guaranteed bandwidth is calculated as follows:

$$2^{(\text{Weight} - 1)} \times 10 \text{ KB}$$

If the weight setting is 5, the actual quantum guaranteed to the associated queue would be as follows:

$$2^4 \times 10\text{KB} = 160 \text{ KB}$$

69.2 Port by Port Queuing Commands

The following table lists the commands for this feature.

Note: The default queuing method for the PON ports is SPQ. The change of the queuing method could affect the Access Information Rate (AIR) in the downstream bandwidth profile.

Table 235 Port by Port Queuing Commands

COMMAND	DESCRIPTION	M	P
queue priority <0-7> level <0-7>	Sets the IEEE 802.1p priority level-to-physical queue mapping. priority <0-7>: IEEE 802.1p defines up to eight 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. level <0-7>: The OLT has up to 8 physical queues that you can map to the 8 priority levels. On the OLT, traffic assigned to higher index queues gets through faster while traffic in lower index queues is dropped if the network is congested.	C	13
interface port-channel <aid>	Enters sub-command mode for configuring the specified ports. aid: <pon eth>-<port>	C	13
spq	Sets the switch to use Strictly Priority Queuing (SPQ) on the specified ports.	C	13
wfq	Sets the switch to use Weighted Fair Queuing (WFQ) on the specified ports.	C	13
weight <wt1> <wt2> ... <wt8>	Assigns a weight value to each physical queue on the OLT. When the OLT is using WRR or WFQ, bandwidth is divided across different traffic queues according to their weights. Queues with larger weights get more service than queues with smaller weights. Weight values range: 1-127.	C	13

69.3 Port by Port Queuing Command Examples

This example configures WFQ on port 5 and assigns weight values (1,2,3,4,12,13,14,15) to the physical queues (Q0 to Q8).

```
sysname(config)# interface port-channel eth-5
sysname(config-interface)# wfq
sysname(config-interface)# weight 1 2 3 4 12 13 14 15
```

69.4 System-Wide Queuing Commands

The following section lists the commands for this feature.

Table 236 System-Wide Queuing Commands

COMMAND	DESCRIPTION	M	P
<code>queue priority <0-7> level <0-7></code>	<p>Sets the IEEE 802.1p priority level-to-physical queue mapping.</p> <p>priority <0-7>: IEEE 802.1p defines up to eight 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.</p> <p>level <0-7>: The OLT has up to seven physical queues that you can map to the eight priority levels. On the OLT, traffic assigned to higher index queues gets through faster while traffic in lower index queues will be dropped if the network is congested.</p>	C	13

69.5 System-Wide Queuing Command Examples

This example assigns weight values (1, 2, 3, 4, 12, 13, 14, and 15) to the physical queues (Q0 to Q8) on port 5.

```
sysname(config)# interface port-channel eth-5
sysname(config-interface)# weight 1 2 3 4 12 13 14 15
```

This example configures Gigabit port 1 to use SPQ.

```
sysname(config)# interface port-channel eth-1
sysname(config-interface)# spq
```

CHAPTER 70

VLAN Stacking and

Translation

This chapter shows you how to configure VLAN stacking and VLAN translation on your OLT. See [Chapter 51 on page 400](#) for more background information on Virtual LAN.

70.1 VLAN Stacking Overview

A service provider can use VLAN stacking to allow it to distinguish multiple customers VLANs, even those with the same (Customer-assigned) VLAN ID, within its network.

Use VLAN stacking 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 4,094 VLAN groups with each group containing up to 4,094 customer VLANs. This allows a service provider to provide different service, 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 on ports for these applications. 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.

70.1.1 VLAN Stacking Port Roles

Each port can have three VLAN stacking "roles", normal, access port and tunnel port (The latter is for Gigabit ports only).

- Use normal for "regular" (Non-VLAN stacking) IEEE 802.1Q frame switching.
- Use access port for ingress ports on the service provider's edge devices (1 and 2 in the VLAN stacking example figure). The incoming frame is treated as inner tagged or untagged, so a second VLAN tag (outer VLAN tag) can be added.

Note: If you use Q in Q, static VLAN Tx tagging must be enabled on a port set to the normal or access port role.

Otherwise static VLAN Tx Tagging must be disabled on a port set to the normal or access port role.

- Use Tunnel Port (Available for Gigabit ports only) for egress ports at the edge of the service provider's network. All VLANs belonging to a customer can be aggregated into a single service provider's VLAN (Using the outer VLAN tag defined by the Service Provider's (SP) VLAN ID (VID)).

Note: Static VLAN Tx tagging MUST be enabled on a port where you choose tunnel port.

70.2 VLAN Translation Overview

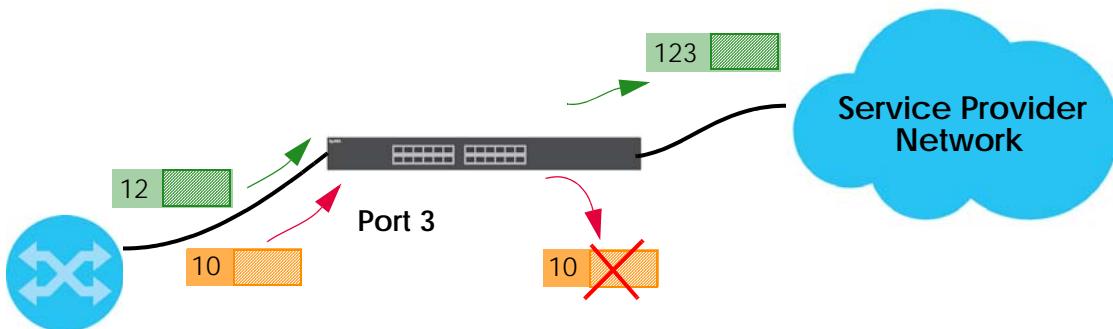
With VLAN translation enabled, the OLT can map the VLAN ID and priority level of packets received from a private network to those used in the service provider's network.

The OLT checks incoming traffic from the switch ports (Non-management ports) against the VLAN translation table first, the MAC learning table and then the VLAN table before forwarding them through an uplink port. When VLAN translation miss drop is enabled, the OLT discards the tagged packets that do not match an entry in the VLAN translation table.

70.2.1 VLAN Translation Example

In the following example figure, packets that carry VLAN ID 12 and are received on port 3 match a pre-configured VLAN translation rule. The OLT translates the VLAN ID from 12 into 123 before forwarding the packets.

Figure 231 VLAN Translation Example



70.3 VLAN Tag Format

A VLAN tag (Service provider VLAN stacking or customer IEEE 802.1Q) consists of the following three fields.

Table 237 VLAN Tag Format

Type	Priority	VID

"Type" is a standard Ethernet type code identifying the frame and indicates that whether the frame carries IEEE 802.1Q tag information. SP TPID (Service Provider Tag Protocol Identifier) is the service provider VLAN stacking tag type. Many vendors use 0x8100 or 0x9100.

TPID (Tag Protocol Identifier) is the customer IEEE 802.1Q tag.

- If the VLAN stacking port role is access port, then the OLT adds the SP TPID tag to all incoming frames on the service provider's edge devices (1 and 2 in the VLAN stacking example figure).

Priority refers to the IEEE 802.1p standard that allows the service provider to prioritize traffic based on the class of service (CoS) the customer has paid for.

- On the OLT, configure priority level of the inner IEEE 802.1Q tag.
- “0” is the lowest priority level and “7” is the highest priority level.

VID is the VLAN ID. SP VID is the VID for the second (Service provider’s) VLAN tag.

70.3.1 Frame Format

The frame format for an untagged Ethernet frame, a single-tagged 802.1Q frame (Customer) and a “double-tagged” 802.1Q frame (Service provider) is shown next.

Table 238 Single and Double Tagged 802.11Q Frame Format

Single and Double Tagged 802.11Q Frame Format											
IEEE 802.1Q customer tagged frame											
Double-tagged frame											
DA	SA	SPTPID	Priority	VID	TPID	Priority	VID	Len/Etype	Data	FCS	Untagged Ethernet frame
			DA	SA	TPID	Priority	VID	Len/Etype	Data	FCS	IEEE 802.1Q customer tagged frame
DA	SA	SPTPID	Priority	VID	TPID	Priority	VID	Len/Etype	Data	FCS	Double-tagged frame

Table 239 802.1Q Frame

DA	Destination Address	Priority	802.1p Priority
SA	Source Address	Len/Etype	Length and type of Ethernet frame
(SP)TPID	(Service Provider) Tag Protocol IDentifier	Data	Frame data
VID	VLAN ID	FCS	Frame Check Sequence

70.4 Port-based Q-in-Q

Port-based Q-in-Q lets the OLT treat all frames received on the same port as the same VLAN flows and add the same outer VLAN tag to them, even if they have different customer VLAN IDs.

70.5 Selective Q-in-Q

Selective Q-in-Q is VLAN-based. It allows the OLT to add different outer VLAN tags to the incoming frames received on one port according to their inner VLAN tags.

Note: Selective Q-in-Q rules are only applied to single-tagged frames received on the access ports. If the incoming frames are untagged or single-tagged but received on a tunnel port or cannot match any selective Q-in-Q rules, the OLT applies the port-based Q-in-Q rules to them.

70.6 VLAN Stacking Commands

Use these commands to add an outer VLAN tag to the inner IEEE 802.1Q tagged frames that enter your network.

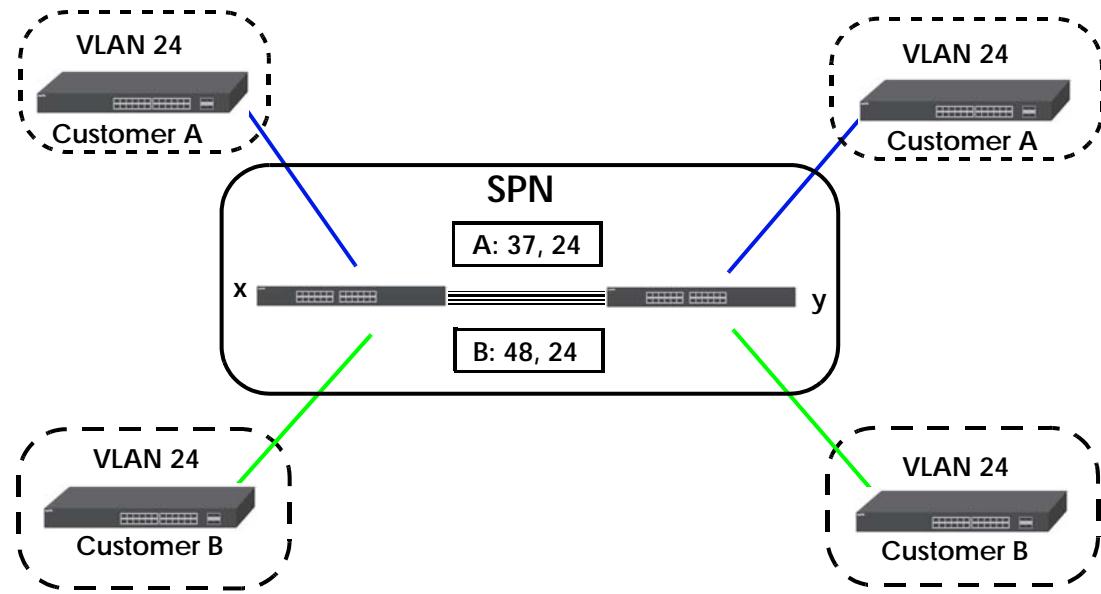
Table 240 VLAN Stacking Commands

COMMAND	DESCRIPTION	M	P
interface port-channel <aid>	Enters config-interface mode for the specified port(s). aid: <pon eth>-<port>	C	13
vlan-stacking priority <0-7>	Sets the priority of the specified port(s) in port-based VLAN stacking.	C	13
vlan-stacking role <normal access tunnel>	Sets the VLAN stacking port roles of the specified port(s). normal: The OLT ignores frames received (Or transmitted) on this port with VLAN stacking tags. access: the OLT adds the SP TPID tag to all incoming frames received on this port. tunnel: (Available for Gigabit and faster ports only) for egress ports at the edge of the service provider's network. Note: In order to support VLAN stacking on a port, the port must be able to allow frames of 1526 Bytes (1522 Bytes + 4 Bytes for the second tag) to pass through it.	C	13
vlan-stacking SPVID <1-4094>	Sets the service provider VID of the specified port(s).	C	13
vlan-stacking tunnel-tpid <tpid>	Sets a four-digit hexadecimal number from 0000 to FFFF that the OLT adds in the outer VLAN tag of the outgoing frames sent on the tunnel port(s).	C	13
show vlan-stacking	Displays the VLAN stacking configuration.	E	3

70.7 VLAN Stacking Command Examples

In the following example figure, both **A** and **B** are Service Provider's Network (**SPN**) customers with VPN tunnels between their head offices and branch offices respectively. Both have an identical VLAN tag for their VLAN group. The service provider can separate these two VLANs within its network by adding tag **37** to distinguish customer **A** and tag **48** to distinguish customer **B** at edge device **x** and then stripping those tags at edge device **y** as the data frames leave the network.

Figure 232 Example: VLAN Stacking



This example shows how to configure ports 1 and 2 on the OLT to tag incoming frames with the service provider's VID of 37 (Ports are connected to customer **A** network). This example also shows how to set the priority for ports 1 and 2. It also sets port 5 as a tunnel port with TPID 8100.

```

sysname(config)# interface port-channel eth-1
sysname(config-interface)# vlan-stacking role access
sysname(config-interface)# exit
sysname(config)# interface port-channel eth-2
sysname(config-interface)# vlan-stacking role access
sysname(config-interface)# exit
sysname(config)# interface port-channel eth-5
sysname(config-interface)# vlan-stacking role tunnel
sysname(config-interface)# vlan-stacking tunnel-tpid 8100
sysname(config-interface)# exit
sysname(config)# interface uni-port pon-1
sysname(config-interface)# vlan-translation name 37 ing-vid 24 egr-cvid
24 egr-svid 37 egr-spri 3 active on
sysname(config-interface)# vlan-translation
sysname(config-interface)# exit
sysname(config)# interface uni-port pon-2
sysname(config-interface)# vlan-translation name 37 ing-vid 24 egr-cvid
24 egr-svid 37 egr-spri 3 active on
sysname(config-interface)# vlan-translation
sysname(config-interface)# exit
sysname# show vlan-stacking
Switch Vlan Stacking Configuration
Operation: active
STPID: 0x8100

      Port        Role       Tunnel Port TPID          SPVID
Priority
pon-1        normal     0x88a8           1            0
pon-2        normal     0x88a8           1            0
pon-3        normal     0x88a8           1            0
pon-4        normal     0x88a8           1            0
eth-1        access     0x88a8           1            0
eth-2        access     0x88a8           1            0
eth-3        normal     0x88a8           1            0
eth-4        normal     0x88a8           1            0
eth-5        tunnel     0x8100           1            0
eth-6        normal     0x88a8           1            0
eth-7        normal     0x88a8           1            0
eth-8        normal     0x88a8           1            0
-----
---
eth-16       normal     0x88a8           1            0
eth-17       normal     0x88a8           1            0
eth-18       normal     0x88a8           1            0
eth-19       normal     0x88a8           1            0
eth-20       normal     0x88a8           1            0

```

70.8 VLAN Translation Commands

Use these commands to configure VLAN translation on the OLT. With VLAN translation enabled, the OLT can translate the VLAN ID and priority level of packets received from a private network to those used in the service provider's network.

Table 241 VLAN Translation Commands

COMMAND	DESCRIPTION	M	P
interface uni-port <aid>	Enters config-uniport mode for the specified port. <i>aid</i> : pon-<pon>	C	13
vlan-translation	Enables VLAN translation on the port.	C	13
vlan-translation help	Lists VLAN translation rule options.	C	13

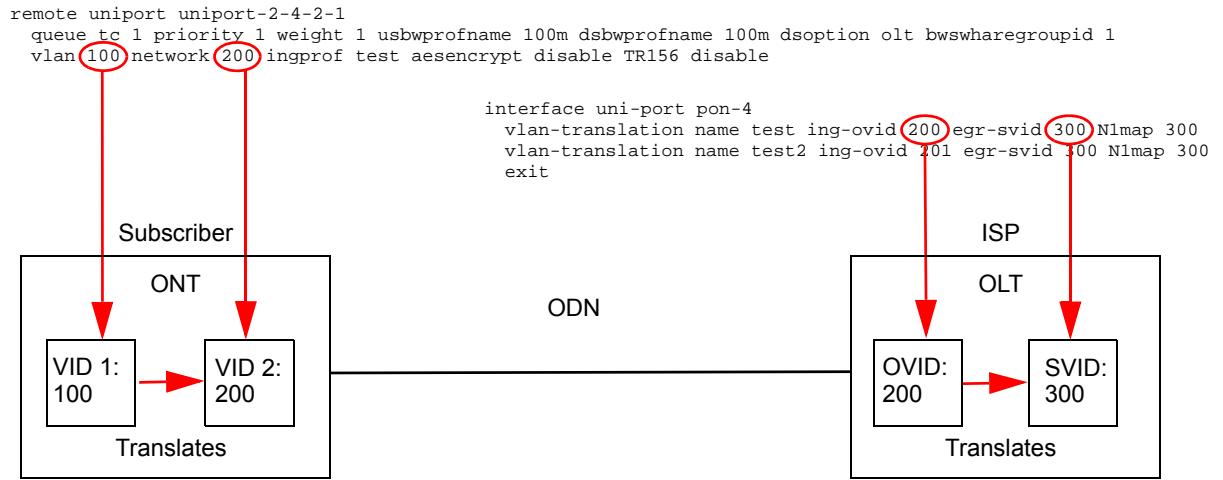
Table 241 VLAN Translation Commands (continued)

COMMAND	DESCRIPTION	M	P
<pre>vlan-translation name<name> [ing-ovid <vid>] [ing-ivid <vid>] [ing-opri <pri>] [ing- ipri <pri>] [egr-svid <vid>] [egr-cvid <vid>] [egr-spri <pri>] [egr-cpri <pri>] [N1map <group>] [cross- connect <enable disable>] [cross-port <aid>] [tr156 <on off>] [active <on off>]</pre>	<p>Creates a VLAN translation rule (with the specified name) on the port.</p> <p><i>vid</i>: VLAN ID, 1 ~ 4094.</p> <p><i>pri</i>: Priority (0 ~ 7), lower numbers are higher priority.</p> <p>The ingress parameters (ing-<xxxx>) mean the VLAN tag of the target traffic to which the OLT applies this translation rule. That is the ingress (incoming, upstream) packets coming from the subscribers.</p> <p>ing-ovid <vid>: The outer tag of incoming packets.</p> <p>ing-ivid <vid>: The inner tag of incoming packets.</p> <p>ing-opri <pri>: The outer priority of incoming packets.</p> <p>ing-ipri <pri>: The inner priority of incoming packets.</p> <p>The OLT applies the egress parameters (egr-<xxxx>) to the egress (outgoing) packets going out the uplink ports towards the backbone network.</p> <p>egr-svid <vid>: The Service provider VID (outer) tag of outgoing packets.</p> <p>egr-cvid <vid>: The Customer VID (inner) tag of outgoing packets.</p> <p>egr-spri <vid>: The Service provider (outer) priority of outgoing packets.</p> <p>egr-cpri <vid>: The Customer (inner) priority of outgoing packets.</p> <p>N1map <group>: Use a group ID (1 ~ 16384) to map multiple ingress (ing) VLANs to one egress (egr) VLAN. All VLAN translation rules with the same N1map group ID must use the same egress VLAN.</p> <p>cross-connect <enable disable>: Connect this rule's VLAN on this port to another port. The OLT ignores the MAC address of ingress packets and forwards them by VID to the cross-connected port. The OLT does not need to learn a destination MAC address before forwarding packets for it to the cross-connected port. No other ports can be members of the VLAN. You cannot use N1map and cross connect in the same VLAN translation rule.</p>	C	13

Table 241 VLAN Translation Commands (continued)

COMMAND	DESCRIPTION	M	P
	<p>cross-port <aid>: Cross connect connects this rule's VLAN on this port to another port. Specify the other port here.</p> <p>tr156 <on off>: Turns TR156 mode on or off. TR156 mode adds a VLAN tag based on the GEM tag of incoming upstream packets.</p> <p>active <on off>: Turns the VLAN translation rule on or off.</p>	C	13
vlan-xlate-miss-drop	Enables upstream VLAN translation miss drop on the port. The OLT discards incoming tagged packets from the subscribers that do not match an entry in the VLAN translation table.	C	13
egr-vlan-xlate-miss-drop	Enables downstream VLAN translation miss drop on the port. The OLT discards outgoing tagged packets destined for the subscribers that do not match an entry in the VLAN translation table.	C	13
no vlan-translation	Disables VLAN translation on the port.	C	13
no vlan-translation all	Removes all VLAN translation rules on the port.	C	13
no vlan-translation name <name>	Removes the specified VLAN translation rule on the port.	C	13
no vlan-xlate-miss-drop	Disables upstream VLAN translation miss drop on the port. The OLT floods incoming tagged packets from the subscribers that do not match an entry in the VLAN translation table.	C	13
no egr-vlan-xlate-miss-drop	Disables downstream VLAN translation miss drop on the port. The OLT floods outgoing tagged packets destined for the subscribers that do not match an entry in the VLAN translation table.	C	13
exit	Exit the config-uniport mode.	C	13
help	Provides more information about the specified command.	C	13
show interfaces uni-port <aid>	Shows all UNI port (OLT PON or GE port) VLAN translation rules on the port. <i>aid: pon-<pon></i>	E	13

The following figure shows the relationship between the VLAN IDs in the UNI port VLAN and VLAN translation commands.

Figure 233 VLANs in the UNI Port VLAN and VLAN Translation Commands

70.9 VLAN Translation Command Examples

This example enables VLAN translation on the OLT and creates a VLAN translation rule to translate the VLAN ID from 123 to 234 in the packets received on PON1.

```
sysname# configure
sysname(config)# interface uni-port pon-1
sysname(config-uniport)# vlan-translation name test ing-ovid 123 egr-
svid 234 egr-spri 3
sysname(config-uniport)# vlan-translation
```

CHAPTER 71

Multicast

This chapter shows you how to configure various multicast features.

71.1 Multicast Overview

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

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

71.1.1 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 subnet. 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 website for more information).

71.1.2 IGMP Snooping

The OLT can passively snoop on IGMP 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 OLT to learn multicast groups without you having to manually configure them.

The OLT 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. IGMP snooping generates no additional network traffic, allowing you to significantly reduce multicast traffic passing through your OLT.

71.2 Multicast Status

Use the `show multicast` command to display the multicast group information.

sysname# show multicast			
Multicast Status			
Total	VID	Multicast Group(Filter Mode)	Timeout
		[Source Address] {IGMP channel, univid}	
-----	-----	-----	-----
1	1001	225.1.1.1(Exclude) {uniport-5-1-1-4, 1001}	98 0:23:58 Source IP 1.5.1.1
-----	-----	-----	-----

The following table describes the labels in the output.

Table 242 Multicast Status

LABEL	DESCRIPTION
Total	This field displays the number of groups that a port belongs to.
VID	This field displays the multicast VLAN ID.
Multicast Group	This field displays IP multicast group addresses.
Filter Mode	This field displays the IGMP v3 filter mode of the group, such as INCLUDE or EXCLUDE.
Timeout	This field displays the time in seconds after which the group will expire.
Up Time	This field displays how long a port has belonged to a group.
Source Address	This field displays the source IP address of a multicast server.
IGMP channel	This field displays the port number that belongs to the multicast group.
univid	This field displays the unicast VLAN ID for the IGMP channel.
Source IP	This field displays the source IP address of a multicast client.

71.3 IGMP Proxy Commands

Use the `igmp-proxy` commands to configure the IGMP proxy settings on the OLT. The following table describes the commands options.

Table 243 igmp-proxy Commands

COMMAND	DESCRIPTION	M	P
<code>igmp-proxy</code>	Enables IGMP proxy on the OLT.	C	13
<code>igmp-proxy ip <ip-address></code>	Sets the IGMP proxy's working IP address.	C	13
<code>igmp-proxy v3mode</code>	Enables IGMPv3 and MLDv2 modes.	C	13
<code>no igmp-proxy</code>	Disables IGMP proxy on the OLT.	C	13
<code>no igmp-proxy v3mode</code>	Disables IGMPv3 and MLDv2 modes.	C	13
<code>show igmp</code>	Displays the IGMP settings.	E	3

71.4 IGMP Snooping/Multicast Commands

Use the `igmp-snooping/multicast` commands in configure mode to configure the multicast settings. The following table describes the command options.

Table 244 igmp-snooping/multicast Commands

COMMAND	DESCRIPTION	M	P
<code>igmp-snooping <cr></code>	Enables IGMP snooping to forward group multicast traffic only to ports that are members of that group.	C	13
<code>igmp-snooping host-timeout <1-16711450></code>	Configures the time in seconds that elapses before the OLT removes an IGMP group membership entry if it does not receive report messages from the port.	C	13
<code>igmp-snooping leave-timeout <1-16711450></code>	Configures the leave-timeout interval, in seconds, for a port without receiving an IGMP report after an IGMP leave was received.	C	13
<code>igmp-snooping 8021p-priority <0-7></code>	Sets the IEEE 802.1p priority for outgoing IGMP snooping packets.	C	13
<code>igmp-snooping mld-support <cr></code>	Enables MLDv1/v2 ability.	C	13
<code>igmp-snooping query-tag <mvlan ani-vlan></code>	Configures the query tag to be either multicast VLAN or ANI VLAN on NNI ports.	C	13
<code>igmp-snooping report-tag <mvlan ani-vlan></code>	Configures the tag of outgoing IGMP control packets to be either multicast VLAN or ANI VLAN on NNI ports.	C	13
<code>igmp-snooping reserved-multicast-group <drop flooding></code>	<p>Specifies the action to perform when the OLT receives a frame with a reserved multicast address. Select drop to discard the frame(s). Select flooding to send the frame(s) to all ports.</p> <p>The IP address range of 224.0.0.0 to 224.0.0.255 is reserved for multicasting on the local network only. For example, 224.0.0.1 is for all hosts on a local network segment and 224.0.0.9 is used to send RIP routing information to all RIP v2 routers on the same network segment. A multicast router will not forward a packet with the destination IP address within this range to other networks. See the IANA web site for more information.</p> <p>The layer 2 multicast MAC addresses used by Cisco layer 2 protocols, 01:00:0C:CC:CC:CC and 01:00:0C:CC:CC:CD, are also included in this group.</p>	C	13
<code>igmp-snooping unknown-multicast-frame <drop flooding></code>	Specifies the action to perform when the OLT receives an unknown multicast frame. Select drop to discard the frame(s). Select flooding to send the frame(s) to all ports.	C	13
<code>no igmp-snooping <cr></code>	Disables IGMP snooping on the OLT.	C	13
<code>no igmp-snooping mld-support</code>	Disables MLDv1/v2 ability.	C	13
<code>no igmp-snooping 8021p-priority</code>	Disables the IEEE 802.1p priority for outgoing IGMP snooping packets.	C	13
<code>clear multicast port all</code>	Removes all multicast port counters.	E	3
<code>clear multicast port <pon eth>-<port></code>	Remove the specified multicast port counter.	E	13

Table 244 igmp-snooping/multicast Commands (continued)

COMMAND	DESCRIPTION	M	P
show igmpchannel counter	Displays the IGMP channel counter.	E	13
show igmp	Displays the IGMP snooping settings.	E	3
show multicast port <cr>	Displays all multicast port counters.	E	3
show multicast port <pon eth>-<port>	Displays the specified multicast port counters.	E	3
show multicast port query <pon eth>-<port> <all>	Displays the port query packet counter.	E	13
show multicast port receive <pon eth>-<port> <all>	Displays the port received packet counter.	E	13
show multicast port report <pon eth>-<port> <all>	Displays the port report packet counter.	E	13
show multicast port specific <pon eth>-<port> <all>	Displays the specified port's transmit packet counters. Displays all port transmit packet counters.	E	13
show multicast snooping-vlan	Displays the IGMP snooping VLAN settings.	E	3
show multicast join-port	Displays multicast group member information.	E	3
show multicast querier-source-IP	Displays the IP address of the device which sent the multicast queries.	E	3
show mcast-channel	Displays the following information of the multicast group(s) that was created. <ul style="list-style-type: none">• Package member• Preview-duration• Preview-count• Preview-blackout• pbit• Cac profile	E	13
show multicast	Displays multicast status, including the port number, VLAN ID and multicast group members on the OLT.	E	3
show multicast vlan	Displays a number of the available multicast groups in all VLANs.	E	3
show multicast vlan <VID>	Displays a number of the available multicast groups on the specified VLAN.	E	3
show multicast port transmit <pon eth>-<port> <all>	Displays outgoing multicast traffic statistics of the specified port or all ports.	E	13
show multicast vlan receive	Displays incoming multicast traffic statistics per VLAN network.	E	3
show multicast vlan specific	Displays multicast traffic statistics per VLAN network.	E	3
show multicast vlan transmit	Displays incoming multicast traffic statistics per VLAN network.	E	3
show interfaces config <aid> igmp-immediate-leave	Displays the immediate leave settings for IGMP snooping. <i>aid: <pon eth>-<port></i>	E	3

Table 244 igmp-snooping/multicast Commands (continued)

COMMAND	DESCRIPTION	M	P
show interfaces config <aid> igmp-query-mode aid: <pon eth>-<port>	Displays the IGMP query mode for the specified port(s).	E	3
mcast-channel <start-group-ip> <end-group-ip> vlan <1-4094> <i>start-group-ip</i> : The beginning IP address of the multicast IP address range. The range of addresses must be between 224.0.0.0 and 239.255.255.255. <i>end-group-ip</i> : The ending IP address of the multicast IP address range. The range of addresses must be between 224.0.0.0 and 239.255.255.255. <i>vlan</i> : 1 ~ 4094. Configures a multivast VLAN.	Sets a range of multicast IP addresses on the specified VLAN.	C	13
no mcast-channel <start-group-ip> <end-group-ip> vlan <1-4094> <cr>	Clears the specified range of multicast IP addresses on the specified VLAN.	C	13

Table 244 igmp-snooping/multicast Commands (continued)

COMMAND	DESCRIPTION	M	P
<pre>mcast-channel <start-group-ip> <end-group-ip> vlan <1-4094> [active <on off>] [pbit <0-7>] [name <1-31 chars>] [src-ip <ip>] [package-member <0-32>] [cacprof <prof>] [preview-duration <1-6000 sec>] [preview-count <1-100 count>] [preview-blackout <0-7200 sec>]</pre>	<p>Configures a GPON client multicast channel. See Section 87.3.6 on page 601 for associating multicast channels to the IGMP channel of a uniport of the ONT.</p> <p><i>start-group-ip</i>: The beginning IP address of the multicast IP address range. The range of addresses must be between 224.0.0.0 and 239.255.255.255.</p> <p><i>end-group-ip</i>: The ending IP address of the multicast IP address range. The range of addresses must be between 224.0.0.0 and 239.255.255.255.</p> <p><i>vlan</i>: 1 ~ 4094. Configures an MVR.</p> <p><i>active</i>: Use “on” to activate this CLI configuration and, for any remote ONT UNI port adapting this package member, provision OMCI to the ONT.</p> <p><i>pbit</i>: 0 ~ 7. Sets the IEEE 802.1p priority level to add to the untagged frames of this multicast channel.</p> <p><i>groupname</i>: Configures the name of the multicast channel.</p> <p><i>src-ip</i>: Configures the source IP of the IGMP server supplying this range of groups.</p> <p><i>package</i>: 0 ~ 32. Assigns an ID number to this multicast channel. Subscribers will be able to order package members according to this identifier.</p> <p><i>cacprof <prof></i>: Specify the QoS CAC profile which contains multicast bandwidth settings and is created by the <code>qos cacprof</code> command.</p> <p><i>preview-duration <sec></i>: 1 ~ 6000. Configures the duration that a subscriber can join to a group. This field is meaningful only when this multicast channel is ordered by subscribers with preview privilege.</p> <p><i>preview-count <count></i>: 1 ~ 100. Configures the maximum number of times a subscriber can preview this multicast channel’s content. This field is meaningful only when this multicast channel is ordered by subscribers with preview privilege.</p> <p><i>preview-blackout <sec></i>: 0 ~ 7200. Configures the duration that a subscriber has to wait between 2 times of previewing a group. This field is meaningful only when this multicast channel is ordered by subscribers with preview privilege.</p>	C	13
<code>mcast-channel help</code>	Displays the help about the multicast channel command.	C	13

Table 244 igmp-snooping/multicast Commands (continued)

COMMAND	DESCRIPTION	M	P
interface port-channel <aid>	Enters the sub-commands for configuring the specified interface. <i>aid: <pon eth>-<port></i>	C	13
igmp-immediate-leave	Enables the OLT to remove this port from the multicast tree when an IGMP version 2 leave message is received on this port. Select this option if there is only one host connected to this port.	C	13
no igmp-immediate-leave	Disables the immediate leave function for IGMP snooping.	C	13
igmp-querier-mode <auto fixed edge>	Enables IGMP query mode on the specified port.	C	13
exit	Exits from interface port channel sub commands.	C	13
show multicast mode-querier	Displays IGMP querier mode settings.	E	3
show igmpchannel	Displays IGMP channel's status.	E	3

The following table shows the IGMP commands for an interface port channel.

Table 245 IGMP Commands on Interface Port Channel

LABEL	DESCRIPTION	M	P
remote uniport <aid>	Configures UNI port settings. <i>aid: uniport-<pon>-<ont>-<card>-<port></i>	C	13
igmpchannel <uni-vid> <cr>	Creates an IGMP channel on this port. <i>uni-vid:</i> The default VLAN ID for IGMP reports, that is Join and Leave packets. You must first create the VLAN using the <i>vlan</i> command under the <i>remote uniport</i> command. (Required.)	C	13

Table 245 IGMP Commands on Interface Port Channel (continued)

LABEL	DESCRIPTION	M	P
<code>igmpchannel <uni-vid> [version <IGMPv2 IGMPv3> [<prof>] [maxgroup <num>] [maxmsg <num>] [signaling <on off>] [previewpkg <packages>] [fullviewpkg <packages>] [txtag <transparent untag replace <1~4094>>] [active <on off>]</code>	<p>Configures a UNI port IGMP channel.</p> <p><i>uni-vid</i>: The default VLAN ID for IGMP reports, that is Join and Leave packets. You must create the VLAN using the <code>vlan</code> command under the <code>remote uniport</code> command. (Required)</p> <p><i>version</i>: Configures the IGMP version to either IGMPv2 or IGMPv3. (Optional, default IGMPv2.)</p> <p><i><prof></i>: Adapts a QoS CAC profile which contains multicast bandwidth settings and is created by the <code>qos cacprof</code> command. (Optional)</p> <p><i>maxgroup</i>: <0-512>. The maximum number of multicast groups a client can join concurrently. (Optional, default 64.)</p> <p><i>maxmsg</i>: <0-255>. The maximum number of IGMP reports a client can send per second. (Optional, default 0.)</p> <p><i>signaling</i>: <on off>. Enables the IGMP signaling mode. That is, it lets the OLT control and decide the multicast table of the ONT. The ONT must also support this feature. (Optional, default off.)</p> <p><i>previewpkg</i>: Configures a list of package members with preview privilege. That is, IGMP clients can join groups in these package members only in a period of time. Use the <code>mcast-channel</code> command to create the package members. The ONT must also support this feature. (Optional)</p> <p><i>fullviewpkg</i>: Configures a list of package members with full view privilege. That is, IGMP clients can join groups in these package members all the time. Use the <code>mcast-channel</code> command to create the package members. (Optional)</p> <p><i>txtag</i>: Sets whether the ONT sends multicast downstream traffic with a VLAN behavior. Use <code>transparent</code> if you want to follow the uniport VLAN txtag setting. Use <code>untag</code> for untagged VLAN. Use <code>replace</code> to replace the original VLAN with a specific VID.</p> <p><i>active</i>: Activates/deactivates this CLI configuration and, for the remote ONT UNI port, provisions OMCI to ONT. (Optional, default is on.)</p>	C	13
<code>no igmpchannel <cr></code>	Deletes the UNI port IGMP channel.	C	13
<code>igmpchannel help</code>	Displays the help about IGMP channel.	C	13

71.5 IGMP CDR Commands

The following table shows the IGMP Call Detail Record (CDR) commands. CDR is used by telephone companies for call related information.

Table 246 IGMP CDR Commands

LABEL	DESCRIPTION	M	P
cdr igmp <cr>	Enables the IGMP CDR feature on the OLT.	C	13
no cdr igmp <cr>	Disables the IGMP CDR feature on the OLT.	C	13
cdr igmp logsize <0 - 65535>	Sets the maximum number of IGMP CDR logs allowed.	C	13
cdr-flush igmp	Flushes the IGMP CDR table.	E	13
show cdr igmp	Displays the IGMP CDR settings.	E	13
remote uniport <aid>	Configures UNI port settings. aid: <i>uniport-<pon>-<ont>-<card>-<port></i>	C	13
no igmpchannel <cr>	Delete the UNI port IGMP channel.	C	13
igmpchannel help	Displays the help about IGMP channel.	C	13
show igmpchannel CDR <cr>	Displays the IGMP channel CDR settings.	E	13
show igmpchannel CDR <aid>	Displays the specified uniport's IGMP channel CDR settings. aid: <i>uniport-<pon>-<ont>-<card>-<port></i>	E	13
interface port-channel <aid>	Enables a port or a list of ports for configuration. aid: <pon eth>-<port>	C	13
igmp-immediate-leave	Enables IGMP immediate leave on the specified port.	C	13

71.6 IGMP Snooping VLAN Commands

Use the `igmp-snooping vlan` command to configure the IGMP snooping VLAN and the `show multicast snooping-vlan` command to display the settings.

```
sysname# show multicast snooping-vlan
IGMP Snooping VLAN mode      :Auto

Index          VID          Name
-----        -----
 1            100          vlan100
```

The following table describes the commands for IGMP snooping VLAN.

Table 247 IGMP Snooping VLAN Commands

COMMAND	DESCRIPTION	M	P
clear multicast vlan all	Removes all multicast VLAN counters.	E	3
clear multicast vlan <vid>	Removes multicast VLAN counter of the specified VLAN.	E	13

CHAPTER 72

IP Source Guard

Use IP source guard to filter unauthorized DHCP and ARP packets in your network.

72.1 IP Source Guard Binding Commands

Use these commands to manage the bindings table for IP source guard.

Table 248 IP Source Guard Binding Commands

COMMAND	DESCRIPTION	M	P
show ip source binding [<mac-addr>] [...]	Displays the bindings configured on the OLT, optionally based on the specified parameters.	E	3
show ip source binding help	Provides more information about the specified command.	E	3
ip source binding <mac-addr> vlan <vlan-id> <ip> [interface port-channel <interface-id>]	Creates a static binding for ARP inspection.	C	13
no ip source binding <mac-addr> vlan <vlan-id>	Removes the specified static binding.	C	13

72.2 IP Source Guard Binding Command Examples

This example shows the current binding table.

```
sysname# show ip source binding
      MacAddress      IpAddress      Lease          Type  VLAN  Port
-----  -----  -----
Total number of bindings: 0
```

The following table describes the labels in this display.

Table 249 show ip source binding

LABEL	DESCRIPTION
MacAddress	This field displays the source MAC address in the binding.
IpAddress	This field displays the IP address assigned to the MAC address in the binding.
Lease	This field displays how many days, hours, minutes, and seconds the binding is valid; for example, 2d3h4m5s means the binding is still valid for 2 days, 3 hours, 4 minutes, and 5 seconds. This field displays infinity if the binding is always valid (For example, a static binding).

Table 249 show ip source binding (continued)

LABEL	DESCRIPTION
Type	This field displays how the switch learned the binding. static: This binding was learned from information provided manually by an administrator.
VLAN	This field displays the source VLAN ID in the binding.
Port	This field displays the port number in the binding. If this field is blank, the binding applies to all ports.

72.3 DHCP Snooping & DHCP VLAN Commands

Use the `dhcp snooping` commands to configure the DHCP snooping on the OLT and the `dhcp vlan` commands to specify a DHCP VLAN on your network. DHCP snooping filters unauthorized DHCP packets on the network and builds the binding table dynamically.

Note: You must set up a management IP address for each VLAN that you want to configure DHCP settings for on the OLT.

Table 250 DHCP Snooping Commands

COMMAND	DESCRIPTION	M	P
<code>show dhcp snooping</code>	Displays DHCP snooping configuration on the OLT.	E	3
<code>show dhcp snooping binding</code>	Displays the DHCP binding table.	E	3
<code>show dhcp snooping database</code>	Displays DHCP snooping database update statistics and settings.	E	3
<code>show dhcp snooping database detail</code>	Displays DHCP snooping database update statistics in full detail form.	E	3
<code>dhcp snooping</code>	Enables DHCP Snooping on the OLT.	C	13
<code>no dhcp snooping</code>	Disables DHCP Snooping on the OLT.	C	13
<code>dhcp snooping database <tftp://host/filename></code>	Specifies the location of the DHCP snooping database. The location should be expressed like this: tftp://(domain name or IP address)/directory, if applicable/file name; for example, tftp://192.168.10.1/database.txt.	E	13
<code>no dhcp snooping database</code>	Removes the location of the DHCP snooping database.	C	13
<code>dhcp snooping database timeout <10-65535 seconds></code>	Specifies how long (10-65535 seconds) the OLT tries to complete a specific update in the DHCP snooping database before it gives up.	C	13
<code>no dhcp snooping database timeout</code>	Resets how long the OLT tries to complete a specific update in the DHCP snooping database before it gives up to the default value (300).	C	13
<code>dhcp snooping database write-delay <10-65535 seconds></code>	Specifies how long (10-65535 seconds) the OLT waits to update the DHCP snooping database the first time the current bindings change after an update.	C	13

Table 250 DHCP Snooping Commands (continued)

COMMAND	DESCRIPTION	M	P
no dhcp snooping database write-delay	Resets how long the OLT waits to update the DHCP snooping database the first time the current bindings change after an update to the default value (300).	C	13
dhcp snooping vlan <vlan-list>	Specifies the VLAN IDs for VLANs you want to enable DHCP snooping on.	C	13
no dhcp snooping vlan <vlan-list>	Specifies the VLAN IDs for VLANs you want to disable DHCP snooping on.	C	13
dhcp snooping vlan <vlan-list> information	Sets the OLT to add the system name to DHCP requests that it broadcasts to the DHCP VLAN, if specified, or VLAN.	C	13
no dhcp snooping vlan <vlan-list> information	Sets the OLT to not add the system name to DHCP requests that it broadcasts to the DHCP VLAN, if specified, or VLAN.	C	13
dhcp snooping vlan <vlan-list> option	Sets the OLT to add the port number and VLAN ID to DHCP requests that it broadcasts to the DHCP VLAN, if specified, or VLAN.	C	13
no dhcp snooping vlan <vlan-list> option	Sets the OLT to not add the port number and VLAN ID to DHCP requests that it broadcasts to the DHCP VLAN, if specified, or VLAN.	C	13
no dhcp snooping vlan <vlan-list> format	Disables DHCP snooping from appending the option 82 format [SYS_ID PONPORT:NNISVID.SNISVID ONTID/SN] into the Circuit ID.	C	13

Table 250 DHCP Snooping Commands (continued)

COMMAND	DESCRIPTION	M	P
dhcp snooping vlan <vlan-list> format	<p>Enables DHCP option 82 with a specific format. Commands available are:</p> <p>(A) option: 1. append [ponport vlan] into the Circuit ID of DHCP option 82 2. append [client's mac] into the Remote ID of DHCP option 82</p> <p>(B) information: append [system_name] behind [ponport vlan] into the Circuit ID of DHCP option 82</p> <p>If (A) & (B) are set at the same time, the Circuit ID format is [ponport vlan system_name]</p> <p>(C) format: append the following specific format into the Circuit ID and Remote ID: circuit-id: [SYS_ID PONPORT:NNISVID.SNISVID ONTID/SN] remote-id: none (since it is not needed)</p> <p>(D) option-info per system:DHCP l2agent VLAN <info></p> <p>Note: The OLT uses the following rules for DHCP option 82 configuration: (D) > (C) > (A) = (B).</p>	C	13
dhcp snooping vlan <vlan-list> help	Provides more information about the specified command.	C	13
clear dhcp snooping database statistics	Deletes all statistics records of DHCP requests going through the OLT.	E	13
renew dhcp snooping database	Loads dynamic bindings from the default DHCP snooping database.	E	13
renew dhcp snooping database <tftp://host/filename>	Loads dynamic bindings from the specified DHCP snooping database.	E	13
interface port-channel <aid>	Enables a port or a list of ports for configuration. aid: <pon eth>-<port>	C	13
dhcp snooping trust	Sets this port as a trusted DHCP snooping port. Trusted ports are connected to DHCP servers or other switches, and the OLT discards DHCP packets from trusted ports only if the rate at which DHCP packets arrive is too high.	C	13
dhcp snooping limit rate <pps>	Sets the maximum rate in packets per second (pps) that DHCP packets are allowed to arrive at a trusted DHCP snooping port.	C	13

Table 250 DHCP Snooping Commands (continued)

COMMAND	DESCRIPTION	M	P
no dhcp snooping trust	Disables this port from being a trusted port for DHCP snooping.	C	13
no dhcp snooping limit rate	Resets the DHCP snooping rate to the default (0).	C	13

The following table describes the `dhcp-vlan` commands.

Table 251 DHCP VLAN Commands

COMMAND	DESCRIPTION	M	P
<code>dhcp dhcp-vlan <vlan-id></code>	Specifies the VLAN ID of the DHCP VLAN.	C	13
<code>no dhcp dhcp-vlan</code>	Disables DHCP VLAN on the OLT.	C	13

72.4 DHCP Snooping & DHCP VLAN Command Examples

This example:

- Enables DHCP snooping OLT.
- Sets up an external DHCP snooping database on a network server with IP address 172.16.37.17.
- Enables DHCP snooping on VLANs 1,2,3,200 and 300.
- Sets the OLT to add the slot number, port number and VLAN ID to DHCP requests that it broadcasts to the DHCP VLAN.
- Sets ports eth-1 to eth-4 as DHCP snooping trusted ports.
- Sets the maximum number of DHCP packets that can be received on ports eth-1 to eth-4 to 100 packets per second.
- Configures a DHCP VLAN with a VLAN ID 300.

- Displays DHCP snooping configuration details.

```

OLT1404A(config)# dhcp snooping
OLT1404A(config)# dhcp snooping database tftp://172.16.37.17/
OLT1404A(config)# dhcp snooping vlan 1,2,3,200,300
OLT1404A(config)# dhcp snooping vlan 1,2,3,200,300 option
OLT1404A(config)# interface port-channel eth-1&&-4
OLT1404A(config-interface)# dhcp snooping trust
OLT1404A(config-interface)# dhcp snooping limit rate 100
OLT1404A(config-interface)#

OLT1404A(config)# dhcp dhcp-vlan 300
OLT1404A(config)#

OLT1404A# show dhcp snooping
Switch DHCP snooping is enabled
DHCP Snooping is configured on the following VLANs:
  1-3,200,300
Option 82 is configured on the following VLANs:
  1-3,200,300
Apending system name is configured on the following VLANs:

Apending specific format for option-82 is configured on the following
VLANs:

  DHCP VLAN is enabled on VLAN 300
Interface Trusted Rate Limit (pps)
-----
pon-1      no      unlimited
pon-2      no      unlimited
pon-3      no      unlimited
pon-4      no      unlimited
eth-1      yes     100
eth-2      yes     100
eth-3      yes     100
eth-4      yes     100
eth-5      no      unlimited
eth-6      no      unlimited
eth-7      no      unlimited
eth-8      no      unlimited
eth-9      no      unlimited
eth-10     no      unlimited
eth-11     no      unlimited
eth-12     no      unlimited
eth-13     no      unlimited
eth-14     no      unlimited
eth-15     no      unlimited
eth-16     no      unlimited
eth-17     no      unlimited
eth-18     no      unlimited
eth-19     no      unlimited
eth-20     no      unlimited

```

72.5 ARP Inspection Commands

Use ARP inspection to look at the current list of MAC address filters that were created because the OLT identified an unauthorized ARP packet. When the OLT identifies an unauthorized ARP packet, it

automatically creates a MAC address filter to block traffic from the source MAC address and source VLAN ID of the unauthorized ARP packet.

Use these commands to filter unauthorized ARP packets in your network.

Table 252 ARP Inspection Commands

COMMAND	DESCRIPTION	M	P
arp inspection	Enables ARP inspection on the OLT. You still have to enable ARP inspection on specific VLAN and specify trusted ports.	C	13
no arp inspection	Disables ARP inspection on the OLT.	C	13
show arp inspection	Displays ARP inspection configuration details.	E	3
clear arp inspection statistics	Removes all ARP inspection statistics on the OLT.	E	13
clear arp inspection statistics vlan <vlan-list>	Removes ARP inspection statistics for the specified VLAN(s).	E	13
show arp inspection statistics	Displays all ARP inspection statistics on the OLT.	E	3
show arp inspection statistics vlan <vlan-list>	Displays ARP inspection statistics for the specified VLAN(s).	E	3
show arp inspection vlan <vlan-list>	Displays ARP inspection status for the specified VLAN(s).	E	3

Table 253 ARP Inspection Filter Commands

COMMAND	DESCRIPTION	M	P
show arp inspection filter	Displays all ARP inspection filters.	E	3
show arp inspection filter [<mac-addr>] [vlan <vlan-id>]	Displays the current list of MAC address filters that were created because the OLT identified an unauthorized ARP packet. Optionally, lists MAC address filters based on the MAC address or VLAN ID in the filter.	E	3
clear arp inspection filter	Deletes all ARP inspection filters from the OLT.	E	13
arp inspection filter-aging-time <1-2147483647>	Specifies how long (1-2147483647 seconds) MAC address filters remain in the OLT after the OLT identifies an unauthorized ARP packet. The OLT automatically deletes the MAC address filter afterwards.	C	13
no arp inspection filter-aging-time	Resets ARP inspection filter-aging time to the default value (300 seconds).	C	13
arp inspection filter-aging-time none	Specifies the MAC address filter to be permanent.	C	13
no arp inspection filter <mac-addr> vlan <vlan-id>	Deletes the MAC address filter for the specified MAC address and VLAN ID.	E	13

Table 254 ARP Inspection Log Commands

COMMAND	DESCRIPTION	M	P
show arp inspection log	Displays the log settings configured on the OLT. It also displays the log entries recorded on the OLT.	E	3
clear arp inspection log	Deletes all ARP inspection log entries from the OLT.	E	13

Table 254 ARP Inspection Log Commands (continued)

COMMAND	DESCRIPTION	M	P
arp inspection log-buffer entries <0-1024>	Specifies the maximum number (1-1024) of log messages that can be generated by ARP packets and not sent to the syslog server. If the number of log messages in the OLT exceeds this number, the OLT stops recording log messages and simply starts counting the number of entries that were dropped due to unavailable buffer.	C	13
arp inspection log-buffer logs <0-1024> interval <0-86400>	Specifies the number of syslog messages that can be sent to the syslog server in one batch and how often (1-86400 seconds) the OLT sends a batch of syslog messages to the syslog server.	C	13
no arp inspection log-buffer entries	Resets the maximum number (1-1024) of log messages that can be generated by ARP packets and not sent to the syslog server to the default value.	C	13
no arp inspection log-buffer logs	Resets the maximum number of syslog messages the OLT can send to the syslog server in one batch to the default value.	C	13

Table 255 Interface ARP Inspection Commands

COMMAND	DESCRIPTION	M	P
show arp inspection interface port-channel <aid>	Displays the ARP inspection settings for the specified port(s). aid: <pon eth>-<port>	E	3
interface port-channel <aid>	Enters config-interface mode for the specified port(s). aid: <pon eth>-<port>	C	13
arp inspection limit rate <0-2048>	Configures the rate limit of ARP inspection.	C	13
arp inspection limit rate <0-2048> burst interval <seconds>	Enter the length (1-15 seconds) of the burst interval. The burst interval is the length of time over which the rate of ARP packets is monitored for each port. For example, if the rate is 15 pps and the burst interval is 1 second, then the OLT accepts a maximum of 15 ARP packets in every one-second interval. If the burst interval is 5 seconds, then the OLT accepts a maximum of 75 ARP packets in every five-second interval.	C	13
arp inspection trust	Sets the port to be a trusted port for arp inspection. The OLT does not discard ARP packets on trusted ports for any reason.	C	13
no arp inspection trust	Disables this port from being a trusted port for ARP inspection.	C	13
exit	Leaves the interface configuration sub-command mode.	C	13

Table 256 ARP Inspection VLAN Commands

COMMAND	DESCRIPTION	M	P
show arp inspection vlan <vlan-list>	Displays ARP inspection settings for the specified VLAN(s).	E	3
arp inspection vlan <vlan-list>	Enables ARP inspection on the specified VLAN(s).	C	13
no arp inspection vlan <vlan-list>	Disables ARP inspection on the specified VLAN(s).	C	13
arp inspection vlan <vlan-list> logging [all none permit deny]	Enables logging of ARP inspection events on the specified VLAN(s). Optionally specifies which types of events to log.	C	13
no arp inspection vlan <vlan-list> logging	Disables logging of messages generated by ARP inspection for the specified VLAN(s).	C	13

Table 257 ARP Learning Commands

COMMAND	DESCRIPTION	M	P
interface port-channel <aid>	Enters config-interface mode for the specified port(s). aid: <pon eth>-<port>	C	13
arp-learning <arp-reply gratuitous-arp arp-request>	Sets the ARP learning mode for the specified port(s).	C	13
no arp-learning	Resets the ARP learning mode to the default value (arp-reply).	C	13
exit	Leaves the interface configuration sub-command mode.	C	13

72.6 ARP Inspection Command Examples

This example looks at the current list of MAC address filters that were created because the OLT identified an unauthorized ARP packet. When the OLT identifies an unauthorized ARP packet, it automatically creates a MAC address filter to block traffic from the source MAC address and source VLAN ID of the unauthorized ARP packet.

```
sysname# show arp inspection filter
Filtering aging timeout : 300

      MacAddress    VLAN    Port    Expiry (sec)      Reason
-----  -----  -----  -----  -----
Total number of bindings: 0
```

The following table describes the labels in this display.

Table 258 show arp inspection filter

LABEL	DESCRIPTION
Filtering aging timeout	This field displays how long the MAC address filters remain in the OLT after the OLT identifies an unauthorized ARP packet. The OLT automatically deletes the MAC address filter afterwards.
MacAddress	This field displays the source MAC address in the MAC address filter.
VLAN	This field displays the source VLAN ID in the MAC address filter.
Port	This field displays the source port of the discarded ARP packet.
Expiry (sec)	This field displays how long (in seconds) the MAC address filter remains in the OLT. You can also delete the record manually (Delete).
Reason	<p>This field displays the reason the ARP packet was discarded.</p> <p>MAC+VLAN: The MAC address and VLAN ID were not in the binding table.</p> <p>IP: The MAC address and VLAN ID were in the binding table, but the IP address was not valid.</p> <p>Port: The MAC address, VLAN ID, and IP address were in the binding table, but the port number was not valid.</p>

This example looks at log messages that were generated by ARP packets and that have not been sent to the syslog server yet.

```
sysname# show arp inspection log
Total Log Buffer Size : 32
Syslog rate : 5 entries per 1 seconds

Port  Vlan          Sender MAC        Sender IP   Pkts      Reason
      Time
-----  -----  -----  -----  -----  -----  -----
-----  -----  -----  -----  -----  -----  -----
Total number of logs: 0
```

The following table describes the labels in this display.

Table 259 show arp inspection log

LABEL	DESCRIPTION
Total Log Buffer Size	<p>This field displays the maximum number (1-1024) of log messages that were generated by ARP packets and have not been sent to the syslog server yet.</p> <p>If the number of log messages in the OLT exceeds this number, the OLT stops recording log messages and simply starts counting the number of entries that were dropped due to unavailable buffer.</p>
Syslog rate	This field displays the maximum number of syslog messages the OLT can send to the syslog server in one batch. This number is expressed as a rate because the batch frequency is determined by the Log Interval .
Port	This field displays the source port of the ARP packet.
Vlan	This field displays the source VLAN ID of the ARP packet.
Sender MAC	This field displays the source MAC address of the ARP packet.
Sender IP	This field displays the source IP address of the ARP packet.

Table 259 show arp inspection log (continued)

LABEL	DESCRIPTION
Pkts	This field displays the number of ARP packets that were consolidated into this log message. The OLT consolidates identical log messages generated by ARP packets in the log consolidation interval into one log message.
Reason	This field displays the reason the log message was generated. dhcp deny: An ARP packet was discarded because it violated a dynamic binding with the same MAC address and VLAN ID. static deny: An ARP packet was discarded because it violated a static binding with the same MAC address and VLAN ID. deny: An ARP packet was discarded because there were no bindings with the same MAC address and VLAN ID. static permit: An ARP packet was forwarded because it matched a static binding. dhcp permit: An ARP packet was forwarded because it matched a dynamic binding.
Time	This field displays when the log message was generated.
Total number of logs	This field displays the number of log messages that were generated by ARP packets and that have not been sent to the syslog server yet. If one or more log messages are dropped due to unavailable buffer, there is an entry called overflow with the current number of dropped log messages.

This example displays whether ports are trusted or untrusted ports for ARP inspection.

```
sysname# show arp inspection interface port-channel pon-1
Interface Trusted State Rate (pps) Burst Interval
-----
pon-1 Untrusted 15 1
```

The following table describes the labels in this display.

Table 260 show arp inspection interface port-channel

LABEL	DESCRIPTION
Interface	This field displays the port number. If you configure the * port, the settings are applied to all of the ports.
Trusted State	This field displays whether this port is a trusted port (Trusted) or an untrusted port (Untrusted). Trusted ports are connected to DHCP servers or other switches, and the switch discards DHCP packets from trusted ports only if the rate at which DHCP packets arrive is too high.
Rate (pps)	This field displays the maximum number for DHCP packets that the switch receives from each port each second. The switch discards any additional DHCP packets.
Burst Interval	This field displays the length of time over which the rate of ARP packets is monitored for each port. For example, if the Rate is 15 pps and the burst interval is 1 second, then the switch accepts a maximum of 15 ARP packets in every one-second interval. If the burst interval is 5 seconds, then the switch accepts a maximum of 75 ARP packets in every five-second interval.

CHAPTER 73

VoIP

73.1 VoIP Overview

Use the VoIP commands to configure VoIP on an ONT (Such as the PMG5318) through OMCI.

73.2 VoIP Common Profile Commands

The following table lists the commands for configuring profiles of common VoIP settings.

Table 261 VoIP Common Profile Commands

COMMAND	DESCRIPTION	M	P
<code>voip-common-profile <name></code>	Creates the specified profile of common VoIP settings (1 to 15 character name) and enters the sub-command mode for configuring it. Common VoIP settings can be shared by multiple subscribers.	C	13
<code>1st-codec <encoding name></code>	Specifies the first audio codec to tell the remote ONT. The remote ONT must use the same codec as the peer. Here are the options, encoding names, and clock rates (in Hz). See RFC 3551 for more details. PCM: PCMU, 8000 GSM: GSM, 8000 G723: G.723, 8000 DVI4-8000: DVI4, 8000 DVI4-16000: DVI4, 16000 LPC: LPC, 8000 PCMA: PCMA, 8000	C	13

Table 261 VoIP Common Profile Commands (continued)

COMMAND	DESCRIPTION	M	P
	G722: G.722, 8000 L16-2: L16, 2 channels, 44100 L16-1: L16, 1 channel, 44100 QCELP: QCELP, 8000 CN: CN, 8000 MPA: MPA, 90000 G728: G.728, 8000 DVI4-11025: DVI4, 11025 DVI4-22050: DVI4, 22050 G729: G.729, 8000	C	13
1st-codec help	Provides more information about the specified command.	C	13
no 1st-codec	Sets the first audio codec to the default.	C	13
1st-packet-period <ms time>	Specifies the first packet period selection interval (in milliseconds). This value is useful when the media gateway controller does not provide the preferred compression algorithm and packet period parameter to the ONT. The range depends on the type of codec selected. ms time: 10-30	C	13
no 1st-packet-period <cr>	Sets the first packet period selection interval to the default.	C	13
1st-silence <enable disable>	Turns the use of silence suppression with the first codec on or off.	C	13
no 1st-silence <cr>	Sets the use of silence suppression with the first codec to the default.	C	13
2nd-codec <encoding name>	Specifies the second audio codec to tell the remote ONT. The remote ONT must use the same codec as the peer. The options are the same as described for the first codec.	C	13
2nd-codec help	Provides more information about the specified command.	C	13
no 2nd-codec <cr>	Sets the second audio codec to the default.	C	13
2nd-packet-period <ms time>	Specifies the second packet period selection interval (in milliseconds). This value is useful when the media gateway controller does not provide the preferred compression algorithm and packet period parameter to the ONT. The range depends on the type of codec selected. ms time: 10-30	C	13
no 2nd-packet-period <cr>	Sets the second packet period selection interval to the default.	C	13
2nd-silence <enable disable>	Turns the use of silence suppression with the second codec on or off.	C	13
no 2nd-silence <cr>	Sets the use of silence suppression with the second codec to the default.	C	13

Table 261 VoIP Common Profile Commands (continued)

COMMAND	DESCRIPTION	M	P
3rd-codec <encoding name>	Specifies the third audio codec to tell the remote ONT. The remote ONT must use the same codec as the peer. The options are the same as described for the first codec.	C	13
3rd-codec help	Provides more information about the specified command.	C	13
no 3rd-codec <cr>	Sets the third audio codec to the default.	C	13
3rd-packet-period <ms time>	Specifies the third packet period selection interval (In milliseconds). This value is useful when the media gateway controller does not provide the preferred compression algorithm and packet period parameter to the ONT. The range depends on the type of codec selected. ms time: 10-30	C	13
no 3rd-packet-period <cr>	Sets the third packet period selection interval to the default.	C	13
3rd-silence <enable disable>	Turns the use of silence suppression with the third codec on or off.	C	13
no 3rd-silence <cr>	Sets the use of silence suppression with the third codec to the default.	C	13
4th-codec <encoding name>	Specifies the fourth audio codec to tell the remote ONT. The remote ONT must use the same codec as the peer. The options are the same as described for the first codec.	C	13
4th-codec help	Provides more information about the specified command.	C	13
no 4th-codec <cr>	Sets the fourth audio codec to the default.	C	13
4th-packet-period <ms time>	Specifies the fourth packet period selection interval (In milliseconds). This value is useful when the media gateway controller does not provide the preferred compression algorithm and packet period parameter to the ONT. The range depends on the type of codec selected. ms time: 10-30	C	13
no 4th-packet-period <cr>	Sets the fourth packet period selection interval to the default.	C	13
4th-silence <enable disable>	Turns the use of silence suppression with the fourth codec on or off.	C	13
no 4th-silence <cr>	Sets the use of silence suppression with the fourth codec to the default.	C	13
announce-type <action>	Sets the treatment for when a subscriber goes off-hook. Here are the options and what they represent. action: <ul style="list-style-type: none">• silence: Silence• reo-ton: Reorder tone• fas-ton: Fast busy• voi-ann: Voice announcement	C	13
announce-type help	Provides more information about the specified command.	C	13

Table 261 VoIP Common Profile Commands (continued)

COMMAND	DESCRIPTION	M	P
no announce-type <cr>	Sets the treatment for when a subscriber goes off-hook to the default.	C	13
cas <enable disable>	Enables or disables handling of DTMF via RTP cas events as defined in RFC 4733.	C	13
no cas <cr>	Sets the handling of DTMF via RTP cas events to the default.	C	13
dscp-mark <0~63>	Specifies the Diffserv code point (From 0 to 63) to use for outgoing RTP packets.	C	13
no dscp-mark <cr>	Removes the configuration of the Diffserv code point (from 0 to 63) to use for outgoing RTP packets.	C	13
dtmf <enable disable>	Enables or disables handling of DTMF via RTP DTMF events as defined in RFC 4733.	C	13
no dtmf <cr>	Sets whether or not the ONT handles DTMF via RTP DTMF events to the default.	C	13
echo-cancel <enable disable>	Enables or disables echo cancellation.	C	13
no echo-cancel <cr>	Restores the default echo cancellation setting.	C	13
fax-mode <mode>	Sets how to handle faxes. Use passthru to transmit faxes as voice (in-band). Use T38 to transmit faxes as separate packets (out-of-band) according to ITU-T T.38. mode: <passthru T38>	C	13
no fax-mode <cr>	Restores the fax handling mode to the default.	C	13
jitter-buf-max <0~500>	Sets the maximum depth (from 0 to 500) of the jitter buffer in milliseconds.	C	13
no jitter-buf-max <cr>	Restores the jitter buffer maximum depth to the default.	C	13
jitter-target <0~5000>	Sets the target value (from 0 to 5000) of the jitter buffer in milliseconds.	C	13
no jitter-target <cr>	Restores the jitter buffer target value to the default.	C	13
local-port <1~65535> <1~65535>	Sets the RTP port to use for voice traffic. <1~65535>: Specifies the base RTP port. Note that this value cannot be greater than the highest RTP port. <1~65535>: Specifies the highest RTP port. Note that this value cannot be smaller than the base RTP port.	C	13
no local-port <cr>	Restores the RTP port used for voice traffic to the default.	C	13
oob-dtmf <enable disable>	Turns out-of-band DTMF carriage on or off.	C	13
no oob-dtmf <cr>	Restores the default setting for out-of-band DTMF carriage.	C	13
piggyback <enable disable>	Turn RTP piggyback events on or off.	C	13
no piggyback <cr>	Restores the default setting for RTP piggyback events.	C	13
pstn-protocol <0~999>	Sets which variant (from 0 to 999) of POTS signalling to use on the associated UNIs.	C	13

Table 261 VoIP Common Profile Commands (continued)

COMMAND	DESCRIPTION	M	P
no pstn-protocol <cr>	Restores the default setting for which variant (from 0 to 999) of POTS signaling to use on the associated UNIs.	C	13
signalling-code <code>	Sets the signalling code: loo-str: Loop start gro-str: Ground start loo-rev: Loop reverse battery coi-fir: Coin first dia-ton: Dial tone first mul-par: Multi-party	C	13
no signalling-code <cr>	Restores the default signalling code setting.	C	13
tone <enable disable>	Turns the handling of tones through RTP tone events according to RFC 4733 on or off.	C	13
no tone <cr>	Restores the default setting for whether or not the device handles tones through RTP tone events according to RFC 4733.	C	13
exit	Leaves from the VoIP common profile configuration commands.	C	13
no voip-common-profile <name> <cr>	Removes the specified common VoIP profile.	C	13
no voip-common-profile all	Removes all common VoIP profiles.	C	13

73.3 VoIP SIP Profile Commands

The following table lists the commands for configuring VoIP SIP profiles.

Table 262 VoIP SIP Profile Commands

COMMAND	DESCRIPTION	M	P
voip-sip-profile <name>	Creates the specified profile of VoIP SIP settings (1 to 15 character name) and enters the sub-command mode for configuring it.	C	13
bridged-line-agent-uri <1~63 characters>	Sets the bridged line agent URI (from 1 to 63 characters). An interaction SIP bridge enables agents to use an IP telephone at a remote location through a TCP/IP network to a Customer Interaction Center.	C	13
no bridged-line-agent-uri <cr>	Deletes the bridged line agent URI.	C	13

Table 262 VoIP SIP Profile Commands (continued)

COMMAND	DESCRIPTION	M	P
call-present <features>	<p>Configures the list of supported call presentation features. You can specify multiple options separated by commas without spaces; for example: cal-for,dia-ton.</p> <p>spl-rin: Message waiting indication splash ring</p> <p>dia-ton: Message waiting indication special dial tone</p> <p>vis-ind: Message waiting indication visual indication</p> <p>cal-for: Call forwarding indication</p>	C	13
call-present help	Provides more information about the specified command.	C	13
no call-present <cr>	Removes the list of call presentation features.	C	13
call-prog-trans <features>	<p>Configures the list of supported features for calls that are in progress. You can select multiple options separated by commas without spaces; for example: cal-tra,cal-hol.</p> <p>3way: 3-way calling</p> <p>cal-tra: Call transfer</p> <p>cal-hol: Call hold</p> <p>cal-par: Call park</p> <p>not-dis: Do not disturb</p> <p>flash: Flash on emergency service call</p> <p>origin: Emergency service origination hold</p> <p>6way: 6-way calling</p>	C	13
call-prog-trans help	Provides more information about the specified command.	C	13
no call-prog-trans <cr>	Removes the list of features for calls in progress.	C	13
call-wait <features>	<p>Configures the list of supported call waiting features. You can select multiple options separated by commas without spaces; for example: cal-wai,cid-ann.</p> <p>cal-wai: Call waiting</p> <p>cid-ann: Caller ID announcement</p>	C	13
call-wait help	Provides more information about the specified command.	C	13
no call-wait <cr>	Removes the list of call waiting features.	C	13

Table 262 VoIP SIP Profile Commands (continued)

COMMAND	DESCRIPTION	M	P
<code>cid <features></code>	<p>Configures the list of supported caller ID (CID) features. You can select multiple options separated by commas without spaces; for example: <code>cal-nam, cid-num</code>.</p> <p><code>cal-num</code>: Calling number <code>cal-nam</code>: Calling name <code>cid-blo</code>: CID blocking (both number and name) <code>cid-num</code>: CID number <code>cid-nam</code>: CID name <code>ACR</code>: Anonymous CID blocking</p>	C	13
<code>cid help</code>	Provides more information about the specified command.	C	13
<code>no cid <cr></code>	Removes the list of caller ID features.	C	13
<code>conf-factory-uri <1~63 characters></code>	Configures the conference factory URI (from 1 to 63 characters). A conference factory generates a unique conference ID, to identify and address a conference focus, using a call signaling interface.	C	13
<code>no conf-factory-uri <cr></code>	Removes the conference factory URI.	C	13
<code>direct-con <features></code>	<p>Configures the list of direct connect features. You can select multiple options separated by commas without spaces; for example: <code>enable, dia-opt</code>.</p> <p><code>enable</code>: Direct connect feature enabled <code>dia-opt</code>: Dial tone feature delay option</p>	C	13
<code>direct-con help</code>	Provides more information about the specified command.	C	13
<code>no direct-con <cr></code>	Removes the list of direct connect features.	C	13
<code>direct-con-uri <1~63 characters></code>	Configures a direct connect URI (from 1 to 63 characters). Set a direct connect URI to use SIP to direct connect a VoIP Server.	C	13
<code>no direct-con-uri <cr></code>	Removes the direct connect URI.	C	13
<code>host-part-uri <1~63 characters></code>	Configures the host or domain part of the SIP URI (from 1 to 63 characters).	C	13
<code>no host-part-uri <cr></code>	Removes the host or domain part of the SIP URI.	C	13
<code>out-proxy-addr <1~63 characters></code>	Configures an out-band proxy IP address or URI (from 1 to 63 characters).	C	13
<code>no out-proxy-addr <cr></code>	Removes the outband proxy IP address or URI.	C	13
<code>pri-dns <ip></code>	Configures the IP address of the primary DNS server for SIP (input an IP).	C	13
<code>no pri-dns <cr></code>	Removes the IP address of the primary DNS server for SIP.	C	13
<code>proxy-service-addr <1~63 characters></code>	Configures the IP address or URI (from 1 to 63 characters) of a proxy service.	C	13
<code>no proxy-service-addr <cr></code>	Removes the proxy service IP address or URI.	C	13

Table 262 VoIP SIP Profile Commands (continued)

COMMAND	DESCRIPTION	M	P
reg-exp-time <0~25200>	Configures the SIP registration expiration time (from 0 to 25200 seconds).	C	13
no reg-exp-time <cr>	Removes the SIP registration expiration time setting.	C	13
registrar <1~63 characters>	Configures the IP address or URI (from 1 to 63 characters) of a registrar server.	C	13
no registrar <cr>	Removes the registrar server IP address or URI.	C	13
rereg-head-start-time <0~720>	Configures the SIP re-registration head start time (from 0 to 720 seconds).	C	13
no rereg-head-start-time <cr>	Removes the SIP re-registration head start time.	C	13
sec-dns <ip>	Configures the IP address of the secondary DNS server for SIP (input an IP).	C	13
no sec-dns <cr>	Removes the IP address of the secondary DNS server for SIP.	C	13
softswitch <four ascii code>	Configures the SIP gateway soft switch vendor name code (4 characters).	C	13
no softswitch <cr>	Removes the SIP gateway softswitch vendor name code.	C	13
exit	Leaves from the VoIP SIP configuration commands.	C	13
no voip-sip-profile <name> <cr>	Removes the specified VoIP SIP profile.	C	13
no voip-sip-profile all	Removes all VoIP SIP profiles.	C	13

73.4 VoIP Dial Plan Profile Commands

The following table lists the commands for configuring VoIP dial plan profiles.

Table 263 VoIP Dial Plan Profile Commands

COMMAND	DESCRIPTION	M	P
voip-dial-plan <name>	Creates the VoIP dial plan profile (1 to 15 character name) and enters the sub-command mode for configuring it.	C	13
common-set max-size <1 ~ 256> critical-dial-timeout <0 ~ 8000> partial-dial-timeout <0 ~ 32000> format <format>	Sets the dial plan table's common configuration settings. These include the maximum number (from 1 to 256) of dial plans, critical-dial-timeout (from 0 to 8000 milliseconds), partial-dial-timeout (from 0 to 32000 milliseconds) and format. The format options: not-def: Not defined h248: H.248 format with specific plan (table entries define the dialing plan) NSC: NSC format ven-spe: Vendor specific format	C	13
no common-set	Restores the dial plan table's default common configuration settings.	C	13

Table 263 VoIP Dial Plan Profile Commands (continued)

COMMAND	DESCRIPTION	M	P
<code>content-table <1 ~ 4> <token></code>	<p>Configures a dialing token (rule) in the dial plan table.</p> <p>Identify a dial plan table entry number (from 1 to 4) and dial plan rule (from 1 to 28 characters).</p> <p>Dial plan rules: Symbols, and Descriptions:</p> <p>Multiple Rule: , Use " " to separate multiple rules.</p> <p>Any one numeric digit: x, Allow the user to input any numeric digit (0~9), one 'x' means one digit</p> <p>A subset of keys: [], Allow the user to input a range of digits, for example: [1-3] or [148]</p> <p>Repeat: .., Allow the user to input a repeatable digit (above 0 times). For example: (12.) allows 1, 12, 122, and 1222.</p> <p>Append: <:123>, Append '123' digits in the place of the rule.</p> <p>Remove: <123:>, Remove '123' digits in the place of the rule.</p> <p>Replace: <123:456>, Replace '123' digits with '456' digits in the place of the rule.</p> <p>Block: !, Type '!' at the end of the rule, to block the number which matches the rule.</p> <p>Wait Timeout to Dial: T, Type 'T' at the end of the rule, once the dialed number is input, the call is dialed out after the timeout.</p> <p>Gateway: =gw0=,=gw3=, Type one of these at the end of the rule and when a dialed number matches the rule, the device transfers the call to the gateway (0: FXS port; 3: SIP).</p>	C	13
<code>no content-table <cr></code>	Delete all dialing tokens (rule) from the dial plan table.	C	13
<code>exit</code>	Leaves from the VoIP dial plan configuration commands.	C	13
<code>no voip-dial-plan <name> <cr></code>	Removes the specified VoIP dial plan profile.	C	13
<code>no voip-dial-plan all</code>	Removes all VoIP dial plan profiles.	C	13

73.4.1 Dial Plan Rule Details

A dial plan defines the dialing patterns, such as the length and range of the digits for a telephone number. It also includes country codes, access codes, area codes, local numbers, long distance numbers or international call prefixes. For example, the dial plan ([2-9]xxxxxx) does not allow a local number which begins with 1 or 0.

Without a dial plan, users have to manually enter the callee's whole number and wait for the specified dialing interval to time out or press a terminator key (usually the pound key on the phone keypad) before the VoIP device makes the call.

The VoIP device initializes a call when the dialed number matches any one of the rules in the dial plan. Dial plan rules follow these conventions:

- Rules are separated by the | (bar) symbol.
- "x" stands for a wildcard and can be any digit from 0 to 9.
- A subset of keys is in a square bracket []. Ranges are allowed.

For example, [359] means a number matching this rule can be 3, 5 or 9. [26-8*] means a number matching this rule can be 2, 6, 7, 8 or *.

- The dot “.” appended to a digit allows the digit to be ignored or repeated multiple times. Any digit (0~9, *, #) after the dot will be ignored.

For example, (01.) means a number matching this rule can be 0, 01, 0111, 01111, and so on.

- <dialed-number:translated-number> indicates the number after the colon replaces the number before the colon in an angle bracket <>. For example,

(<:1212> xxxxxxx) means the VoIP device automatically prefixes the translated-number "1212" to the number you dialed before making the call. You can use this for local calls in the US.

(<9:> xxx xxxxxxx) means the VoIP device automatically removes the specified prefix "9" from the number you dialed before making the call. Use this for making outside calls from an office.

(xx<123:456>xxxx) means the VoIP device automatically translates "123" to "456" in the number you dialed before making the call.

- Calls with a number followed by the exclamation mark "!" will be dropped.
- Calls with a number followed by the termination character "@" will be made immediately. Any digit (0~9, *, #) after the @ character will be ignored.
- Gateway: Type "=gw0=" or "=gw3=" at the end of the rule. If the number matches the call will be transferred to a gateway (0: FXS port; 3: SIP).

In this example dial plan (0 | [49]11 | 1 [2-9]xx xxxxxxxx | 1 947 xxxxxxx !), you can dial "0" to call the local operator, call 411 or 911, or make a long distance call with an area code starting from 2 to 9 in the US. The calls with the area code 947 will be dropped.

73.5 UNI Port VoIP Service Settings

The following table lists the commands for configuring VoIP service settings for a subscriber port on the remote ONT. The remote ONT must also support the VoIP services you configure for it.

Table 264 UNI Port VoIP Service Commands

COMMAND	DESCRIPTION	M	P
remote uniport <aid>	Configures UNI port settings. <i>aid</i> : uniport-<pon>-<ont>-<card>-<port>	C	13
voip-service mode sip vlan <vid> common-profile <common-profile-name> sip-profile <sip-profile-name> [dial-plan <name>] [username <name>] [password <password>] [aor <uri>] [disp-name <name>] [vmail-uri <uri>] [vmail-extimer <0~3600>] [release-timer <0~30>] [roh-timer <0~30>]	Configures UNI port VoIP settings. mode: sip mode (SIP) is supported. vlan: Specify the VLAN ID (1 to 4094) for the UNI port to use for VoIP traffic. common-profile: Specify the name of an existing SIP common profile. sip-profile: Specify the name of an existing SIP profile. dial-plan: Specify the name of an existing dial plan table. username: The username (from 1 to 25 characters) for VoIP authentication. password: The password (from 1 to 25 characters) for VoIP authentication. aor: The user identification part of the address of record (from 1 to 63 characters). disp-name: The customer ID used for the display attribute in outgoing SIP messages (from 1 to 25 characters). vmail-uri: The IP address or URL (from 1 to 63 characters) of the SIP voicemail server for signaling messages. vmail-extimer: The voicemail subscription expiration time (from 0 to 3600) in seconds (default 3600). release-timer: The release timer (from 0 to 30) defined in seconds (default 10). roh-timer: The time (from 0 to 30) in seconds for deciding the receiver is off hook (default is 15).	C	13
voip-service help	Provides more information about the specified command.	C	13
no voip <cr>	Removes the VoIP service on the specified UNI port.	C	13

73.6 VoIP Show Commands

The following table lists the commands for displaying VoIP settings and status.

Table 265 VoIP Show Commands

COMMAND	DESCRIPTION	M	P
show voip-common-profile	Displays the settings of the VoIP common profiles.	E	13
show voip-dial-plan	Displays the settings of the VoIP dial plan profiles.	E	13
show voip-sip-profile	Displays the settings of the VoIP SIP profiles.	E	13
show remote uniport <aid> vlan	Displays the specified remote ONT UNI port's VLAN status. <i>aid: uniport-<pon>-<ont>-<card>-<uniport></i>	E	13
show remote uniport <aid> voip	Displays the specified remote ONT UNI port's VoIP status. <i>aid: uniport-<pon>-<ont>-<card>-<uniport></i>	E	13

73.7 VoIP Configuration Supported on the PMG5318

The following table lists the VoIP configuration the PMG5318 can support.

Table 266 VoIP Configuration Supported on the PMG5318

COMMAND	DESCRIPTION	M	P
voip-common-profile <name>	Creates the specified profile of common VoIP settings (1 to 15 character name) and enters the sub-command mode for configuring it. You do not actually configure any common VoIP settings for the PMG5318 though. You just need a VoIP common profile name to specify when you configure VoIP service settings for the PMG5318 subscriber port.	C	13
voip-sip-profile <name>	Creates the specified profile of VoIP SIP settings (1 to 15 character name) and enters the sub-command mode for configuring it.	C	13
registrar <1~63 characters>	Configures the IP address or URI (from 1 to 63 characters) of a registrar server.	C	13
voip-dial-plan <name>	Creates the VoIP dial plan profile (1 to 15 character name) and enters the sub-command mode for configuring it.	C	13

Table 266 VoIP Configuration Supported on the PMG5318 (continued)

COMMAND	DESCRIPTION	M	P
<code>common-set max-size <1 ~ 256> critical-dial-timeout <0 ~ 8000> partial-dial-timeout <0 ~ 32000> format <format></code>	<p>Sets the dial plan table's common configuration settings.</p> <p>These include the maximum number (from 1 to 256) of dial plans, critical-dial-timeout (from 0 to 8000 milliseconds), partial-dial-timeout (from 0 to 32000 milliseconds) and format. The format options:</p> <ul style="list-style-type: none"> not-def: Not defined h248: H.248 format with specific plan (table entries define the dialing plan) NSC: NSC format ven-spe: Vendor specific format 	C	13

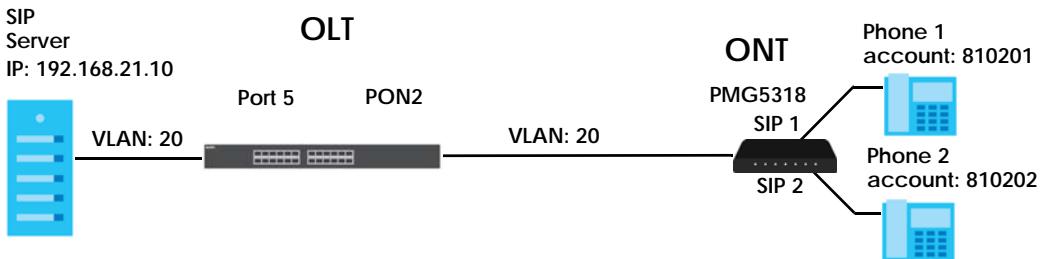
Table 266 VoIP Configuration Supported on the PMG5318 (continued)

COMMAND	DESCRIPTION	M	P
<code>content-table <1 ~ 4> <token></code>	<p>Configures a dialing token (rule) in the dial plan table.</p> <p>Identify a dial plan table entry number (from 1 to 4) and dial plan rule (from 1 to 28 characters).</p> <p>Dial plan rules: Symbols, and Descriptions:</p> <p>Multiple Rule: , Use " " to separate multiple rules.</p> <p>Any one numeric digit: x, Allow the user to input any numeric digit (0~9), one 'x' means one digit</p> <p>A subset of keys: [], Allow the user to input a range of digits, for example: [1-3] or [148]</p> <p>Repeat: .., Allow the user to input a repeatable digit (above 0 times). For example: (12.) allows 1, 12, 122, and 1222.</p> <p>Append: <:123>, Append '123' digits in the place of the rule.</p> <p>Remove: <123:>, Remove '123' digits in the place of the rule.</p> <p>Replace: <123:456>, Replace '123' digits with '456' digits in the place of the rule.</p> <p>Block: !, Type '!' at the end of the rule, to block the number which matches the rule.</p> <p>Wait Timeout to Dial: T, Type 'T' at the end of the rule, once the dialed number is input, the call is dialed out after the timeout.</p> <p>Gateway: =gw0=,=gw3=, Type one of these at the end of the rule and when a dialed number matches the rule, the device transfers the call to the gateway (0: FXS port; 3: SIP).</p>	C	13
<code>voip-service mode sip vlan <1-4094> common-profile <name> sip-profile <name> [dial-plan <name>] [username <name>] [password <password>]</code>	<p>Configures UNI port VoIP settings.</p> <p>mode: sip mode (SIP) is supported.</p> <p>vlan: Specify the VLAN ID (1 to 4094) the UNI port should use for VoIP traffic.</p> <p>common-profile: Specify the name of an existing SIP common profile.</p> <p>sip-profile: Specify the name of an existing SIP profile.</p> <p>dial-plan: Specify the name of an existing dial plan table.</p> <p>username: The username (from 1 to 25 characters) for VoIP authentication.</p> <p>password: The password (from 1 to 25 characters) for VOIP authentication.</p>	C	13

73.8 ONT Subscriber VoIP Port Provisioning Example

The VoIP function is on the ONT, not the OLT. The OLT uses OMCI to configure VoIP settings on the ONT. The ONT must support receiving VoIP configuration by OMCI.

Figure 234 PMG5318 VoIP Example Overview



This example uses VLAN 20 for VoIP traffic and configures **PON2** to link to a PMG5318 and port 5 as an uplink port that links to a SIP server at IP address 192.168.21.10.

- Configure a VLAN 20 with **PON2** and port 5 uplink port as fixed members.

```

sysname# config
sysname(config)# vlan 20
sysname(config-vlan)# fixed pon-2
sysname(config-vlan)# fixed eth-5
sysname(config-vlan)# untagged eth-5
sysname(config-vlan)# exit
sysname(config)# exit
    
```

- Configure the QoS bandwidth and ingress profiles.

- bwprof:** configure a “100m” QoS bandwidth profile that sets the SIR to 10240 kbps and limits the AIR to 10240 kbps and the PIR to 102400 kbps.
- ingprof:** configure a “alltc1” QoS ingress profile to map IEEE 802.1p tags 0 to 7 to traffic class 1.

```

sysname# config
sysname(config)# qos bwprof 100m sir 10240 air 10240 pir 102400
sysname(config)# qos ingprof alltc1 dot1p0tc 1 dot1p1tc 1 dot1p2tc 1 dot1p3tc 1
dot1p4tc 1 dot1p5tc 1 dot1p6tc 1 dot1p7tc 1
sysname(config)# exit
    
```

- Configure VoIP SIP, common, and dial plan profiles.

- The “sip” VoIP SIP profile sets 192.168.21.10 as the registrar server’s IP address.
- Create the “common” VoIP common profile without any settings.
- Create the “dial” plan profile with an entry that defines the following dialing rules:
 - The first rule is before the | (bar) symbol. It has the PMG5318 dial a call when users dial a 1 followed by any number of digits from 0 to 9, an asterisks (*), any number of digits from 0 to 9, and the pound key (#).

- The second rule is between the | symbols. It has the PMG5318 dial a call when users dial a hash symbol (#) followed by any number of digits from 0 to 9, an asterisks (*), any number of digits from 0 to 9, and the pound key twice (##).
- The third rule comes after the second | symbol. It has the PMG5318 dial a call when users dial the pound key (#) followed by any number of digits from 0 to 9, an asterisks (*), and any number of digits from 0 to 9.

```
sysname# config
sysname(config)# voip-sip-profile sip
sysname(config-voip-sip-prof)# registrar 192.168.21.10
sysname(config-voip-sip-prof)# exit
sysname(config)# voip-common-profile common
sysname(config-com-prof)# exit
sysname(config)# voip-dial-plan dial
sysname(config-dial-plan-prof)# content 1 X*.X.#|#X.*.X.##|#X.*.X.
sysname(config-dial-plan-prof)# exit
sysname(config)# exit
```

- 4** Set the PON port's register method for how the OLT registers ONTs connected to the port (A in this example) and the PON port's transceiver type (12 in this example). Then enable the PON port.

```
sysname# config
sysname(config)# interface olt pon-2
sysname(config-olt)# register-method A
sysname(config-olt)# transceiver 12
sysname(config-olt)# no inactive
sysname(config-olt)# exit
sysname(config)# exit
```

- 5** Configure the remote ONT's provisioning and bandwidth group settings. (When you configure "remote ONT" settings, the OLT configures the ONT with those settings.)

- Port 2, and sets the ONT's ID to 1.
- sn: serial number, 5A59584517035116 in this example.
- pa: password, 44454641554C54000000 in this example.
- Enable the ONT.
- bwgroup: number 1 in this example.
 - usbwprofilename: this example uses the 100m bandwidth profile for upstream traffic.
 - dsbwprofilename: this example uses the 100m bandwidth profile for downstream traffic.

```
sysname# config
sysname(config)# remote ont ont-2-1
sysname(config-ont)# sn 5A59584517035116
sysname(config-ont)# password 44454641554C54000000
sysname(config-ont)# no inactive
sysname(config-ont)# bwgroup 1 usbwprofilename 100m dsbwprofilename 100m
sysname(config-ont)# exit
sysname(config)# exit
```

- 6** Configure VLAN flow and VoIP service settings for the UNI (subscriber) port on the remote ONT.

- The subscriber User Network Interface (UNI) port at port 2, ONT 1, card 2, card port 1.
- QoS queue: configure QoS settings to apply to a specific traffic class.

- tc: traffic class 0-7 to which to apply this queue, 1 in this example.
- priority: 0-7 to apply to the traffic class, 2 in this example.
- weight 0-255 to use for the traffic class, 2 in this example.
- usbwprofilename: the bandwidth profile for the traffic class's upstream traffic (100m here).
- dsbwprofilename: the bandwidth profile for the traffic class's downstream traffic (100m here).
- bwsharegroupid: this example uses bandwidth group ID 1.
- VLAN settings:
 - VLAN: apply this command's QoS ingress profile to UNI VLAN 20 traffic.
 - ingprof: apply the alltc1 QoS ingress profile to apply to the VLAN's traffic.

```
sysname# config
sysname(config)# remote uniport uniport-2-1-2-1
sysname(config-uniport)# queue tc 1 priority 2 weight 2 usbwprofilename 100m
dsbwprofilename 100m bwsharegroupid 1
sysname(config-uniport)# vlan 20 ingprof alltc1
sysname(config-uniport)# exit
sysname(config)# exit
```

73.8.1 Show the OLT VoIP Setup and Status

- 1 Display the VoIP SIP profile configuration.

Profile Name : [sip]	
configured	enable
proxy service address	No set
outband proxy address	No set
primary dns	No set
secondary dns	No Set
registration expiration time(sec)	3600
re-registerion head start time(sec)	360
host part uri	No set
sip registrar	192.168.21.10
softswitch	No set
caller id	No set
call waiting	No set
call progress or transfer	No set
call presentation	No set
direction connect	No set
direction connect uri	No set
bridged line agent uri	No set
conference factory uri	No set

- 2 Display the VoIP dial plan profile configuration.

```
sysname# show voip-dial-plan-profile
Dial Plan Name : [dial]
+-----+
| configured| max size| critical timeout| partial timeout| format|
+-----+
| enable| 256| 8000| 32000| not-def|
+-----+
| id| token|
+-----+
| 1| X*.X.#|#X.*.X.##|#X.*.X.|
+-----+
```

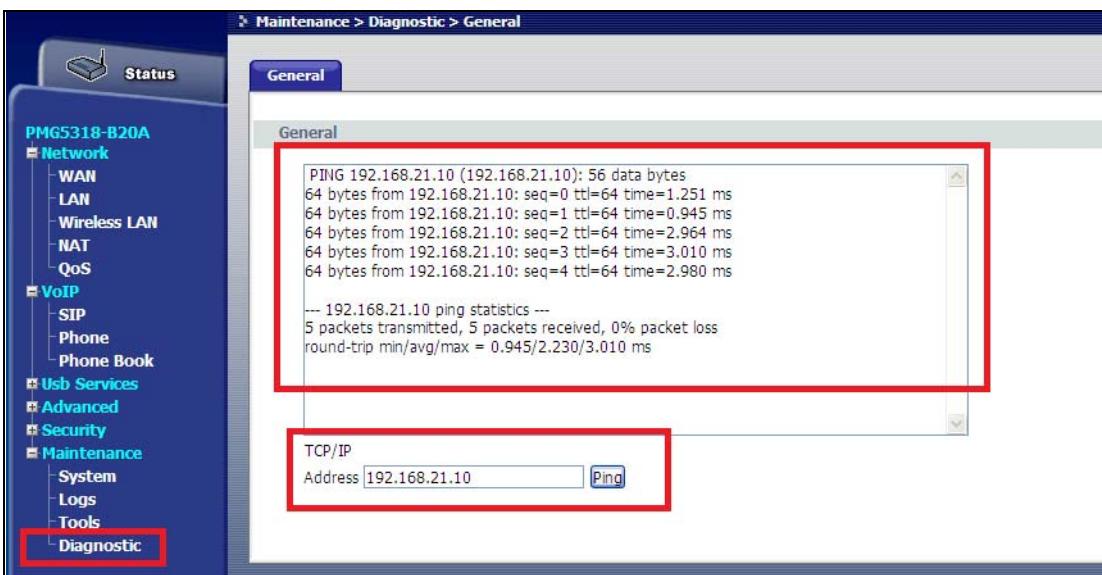
- 3 Display the VoIP common profile configuration.

```
sysname# show voip-common-profile
Profile Name : [common]
+-----+
|configured| enable
|min local port| 65535
|max local port| 65535
|dscp mark| 0
|piggyback| disable
|tone| disable
|dtmf| disable
|cas| disable
|jitter target| 60
|max jitter buffer| 135
|pstn protocol| 0
|announce type| fas-bus
|echo cancel| enable
|fax mode| passthru
|1st codec| PCMU
|2nd codec| PCMU
|3rd codec| PCMU
|4th codec| PCMU
|1st packet period| 20
|2nd packet period| 20
|3rd packet period| 20
|4th packet period| 20
|1st silence| disable
|2nd silence| disable
|3rd silence| disable
|4th silence| disable
|oob dtmf| disable
|signal code| loo-str
+-----+
```

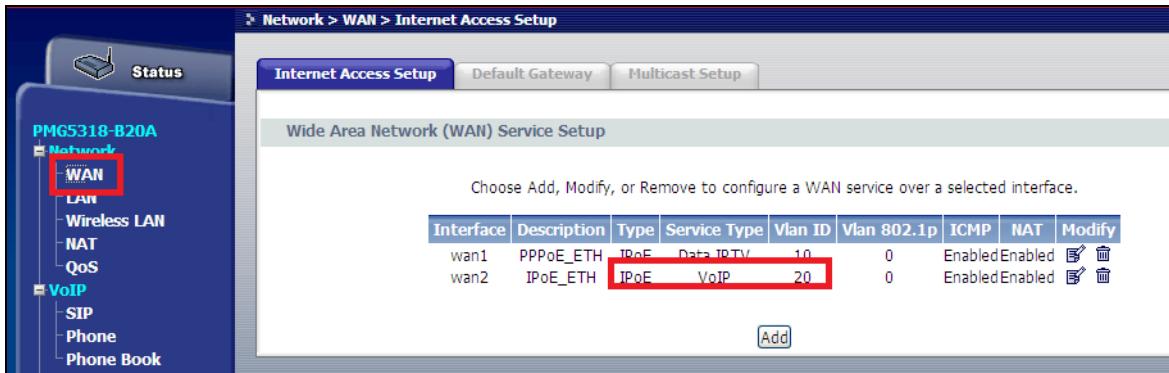
73.9 PMG5318 VoIP Setup Example

Do the following in the PMG5318's Web Configurator screens to make sure it works for VoIP.

- 1** Click **Maintenance > Diagnostic** and ping the SIP server at 192.168.21.10.



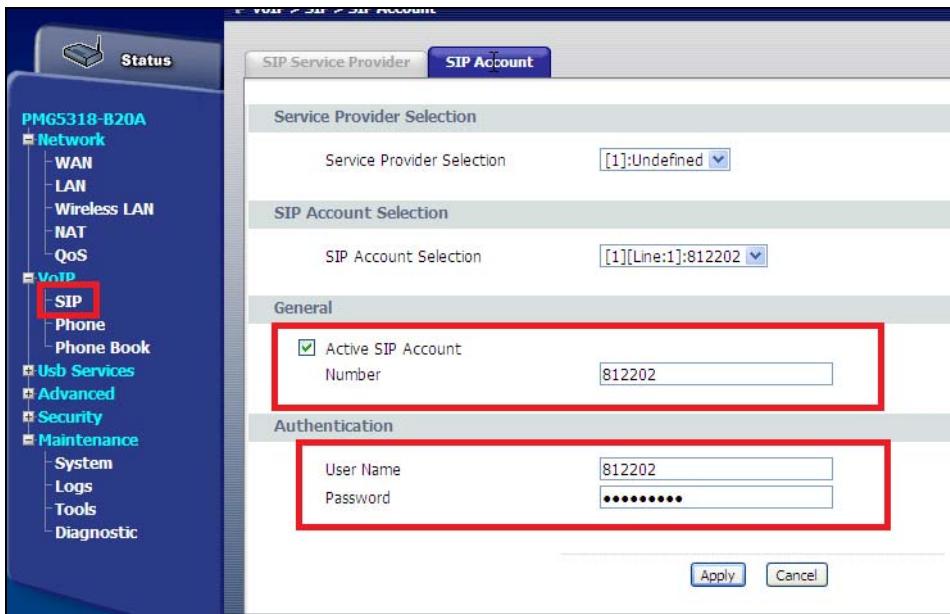
- 2 Click **Network > WAN** and configure a WAN interface with **Type** set to **IPoE**, **Service Type** set to **VoIP**, and **Vlan ID** 20.



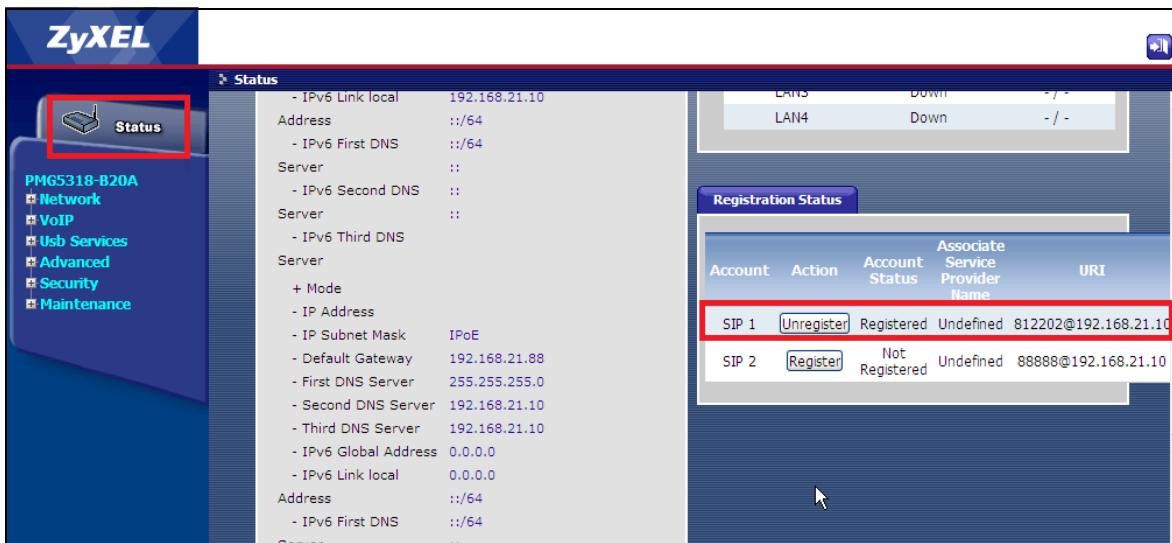
- 3 Click **VoIP > SIP** and check the SIP server address settings.



- 4 Click **VoIP > SIP > SIP Account** and check that the SIP account is active. Check that the SIP account number, user name and password are configured (these depend on the SIP server's configuration).



- 5 Click **Status** and check the account status. It displays **Registered** if the PMG5318 can register the SIP account with the SIP server.



CHAPTER 74

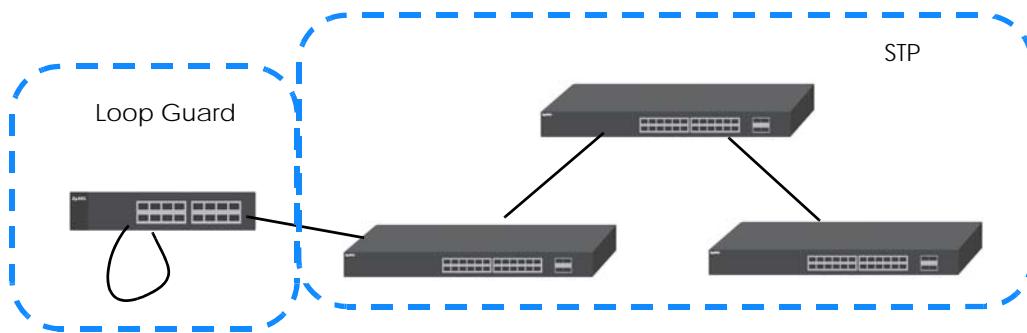
Loop Guard

This chapter shows you how to configure the OLT to guard against loops on the edge of your network.

74.1 Loop Guard Overview

Loop guard allows you to configure the OLT to shut down a port if it detects that packets sent out on that port loop back to the OLT. 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 235 Loop Guard vs STP

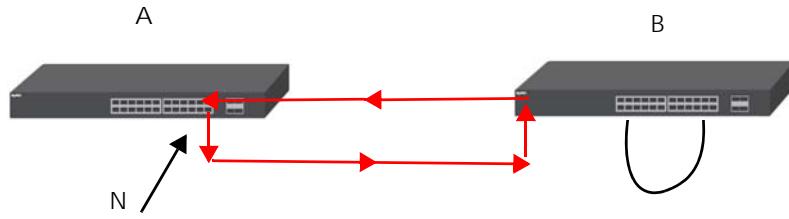


Loop guard is designed to handle loop problems on the edge of your network. This can occur when a port is connected to a OLT that is in a loop state. Loop state occurs as a result of human error. It happens when two ports on a switch are connected with the same cable. When a switch in loop state sends 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:

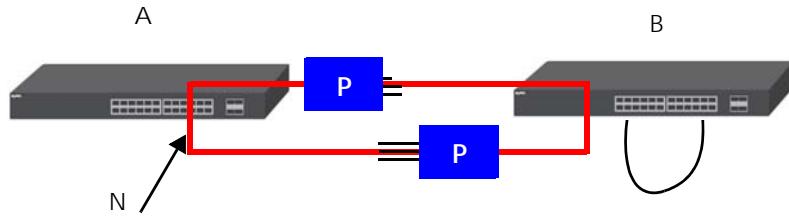
- It will receive broadcast messages sent out from the switch in loop state.
- It will receive its own broadcast messages that it sends out as they loop back. It will then re-broadcast those messages again.

The following figure shows port **N** on switch **A** connected to switch **B**. Switch **B** is in loop state. When broadcast or multicast packets leave port **N** and reach switch **B**, they are sent back to port **N** on **A** as they are rebroadcast from **B**.

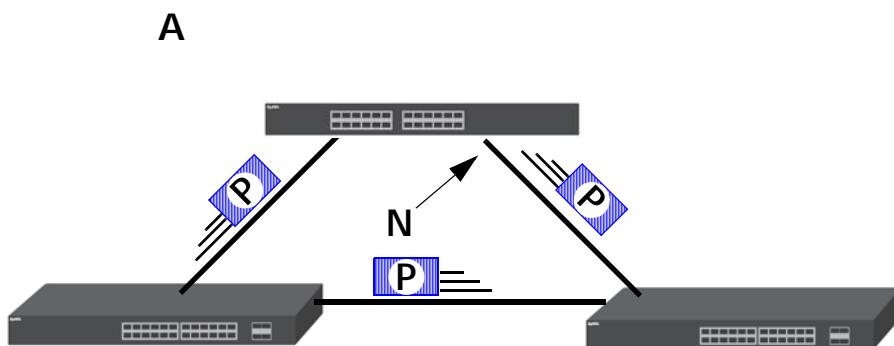
Figure 236 Switch in Loop State

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 OLT will shut down the port connected to the switch in loop state.

The following figure shows a loop guard enabled port **N** on switch **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 OLT then shuts down port **N** to ensure that the rest of the network is not affected by the switch in loop state.

Figure 237 Loop Guard - Probe Packet

The OLT also shuts down port **N** if the probe packet returns to switch **A** on any other port. In other words loop guard also protects against standard network loops. The following figure illustrates three switches forming a loop. A sample path of the loop guard probe packet is also shown. In this example, the probe packet is sent from port **N** and returns on another port. As long as loop guard is enabled on port **N**. The OLT will shut down port **N** if it detects that the probe packet has returned to the OLT.

Figure 238 Loop Guard - Network Loop

74.2 Loopguard Commands

Use these commands to configure the OLT to guard against loops on the edge of your network. The OLT shuts down a port if the OLT detects that packets sent out on the port loop back to the OLT.

Table 267 Loopguard Commands

COMMAND	DESCRIPTION	M	P
show loopguard	Displays which ports have loopguard enabled as well as their status.	E	3
loopguard	Enables loopguard on the OLT.	C	13
no loopguard	Disables loopguard on the OLT.	C	13
interface port-channel <aid>	Enters config-interface mode for the specified port(s). <i>aid: <pon eth>-<port></i>	C	13
loopguard	Enables the loopguard feature on the port(s). You have to enable loopguard on the OLT as well. The OLT shuts down a port if the OLT detects that packets sent out on the port loop back to the OLT.	C	13
no loopguard	Disables the loopguard feature on the port(s).	C	13
clear loopguard	Clears loopguard counters.	E	13

74.3 Loopguard Command Examples

This example enables loopguard on port 1 to port 5.

```

sysname# config
sysname(config)# loopguard
sysname(config)# interface port-channel eth-1&&-5
sysname(config-interface)# loopguard
sysname(config-interface)# exit
sysname(config)#
sysname# show loopguard
LoopGuard Status: Enable

      Port      Port      LoopGuard   Total      Total      Bad      Shutdown
      No       Status     Status    TxPkts    RxPkts   Pkts    Time
      -----  -----  -----  -----  -----  -----  -----
      pon-1    Active    Disable      0        0        0  00:00:00 UTC
Jan 1 1970
      pon-2    Active    Disable      0        0        0  00:00:00 UTC
Jan 1 1970
      pon-3    Active    Disable      0        0        0  00:00:00 UTC
Jan 1 1970
      pon-4    Active    Disable      0        0        0  00:00:00 UTC
Jan 1 1970
      eth-1    Active    Enable      0        0        0  00:00:00 UTC
Jan 1 1970
      eth-2    Active    Enable      0        0        0  00:00:00 UTC
Jan 1 1970
      eth-3    Active    Enable      0        0        0  00:00:00 UTC
Jan 1 1970
      eth-4    Active    Enable      0        0        0  00:00:00 UTC
Jan 1 1970
      eth-5    Active    Enable      0        0        0  00:00:00 UTC
Jan 1 1970
      -----
      eth-19   Active    Disable      0        0        0  00:00:00 UTC
Jan 1 1970
      eth-20   Active    Disable      0        0        0  00:00:00 UTC
Jan 1 1970

```

The following table describes the labels in this display.

Table 268 show loopguard

LABEL	DESCRIPTION
LoopGuard Status	This field displays whether or not loopguard is enabled on the OLT.
Port No	This field displays the port number.
Port Status	This field displays whether or not the port is active.
LoopGuard Status	This field displays whether or not loopguard is enabled on the port.
Total TxPkts	This field displays the number of packets that have been sent on this port since loopguard was enabled on the port.
Total RxPkts	This field displays the number of packets that have been received on this port since loopguard was enabled on the port.

Table 268 show loopguard (continued)

LABEL	DESCRIPTION
Bad Pkts	This field displays the number of invalid probe packets that were received on this port.
Shutdown Time	This field displays the last time the port was shut down because a loop state was detected.

CHAPTER 75

Static Route

This chapter shows you how to configure static routes. Static routes tell the OLT how to forward IP traffic when you configure the TCP/ IP parameters manually.

75.1 Static Route Commands

The following table lists the static route commands.

Table 269 Static Route Commands

COMMAND	DESCRIPTION	M	P
show ip route	Displays the IP routing table.	E	3
show ip route static	Displays the static routes.	E	3
show ip protocols	Displays the routing protocol the OLT is using and its administrative distance value.	E	3
show ip tcp	Displays IP TCP information.	E	3
show ip udp	Displays IP UDP information.	E	3
kick tcp <session id>	Disconnects the specified TCP session. <i>session id</i> : Display the session ID by running the show ip tcp command.	E	13
ip route <ip> <mask> <next-hop-ip> [metric <metric>] [name <name>] [inactive]	Creates a static route. If the <ip> <mask> already exists, the OLT deletes the existing route first. Optionally, also sets the metric, sets the name, and/or deactivates the static route. <i>metric</i> : 1-15 <i>name</i> : 1-10 English keyboard characters Note: If the <next-hop-ip> is not directly connected to the OLT, you must make the static route inactive.	C	13
no ip route <ip> <mask>	Removes a specified static route.	C	13
no ip route <ip> <mask> <next-hop-ip>	Removes a specified static route.	C	13
no ip route <ip> <mask> inactive	Enables a specified static route.	C	13
no ip route <ip> <mask> <next-hop-ip> inactive	Enables a specified static route.	C	13

75.2 Static Route Command Examples

In this routing table, you can create an active static route if the <next-hop-ip> is in 172.16.37.0/24 or 127.0.0.0/16. You cannot create an active static route to other IP addresses.

For example, you cannot create an active static route that routes traffic for 192.168.10.1/24 to 172.23.44.51.

```
sysname# config
sysname(config)# ip route 192.168.10.1 255.255.255.0 172.23.44.51
Error : The Action is failed. Please re-configure setting.
```

You can however, create this static route if it is inactive.

```
sysname# config
sysname(config)# ip route 192.168.10.1 255.255.255.0 172.23.44.51 inactive
```

You can create an active static route that routes traffic for 192.168.10.1/24 to 192.168.1.1.

```
sysname# config
sysname(config)# ip route 192.168.10.1 255.255.255.0 192.168.1.1.
```

This example shows the current routing table.

```
sysname# show ip route static
Idx Active Name Dest. Addr. Subnet Mask Gateway Addr. Metric
01 N static 192.168.10.1 255.255.255.0 172.23.44.51 1
02 Y static 192.168.10.1 255.255.255.0 192.168.1.1 1
```

The following table describes the labels in this display.

Table 270 show ip route static

LABEL	DESCRIPTION
Idx	The number of this static routing entry.
Active	This field displays whether or not the static route is active.
Name	Descriptive name of the static route for identification purposes.
Dest. Addr.	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
Subnet Mask	The subnet mask for this destination.
Gateway Addr.	The IP address of the gateway. The gateway is an immediate neighbor of your OLT that will forward the packet to the destination. The gateway must be a router on the same segment as your OLT.
Metric	The metric represents the "cost" of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks.

CHAPTER 76

DHCP

This chapter shows you how to configure the DHCP feature.

76.1 DHCP Overview

DHCP (Dynamic Host Configuration Protocol RFC 2131 and RFC 2132) allows individual computers to obtain TCP/IP configuration at start-up from a server. You can configure the OLT as a DHCP server or a DHCP relay agent. When configured as a server, the OLT provides the TCP/IP configuration for the clients. If you configure the OLT as a relay agent, then the OLT forwards DHCP requests to DHCP server on your network. If you don't configure the OLT as a DHCP server or relay agent then you must have a DHCP server in the broadcast domain of the client computers or else the client computers must be configured manually.

76.1.1 DHCP Modes

The OLT can be configured as a DHCP server or DHCP relay agent.

- If you configure the OLT as a DHCP server, it will maintain the pool of IP addresses along with subnet masks, DNS server and default gateway information and distribute them to your LAN computers.
- If there is already a DHCP server on your network, then you can configure the OLT as a DHCP relay agent. When the OLT receives a request from a computer on your network, it contacts the DHCP server for the necessary IP information, and then relays the assigned information back to the computer.

76.1.2 DHCP Configuration Options

The DHCP configuration on the OLT is divided into **Global** and **VLAN**. Which you should use for configuration depends on the DHCP services you want to offer the DHCP clients on your network. Choose the configuration based on the following criteria:

- **Global** - The OLT forwards all DHCP requests to the same DHCP server.
- **VLAN** - The OLT is configured on a VLAN by VLAN basis. The OLT can be configured as a DHCP server for one VLAN and at the same time the OLT can be configured to relay DHCP requests for clients in another VLAN.

76.2 DHCP Relay

Configure DHCP relay on the OLT if the DHCP clients and the DHCP server are not in the same broadcast domain. During the initial IP address leasing, the OLT helps to relay network information (such as the IP address and subnet mask) between a DHCP client and a DHCP server. Once the DHCP client obtains an

IP address and can connect to the network, network information renewal is done between the DHCP client and the DHCP server without the help of the OLT.

The OLT can be configured as a global DHCP relay. This means that the OLT forwards all DHCP requests from all domains to the same DHCP server. You can also configure the OLT to relay DHCP information based on the VLAN membership of the DHCP clients.

76.2.1 DHCP Relay Agent Information

The OLT can add information about the source of client DHCP requests that it relays to a DHCP server by adding **Relay Agent Information**. This helps provide authentication about the source of the requests. The DHCP server can then provide an IP address based on this information. Please refer to RFC 3046 for more details.

The DHCP **Relay Agent Information** feature adds an Agent Information field to the **Option 82** field. The **Option 82** field is in the DHCP headers of client DHCP request frames that the OLT relays to a DHCP server.

Relay Agent Information can include the system name of the OLT. See [Section 49.1 on page 370](#) for how to change the system name.

76.3 DHCP Commands

Use these commands to configure DHCP features on the OLT.

- Use the `dhcp relay` commands to configure DHCP relay for specific VLAN.
- Use the `dhcp smart-relay` commands to configure DHCP relay for all broadcast domains.
- Use the `dhcp server` commands to configure the OLT as a DHCP server. (This command is available on a layer 3 switch only.)

Table 271 DHCP Server Commands

COMMAND	DESCRIPTION	M	P
<code>dhcp server <vlan-id> starting-address <ip-addr> <subnet-mask> size-of-client-ip-pool <1-2048> [default-gateway <ip-addr>] [primary-dns <ip-addr>] [secondary-dns <ip-addr>]</code>	Enables DHCP server for the specified VLAN and specifies the TCP/IP configuration to send to DHCP clients. You can optionally include a default gateway IP address and DNS server addresses.	C	13
<code>no dhcp server <vlan-id></code>	Disables DHCP server configuration for the specified VLAN.	C	13
<code>no dhcp server <vlan-id> default-gateway</code>	Removes DHCP server default gateway configuration for the specified VLAN.	C	13
<code>no dhcp server <vlan-id> primary-dns</code>	Removes DHCP server primary DNS IP address configuration for the specified VLAN.	C	13
<code>no dhcp server <vlan-id> secondary-dns</code>	Removes DHCP server secondary DNS IP address configuration for the specified VLAN.	C	13
<code>show dhcp server</code>	Displays DHCP server status.	E	3
<code>show dhcp server <vlan-id></code>	Displays DHCP server status for the specified VLAN.	E	3

Table 272 DHCP Client Test Commands

COMMAND	DESCRIPTION	M	P
<code>test dhcp-client start <aid> vlan <sniivid> [nnisvid <1~4094>] [snicvid <1~4094>] [ontid <1~128>] [ontcardid <1~16>] [uniport <1~128>] [ontsn <string>]</code>	<p>Starts a DHCP client test to simulate an ONT getting IP address information from the DHCP server.</p> <p>aid: <ge pon>-<slot>-<port> slotge-<slot></p> <p>sniivid: Choose Service Node Interface (SNI) SVID on subscriber port (ONT), 1-4094. This is the outer VLAN on the service node interface.</p> <p>nnisvid: NNI SVID setting on subscriber port (ONT), 1-4094. If this is not set and option 82 needs this value, it will show 4096. This is the outer VLAN on the network to network interface.</p> <p>snicvid: SNI CVID setting on subscriber port (ONT), 1-4094. If this is not set and option 82 needs this value, it will show 4096. This is the inner VLAN on the service node interface.</p> <p>ontid: ONT ID to be added to option 82 information, 1-128</p> <p>ontcardid: ONTCARD ID to be added to option 82 information, 1-16</p> <p>uniport: UNIPORT value to be added to option 82 information, 1-128</p> <p>ontsn: ONT serial number to be added to option 82 information, length 1-16</p>	E	13
<code>test dhcp-client start help</code>	Provides more information about the specified command.	E	13
<code>test dhcp-client stop <aid> <cr></code>	Stops a DHCP client test on the specified port.	E	13
<code>aid: pon-<pon></code>			
<code>dhcp client-test timeout <1 to 180 seconds></code>	Specifies the DHCP client test timeout. The default is 3 seconds.	C	13
<code>show dhcp client-test timeout</code>	Displays the DHCP client test timeout.	E	3
<code>show dhcp client-test state <aid></code>	Displays the DHCP client test state of the specified port.	E	3
<code>aid: pon-<port></code>			

Table 273 Global DHCP Relay Commands

COMMAND	DESCRIPTION	M	P
<code>show dhcp smart-relay</code>	Displays global DHCP relay settings.	E	3
<code>dhcp smart-relay</code>	<p>Enables DHCP relay for all broadcast domains on the OLT.</p> <p>Note: You have to disable <code>dhcp relay</code> before you can enable <code>dhcp smart-relay</code>.</p>	C	13

Table 273 Global DHCP Relay Commands (continued)

COMMAND	DESCRIPTION	M	P
no dhcp smart-relay	Disables global DHCP relay settings.	C	13
dhcp smart-relay helper-address <remote-dhcp-server1> [<remote-dhcp-server2>] [<remote-dhcp-server3>]	Sets the IP addresses of up to 3 DHCP servers.	C	13
dhcp smart-relay information	Allows the OLT to add system name to agent information.	C	13
no dhcp smart-relay information	System name is not appended to option 82 information field for global DHCP settings.	C	13
dhcp smart-relay option	Allows the OLT to add DHCP relay agent information.	C	13
no dhcp smart-relay option	Disables the relay agent information option 82 for global DHCP settings.	C	13
dhcp smart-relay format <num>	<p>Enables DHCP option-82 with specific format.</p> <p>(A) option:</p> <ol style="list-style-type: none"> 1. append [ponport vlan] into the DHCP option 82 Circuit ID. 2. append [client's mac] into the DHCP option 82 Remote ID. <p>(B) information: append [system_name] behind [ponport vlan] into the DHCP option 82 Circuit ID.</p> <p>If (A) & (B) are set at the same time, the Circuit ID format would be [ponport vlan system_name]</p> <p>(C) format <num>: append a specific format of information into the Circuit ID and Remote ID.</p> <p>Example:</p> <p>format 1: append [SYS_ID PONPORT:NNISVID.SNISVID ONTID/SN] into the Circuit ID</p> <p>Remote ID is not required.</p> <p>(D) option-info per system: DHCP l2agent VLAN <info></p> <p>Note: The OLT uses the below rules as DHCP option 82 configurations.</p> <p>(D) > (C) > (A) = (B)</p>	C	13
dhcp smart-relay help	Provides more information about the specified command.	C	13
no dhcp smart-relay format	Disables DHCP smart relay from appending the option 82 format [SYS_ID PONPORT:NNISVID.SNISVID ONTID/SN] into the Circuit ID.	C	13

Table 274 DHCP Relay Commands

COMMAND	DESCRIPTION	M	P
show dhcp relay <vlan-id>	Displays DHCP relay settings for the specified VLAN.	E	3
dhcp relay <vlan-id> helper-address <remote-dhcp-server1> [<remote-dhcp-server2>] [<remote-dhcp-server3>] [option] [information] [format <num>]	<p>Enables DHCP relay on the specified VLAN and sets the IP address of up to 3 DHCP servers. Optionally, sets the OLT to add relay agent information and system name.</p> <p>Note: You have to configure the VLAN before you configure a DHCP relay for the VLAN. You have to disable <code>dhcp smart-relay</code> before you can enable <code>dhcp relay</code>.</p> <p>Option 82 setting:</p> <p>(A) option:</p> <ol style="list-style-type: none"> 1. append [ponport vlan] into the DHCP option 82 Circuit ID. 2. append [client's mac] into the DHCP option 82 Remote ID. <p>(B) information: append [system_name] behind [ponport vlan] into the DHCP option 82 Circuit ID.</p> <p>If (A) & (B) are set at the same time, the Circuit ID format would be [ponport vlan system_name]</p> <p>(C) format <num>: append a specific format of information into the Circuit ID and Remote ID.</p> <p>Example:</p> <p>format 1: append [SYS_ID PONPORT>NNISVID.SNISVID ONTID/SN] into the Circuit ID</p> <p>Remote ID is not required.</p> <p>(D) option-info per system:DHCP l2agent VLAN <info></p> <p>Note: The OLT uses the below rules as DHCP option 82 configurations.</p> <p>(D) > (C) > (A) = (B)</p>	C	13
no dhcp relay <vlan-id>	Disables DHCP relay.	C	13
no dhcp relay <vlan-id> information	System name is not appended to option 82 information field.	C	13
no dhcp relay <vlan-id> format	Disables DHCP Relay Agent from appending the option 82 format [SYS_ID PONPORT>NNISVID.SNISVID ONTID/SN] into the Circuit ID.	C	13
no dhcp relay <vlan-id> option	Disables the relay agent information option 82.	C	13

Table 275 DHCP Relay Broadcast Commands

COMMAND	DESCRIPTION	M	P
dhcp relay-broadcast	The broadcast behavior of DHCP packets will not be terminated by the OLT.	C	13
no dhcp relay-broadcast	The OLT terminates the broadcast behavior of DHCP packets.	C	13

The following table describes commonly used parameter notation for these commands.

Table 276 DHCP L2 Agent Commands

COMMAND	DESCRIPTION
info	<p>The string should be composed of the following special characters. The special characters listed in the brackets [~`!@#\$^&*()]) are not allowed except % and space.</p> <ul style="list-style-type: none"> • %%: character % • %space: character space • %mac: client source mac • %hname: host device name • %pid: pon port index • %oid: ONT index • %ocid: ONT card index • %upid: uniport index • %nnisvlan: SVLAN ID on network-network interface • %snisvlan: SVLAN ID on service-network interface • %snicvlan: CVLAN ID on service-network interface • %sn: serial number of remote ONT • %ontname: will be translated into ONT model name • %ontdesc: will be translated into ONT description • %ontpasswd: will be translated into ONT password

Table 277 DHCP L2 Agent Commands

COMMAND	DESCRIPTION	M	P
dhcp l2agent vlan <vid> <cr>	Enables the DHCP L2 Agent relay function on the specified VLAN.	C	13
no dhcp l2agent vlan <vid> <cr>	Disables the DHCP L2 Agent relay function on the specified VLAN.	C	13
dhcp l2agent vlan <vid> [ldra]	<p>Enables DHCP L2 Agent Lightweight DHCPv6 Relay Agent (LDRA) function on the specified VLAN.</p> <p>Lightweight DHCPv6 Relay Agent (LDRA) adds information to client DHCPv6 requests before forwarding them to the DHCPv6 server.</p>	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

Table 277 DHCP L2 Agent Commands (continued)

COMMAND	DESCRIPTION	M	P
dhcp l2agent opt18-interface-id vlan <vlan> option-info <info>	<p>Configures the DHCP L2 Agent option 18 interface ID format on the specified VLAN.</p> <p>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.</p> <p>See Table 276 on page 538 for more information about the <info> string.</p> <p>Note: If the string is composed of more than 127 characters, the string will be truncated to the maximum number of characters allowed when the OLT transforms the string into the Interface ID.</p>	C	13
no dhcp l2agent opt18-interface-id vlan <vlan>	Disables the DHCP L2 Agent option 18 interface ID on the specified VLAN.	C	13
dhcp l2agent opt37-remote-id vlan <vlan> option-info <info>	<p>Configures the DHCP L2 Agent option 37 Remote ID format on the specified VLAN.</p> <p>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.</p> <p>Option 37 (Remote ID Info) is the DHCPv6 equivalent for the Dynamic Host Configuration Protocol for IPv4 (DHCPv4) Relay Agent Option's Remote-ID sub-option.</p> <p>See Table 276 on page 538 for more information about the <info> string.</p> <p>Note: If the string is composed of more than 95 characters, the string will be truncated to the maximum number of characters allowed when the OLT transforms the string into the Remote ID.</p>	C	13
no dhcp l2agent opt37-remote-id vlan <vlan>	Disables the DHCP L2 Agent option 37 Remote ID on the specified VLAN.	C	13

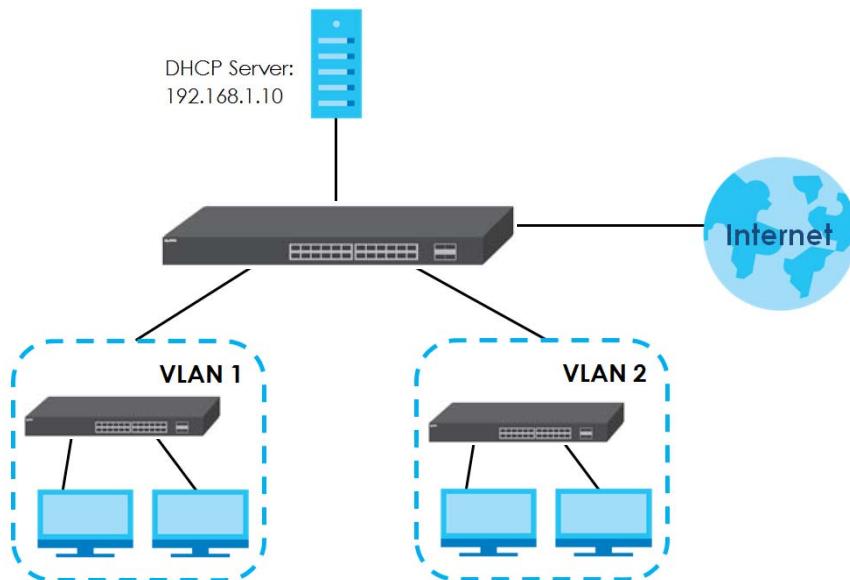
Table 277 DHCP L2 Agent Commands (continued)

COMMAND	DESCRIPTION	M	P
<code>dhcp l2agent opt82-circuit-id vlan <vlan> option-info <info></code>	<p>Configures the DHCP L2 Agent option 82 Circuit ID format on the specified VLAN.</p> <p>Use this command to have the OLT add the originating port numbers to DHCP requests in the specified VLAN.</p> <p>See Table 276 on page 538 for more information about the <info> string.</p> <p>Note: If the string is composed of more than 127 characters, the string will be truncated to the maximum number of characters allowed when the OLT transforms the string into the Circuit ID.</p>	C	13
<code>no dhcp l2agent opt82-circuit-id vlan <vlan></code>	Disables the DHCP L2 Agent option 82 Circuit ID on the specified VLAN.	C	13
<code>dhcp l2agent opt82-remote-id vlan <vlan> option-info <info></code>	<p>Configures the DHCP L2 Agent option 82 Remote ID format on the specified VLAN.</p> <p>Use this command to have the OLT add the Remote ID to DHCP requests in the specified VLAN.</p> <p>See Table 276 on page 538 for more information about the <info> string.</p> <p>Note: If the string is composed of more than 95 characters, the string will be truncated to the maximum number of characters allowed when the OLT transforms the string into the Remote ID.</p>	C	13
<code>no dhcp l2agent opt82-remote-id vlan <vlan></code>	Disables the DHCP L2 Agent option 82 Remote ID on the specified VLAN.	C	13
<code>dhcp relay <vlan-id> helper-address <remote-dhcp-server1> <cr></code>	<p>Enables DHCP relay on the specified VLAN and sets the IP address of up to a DHCP server.</p> <p>Note: You have to configure the VLAN before you configure a DHCP relay for the VLAN. You have to disable <code>dhcp smart-relay</code> before you can enable <code>dhcp relay</code>.</p>	C	13
<code>dhcp server <vlan-id> starting-address <ip-addr> <subnet-mask> size-of-client-ip-pool <1-2048> <cr></code>	Enables DHCP server for the specified VLAN and specifies the TCP/IP configuration details to send to DHCP clients.	C	13
<code>dhcp l2agent help</code>	Displays details about DHCP option 82 rules.	C	13
<code>show dhcp l2agent vlan <vlan/*></code>	Displays the DHCP L2 Agent relay function on the specified VLAN.	E	1

76.4 DHCP Command Examples

In this example, the OLT relays DHCP requests for the **VLAN1** and **VLAN2** domains. There is only one DHCP server for DHCP clients in both domains.

Figure 239 Example: Global DHCP Relay



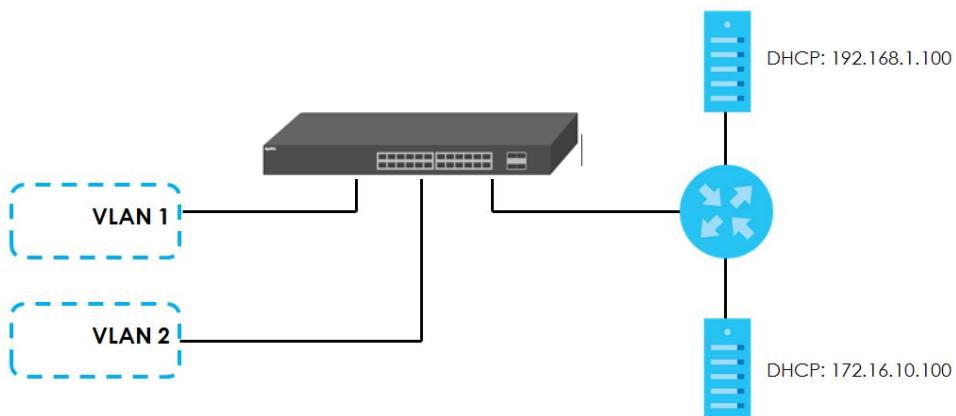
This example shows how to configure the OLT for this configuration. DHCP relay agent information option 82 is also enabled.

```

sysname# configure
sysname(config)# dhcp smart-relay
sysname(config)# dhcp smart-relay helper-address 192.168.1.100
sysname(config)# dhcp smart-relay option
sysname(config)# exit
sysname# show dhcp smart-relay
  DHCP Relay Agent Configuration
  Active:      Yes
  Remote DHCP Server 1:192.168.1.100
  Remote DHCP Server 2:    0.0.0.0
  Remote DHCP Server 3:    0.0.0.0
  Option82:   Enable      Option82Inf: Disable

```

In this example, there are two VLANs (VIDs 1 and 2) in a campus network. Two DHCP servers are installed to serve each VLAN. The OLT forwards DHCP requests from the dormitory rooms (VLAN 1) to the DHCP server with IP address 192.168.1.100. DHCP requests from the academic buildings (VLAN 3) are sent to the other DHCP server with IP address 172.16.10.100.

Figure 240 Example: DHCP Relay for Two VLANs

This example shows how to configure these DHCP servers. The VLANs are already configured.

```
sysname# configure
sysname(config)# dhcp relay 1 helper-address 192.168.1.100
sysname(config)# dhcp relay 2 helper-address 172.16.10.100
sysname(config)# exit
```

76.5 Configuring DHCP VLAN

See [Section 72.3 on page 495](#) for how to configure your DHCP settings based on the VLAN domain of the DHCP clients.

CHAPTER 77

File Management

This chapter explains how to maintain the firmware and configuration files.

77.1 FTP Command Line

This section shows some examples of uploading to or downloading files from the OLT using FTP commands. First, understand the filename conventions.

77.1.1 Filename Conventions

The configuration file (also known as the romfile or ROM) contains the factory default settings. Once you have customized the OLT's settings, they can be saved back to your computer under a filename of your choosing.

ZyNOS is the system firmware and has a "bin" filename extension.

Table 278 Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration Text File	config		This is the text configuration file, including your OLT configurations, system-related data, configurations, system-related data.
Firmware	ras		This is the generic name for the firmware image 1 on the OLT.
Firmware	ras-1		This is the generic name for the firmware image 2 on the OLT.
ONT Image	ont		This is the generic name for the ONT image that is used to do ONT remote firmware upgrade.

77.1.1.1 Example FTP Commands

This is a sample FTP session updating ras to the OLT.

```
ftp> put ras
```

This is a sample FTP session saving the current configuration to a file called "config.cfg" on your computer.

```
ftp> get config config.cfg
```

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 OLT only recognizes "config" and "ras". Be sure you keep unaltered copies of both files for later use.

Be sure to upload the correct model firmware as uploading the wrong model firmware may damage your device.

77.1.2 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 OLT.
- 3 Press [ENTER] when prompted for a username (the default is "admin").
- 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 OLT, for example, `put ras` transfers the firmware on your computer to the OLT and renames it to "ras". Similarly, `put config` transfers the configuration file on your computer (config.cfg) to the OLT and renames it to "config". Likewise `get config config.cfg` transfers the configuration file on the OLT to your computer and renames it to "config.cfg". See [Table 278 on page 543](#) for more information on filename conventions.
- 7 Enter `quit` to exit the ftp prompt.

77.2 GUI-based FTP Clients

The following table describes some of the commands that you may see in GUI-based FTP clients.

Table 279 General Commands for GUI-based FTP Clients

COMMAND	DESCRIPTION
Host Address	Enters the address of the host server.
Login Type	Anonymous. This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option. Normal. The server requires a unique User ID and Password to login.
Transfer Type	Transfers files in either ASCII (plain text format) or in binary mode. Configuration and firmware files should be transferred in binary mode.
Initial Remote Directory	Specifies the default remote directory (path).
Initial Local Directory	Specifies the default local directory (path).

77.2.1 FTP Restrictions

FTP will not work when:

- FTP service is disabled in the service access control configuration.

- The IP addresses in the remote management configuration do not match the client IP address. If it does not match, the OLT will disconnect the FTP session immediately.

CHAPTER 78

Access Control

This chapter describes how to control access to the OLT.

78.1 Access Control Overview

A console port and FTP are allowed one session each, Telnet and SSH share nine sessions, and/or limitless SNMP access control sessions are allowed.

Table 280 Access Control Overview

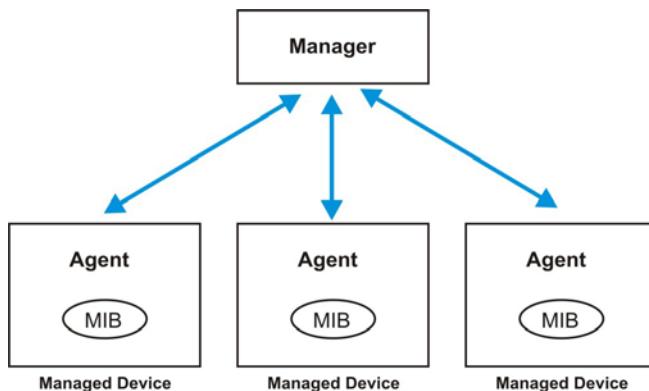
Console Port	SSH	Telnet	FTP	SNMP
One session	Share up to five sessions	One session	No limit	

A console port access control session and Telnet access control session cannot coexist when multi-login is disabled. See the Ethernet Switch CLI Reference Guide for more information on disabling multi-login.

78.2 About SNMP

Simple Network Management Protocol (SNMP) is an application layer protocol used to manage and monitor TCP/IP-based devices. SNMP is used to exchange management information between the network management system (NMS) and a network element (NE). A manager station can manage and monitor the OLT through the network via SNMP version one (SNMPv1), SNMP version 2c or SNMP version 3. The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

Figure 241 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 OLT (the OLT). An agent translates the local management information from the managed OLT 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 OLT. Examples of variables include number of packets received, node port status and so on. 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 281 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.

78.2.1 SNMP v3 and Security

SNMP v3 enhances security for SNMP management. SNMP managers can be required to authenticate with agents before conducting SNMP management sessions.

Security can be further enhanced by encrypting the SNMP messages sent from the managers. Encryption protects the contents of the SNMP messages. When the contents of the SNMP messages are encrypted, only the intended recipients can read them.

78.2.2 Supported MIBs

MIBs let administrators collect statistics and monitor status and performance.

The OLT supports the following MIBs:

- SNMP MIB II (RFC 1213)
- RFC 1157 SNMP v1
- RFC 1493 Bridge MIBs
- RFC 1643 Ethernet MIBs
- RFC 1155 SMI
- RFC 2674 SNMPv2, SNMPv2c
- RFC 1757 RMON
- SNMPv2, SNMPv2c or later version, compliant with RFC 2011 SNMPv2 MIB for IP, RFC 2012 SNMPv2 MIB for TCP, RFC 2013 SNMPv2 MIB for UDP

78.3 SNMP Server Commands

Use these commands to configure SNMP on the OLT.

The following section lists the commands for this feature.

Table 282 SNMP Server Commands

COMMAND	DESCRIPTION	M	P
<code>show snmp-server</code>	Displays SNMP settings.	E	3
<code>snmp-server <[contact <system-contact>] [location <system-location>]></code>	Sets the geographic location and the name of the person in charge of this OLT. <i>system-contact</i> : 1-32 English keyboard characters; spaces are allowed. <i>system-location</i> : 1-32 English keyboard characters; spaces are allowed.	C	13
<code>snmp-server version <v2c v3 v3v2c></code>	Sets the SNMP version to use for communication with the SNMP manager. v2c: allows SNMPv2 read/write access. v3: allows SNMPv3 read/write access. v3v2c: allows SNMPv2 and SNMPv3 read/write access.	C	13
<code>snmp-server get-community <property></code>	Sets the get community. Only for SNMPv2c or lower.	C	13
<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></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.	C	13
<code>snmp-server trap-destination <ip> [udp-port <socket-number>] [version <v1 v2c v3>] [username <name>]</code>	Sets the port number, version, and username of the specified SNMP manager.	C	13
<code>no snmp-server trap-destination <ip></code>	Deletes the specified SNMP manager.	C	13

Table 282 SNMP Server Commands (continued)

COMMAND	DESCRIPTION	M	P
<code>snmp-server username <name> sec-level <noauth auth priv> [auth <md5 sha> auth-password <pwd>] [priv <des aes> priv-password <pwd>] group <admin/readonly/readwrite></code>	<p>Sets the authentication level for SNMP v3 user authentication. Optionally, specifies the authentication and encryption methods for communication with the SNMP manager.</p> <p>name: Enter the SNMP username.</p> <p>noauth: Use the username as the password string sent to the SNMP manager. This is equivalent to the Get, Set and Trap Community in SNMP v2c. This is the lowest security level.</p> <p>auth: Implement an authentication algorithm for SNMP messages sent by this user.</p> <p>priv: Implement privacy settings and encryption for SNMP messages sent by this user. This is the highest security level.</p> <p>auth-password: Set the authentication password for SNMP messages sent by this user.</p> <p>priv-password: Set the privacy settings password for SNMP messages sent by this user.</p> <p>group: Set the View-based Access Control Model (VACM) group. Available group names are:</p> <ul style="list-style-type: none"> admin: The user belongs to the admin group and has maximum access rights to the OLT. readwrite: The user can read and configure the OLT except for confidential options (such as user account and AAA configuration options.) readonly: The user can read but cannot make any configuration changes. <p>Note: The settings on the SNMP manager must be set at the same security level or higher than the security level settings on the OLT.</p>	C	14
<code>no snmp-server username <name></code>	Removes the specified SNMP user's information.	C	14
<code>show snmp-server user</code>	Displays the SNMP information on the OLT. The user flag displays SNMP user information.	E	3

Table 283 snmp-server trap-destination enable traps Commands

COMMAND	DESCRIPTION	M	P
<code>snmp-server trap-destination <ip> enable traps</code>	Enables sending SNMP traps to a manager.	C	13
<code>snmp-server trap-destination <ip> enable traps help</code>	Provides more information about the specified command.	C	13
<code>no snmp-server trap-destination <ip> enable traps</code>	Disables sending of SNMP traps to a manager.	C	13
<code>snmp-server trap-destination <ip> enable traps aaa</code>	Sends all AAA traps to the specified manager.	C	13
<code>no snmp-server trap-destination <ip> enable traps aaa</code>	Prevents the OLT from sending any AAA traps to the specified manager.	C	13

Table 283 snmp-server trap-destination enable traps Commands (continued)

COMMAND	DESCRIPTION	M	P
snmp-server trap-destination <ip> enable traps aaa <options>	Sends the specified AAA traps to the specified manager.	C	13
no snmp-server trap-destination <ip> enable traps aaa <options>	Prevents the OLT from sending the specified AAA traps to the specified manager.	C	13
snmp-server trap-destination <ip> enable traps interface	Sends all interface traps to the specified manager.	C	13
no snmp-server trap-destination <ip> enable traps interface	Prevents the OLT from sending any interface traps to the specified manager.	C	13
snmp-server trap-destination <ip> enable traps interface <options>	Sends the specified interface traps to the specified manager.	C	13
no snmp-server trap-destination <ip> enable traps interface <options>	Prevents the OLT from sending the specified interface traps to the specified manager.	C	13
snmp-server trap-destination <ip> enable traps ip	Sends all IP traps to the specified manager.	C	13
no snmp-server trap-destination <ip> enable traps ip	Prevents the OLT from sending any IP traps to the specified manager.	C	13
snmp-server trap-destination <ip> enable traps ip <options>	Sends the specified IP traps to the specified manager.	C	13
no snmp-server trap-destination <ip> enable traps ip <options>	Prevents the OLT from sending the specified IP traps to the specified manager.	C	13
snmp-server trap-destination <ip> enable traps switch	Sends all switch traps to the specified manager.	C	13
no snmp-server trap-destination <ip> enable traps switch	Prevents the OLT from sending any switch traps to the specified manager.	C	13
snmp-server trap-destination <ip> enable traps switch <options>	Sends the specified switch traps to the specified manager.	C	13
no snmp-server trap-destination <ip> enable traps switch <options>	Prevents the OLT from sending the specified switch traps to the specified manager.	C	13
snmp-server trap-destination <ip> enable traps system	Sends all system traps to the specified manager.	C	13
no snmp-server trap-destination <ip> enable traps system	Prevents the OLT from sending any system traps to the specified manager.	C	13
snmp-server trap-destination <ip> enable traps system <options>	Sends the specified system traps to the specified manager.	C	13
no snmp-server trap-destination <ip> enable traps system <options>	Prevents the OLT from sending the specified system traps to the specified manager.	C	13

78.4 SNMP Command Examples

This example shows you how to display the SNMP information on the OLT.

```
sysname# show snmp-server

[General Setting]
SNMP Version      : v2c
Get Community    : public
Set Community    : public
Trap Community   : public

[ Trap Destination ]
Index  Version     IP          Port  Username
-----  -----  -----
  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
```

This example shows you how to display all SNMP user information on the OLT.

```
sysname# show snmp-server user

[ User Information ]
Index  Name    SecurityLevel  Authentication  Privacy  Group
-----  ----  -----

```

78.5 Setting Up Login Accounts

Up to five people (one administrator and four non-administrators) may access the OLT via telnet at any one time.

- An administrator is someone who can both view and configure OLT changes. The username for the Administrator is always **admin**. The default administrator password is **1234**.

Note: It is highly recommended that you change the default administrator password (**1234**).

- A non-administrator (username is something other than **admin**) is someone who can view but not configure OLT settings.

78.6 Inactive Management Session Timeout Commands

Use these commands to configure the timeout for inactive management sessions.

Table 284 Inactive Management Session Timeout Commands

COMMAND	DESCRIPTION	M	P
show uart-logout-time	Displays the inactive management session timeout value.	E	13
uart-logout-time <time>	Sets the inactive management session timeout value. <i>time</i> : 1-60 minutes. Default value 5 minutes.	C	13
no uart-logout-time	Sets the inactive management session timeout to the default value of 5 minutes.	C	13

78.7 Login Account Commands

Use these commands to configure login accounts on the OLT.

Table 285 Login Account Commands

COMMAND	DESCRIPTION	M	P
show logins	Displays login account information.	E	3
logins username <name> password <pwd>	Creates account with the specified user name and sets the password. <i>name</i> : 1-32 alphanumeric characters. <i>pwd</i> : 1-32 alphanumeric characters.	C	14
logins username <name> password <pwd> privilege <0-14>	Creates account with the specified user name and sets the password and privilege. The privilege level is applied the next time the user logs in. <i>name</i> : 1-32 alphanumeric characters. <i>pwd</i> : 1-32 alphanumeric characters.	C	14
logins username <name> password cipher <pwd>	Creates account with the specified user name and sets the cipher password. <i>name</i> : 1-32 alphanumeric characters. <i>pwd</i> : 32 alphanumeric characters.	C	14
logins username <name> password cipher <pwd> privilege <0-14>	Creates account with the specified user name and sets the cipher password and privilege. This is used for password encryption. The privilege level is applied the next time the user logs in. <i>name</i> : 1-32 alphanumeric characters. <i>pwd</i> : 32 alphanumeric characters.	C	14
no logins username <name>	Removes the specified account.	C	14

78.8 Login Account Command Examples

This example creates a new user **user2** with privilege 13.

```
sysname# configure
sysname(config)# logins username user2 password 1234 privilege 13
sysname(config)# exit
sysname# show logins
Login    Username                      Privilege
1        user2                         13
2                                0
3                                0
4                                0
```

78.9 Password Encryption

Password encryption provides service providers a means to securely enter administrator and login passwords. By default, passwords are sent in plain text. Plain text passwords are also stored temporarily in the OLT's spt and temp buffers. By enabling password encryption, you can hide these plain text passwords in transit as well as in the device buffers.

78.10 Password Commands

Use these commands to configure passwords for specific privilege levels on the OLT.

Table 286 Password Commands

COMMAND	DESCRIPTION	M	P
admin-password <pw-string>	Changes the administrator password. <i>pw-string</i> : 1-32 alphanumeric characters	C	14
admin-password cipher <pw-string>	Sets the administrator cipher password, which is used in administrator password encryption. <i>pw-string</i> : 32 alphanumeric characters	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 <0-14>	Changes the password for the highest privilege level or, optionally, the specified privilege. <i>password</i> : 1-32 alphanumeric characters	C	14
password cipher <password>	Changes the password cipher for the highest privilege level.	C	14
password cipher <password> privilege <0-14>	Changes the password cipher for the highest privilege level or, optionally, the specified privilege. This is used in password encryption. <i>password</i> : 32 alphanumeric characters	C	14

Table 286 Password Commands (continued)

COMMAND	DESCRIPTION	M	P
no password privilege <0-14>	Clears the password for the specified privilege level and prevents users from entering the specified privilege level.	C	14
password encryption	Sets all password setting encryption.	C	14
no password encryption	Disables password encryption. The encrypted password will not be changed back to plain text.	C	14

78.11 SSH Overview

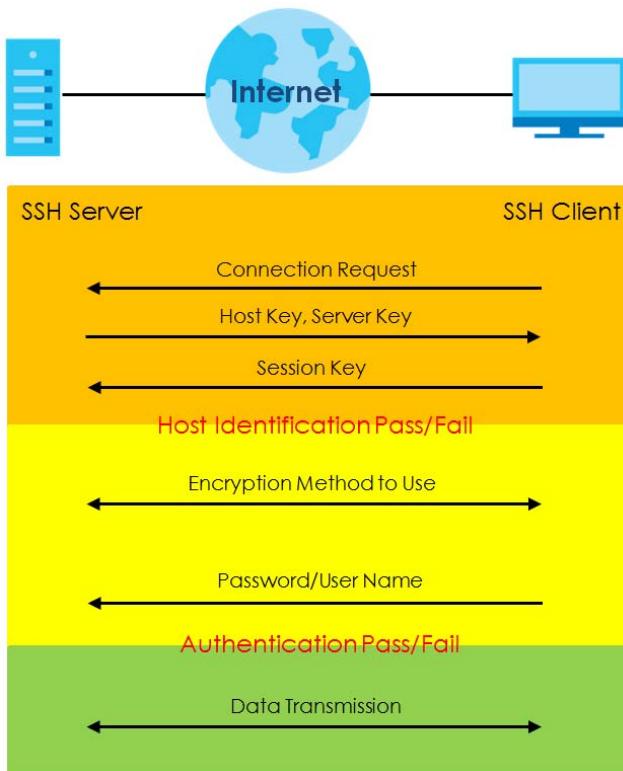
Unlike Telnet or FTP, which transmit data in clear text, SSH (Secure Shell) is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network.

Figure 242 SSH Communication Example



78.12 How SSH works

The following table summarizes how a secure connection is established between two remote hosts.

Figure 243 How SSH Works

1 Host Identification

The SSH client sends a connection request to the SSH server. The server identifies itself with a host key. The client encrypts a randomly generated session key with the host key and server key and sends the result back to the server.

The client automatically saves any new server public keys. In subsequent connections, the server public key is checked against the saved version on the client computer.

2 Encryption Method

Once the identification is verified, both the client and server must agree on the type of encryption method to use.

3 Authentication and Data Transmission

After the identification is verified and data encryption activated, a secure tunnel is established between the client and the server. The client then sends its authentication information (user name and password) to the server to log in to the server.

78.13 SSH Implementation on the OLT

Your OLT supports SSH version 2 using RSA authentication and three encryption methods (DES, 3DES and Blowfish). The SSH server is implemented on the OLT for remote management and file transfer on port 22. Only one SSH connection is allowed at a time.

78.13.1 Requirements for Using SSH

You must install an SSH client program on a client computer (Windows or Linux operating system) that is used to connect to the OLT over SSH.

78.14 Service Access Control Commands

Use these commands to control what services you may use to access the OLT. You may also change the default service port for each service.

Table 287 Service Access Control Commands

COMMAND	DESCRIPTION	M	P
show service-control	Displays service control settings.	E	3
service-control ftp	Allows FTP access to the OLT.	C	13
service-control ftp <socket-number>	Specifies the service port for the FTP service.	C	13
no service-control ftp	Disables FTP access to the OLT.	C	13
service-control http	Allows HTTP access to the OLT.	C	13
service-control http <socket-number> <timeout>	Specifies the service port for the HTTP service and defines the timeout period (in minutes). <i>timeout</i> : 1-255	C	13
no service-control http	Disables HTTP access to the OLT.	C	13
service-control https	Allows HTTPS access to the OLT.	C	13
service-control https <socket-number>	Specifies the service port for the HTTPS service.	C	13
no service-control https	Disables HTTPS access to the OLT.	C	13
service-control icmp	Allows ICMP management packets.	C	13
no service-control icmp	Disables ICMP access to the OLT.	C	13
service-control snmp	Allows SNMP management.	C	13
no service-control snmp	Disables SNMP access to the OLT.	C	13
service-control ssh	Allows SSH access to the OLT.	C	13
service-control ssh <socket-number>	Specifies the service port for the SSH service.	C	13
no service-control ssh	Disables SSH access to the OLT.	C	13
service-control telnet	Allows Telnet access to the OLT.	C	13
service-control telnet <socket-number>	Specifies the service port for the Telnet service.	C	13
no service-control telnet	Disables Telnet access to the OLT.	C	13
show ssh <cr>	Displays SSH access information.	E	3
show ssh key <rsa1 rsa dsa>	Displays internal SSH public and private key information.	E	3
no ssh key <rsa1 rsa dsa>	Disables the secure shell server encryption key. Your OLT supports SSH versions 1 and 2 using RSA and DSA authentication.	C	13

Table 287 Service Access Control Commands (continued)

COMMAND	DESCRIPTION	M	P
no ssh known-hosts <host-ip> [1024 ssh-rsa ssh-dsa]	Removes the specified remote hosts with the specified public key (1024-bit RSA1, RSA or DSA).	C	13
no ssh known-hosts <host-ip>	Removes the specified remote hosts from the list of all known hosts.	C	13
show ssh known-hosts	Displays the SSH known hosts information.	E	3
show ssh session	Displays the SSH's current sessions.	E	3

78.15 Service Access Control Command Example

This example disables all SNMP and ICMP access to the OLT.

```
sysname# configure
sysname(config)# no service-control snmp
sysname(config)# no service-control icmp
sysname(config)# exit
```

78.16 Remote Management Commands

Use these commands to specify a group of one or more “trusted computers” from which an administrator may use one or more services to manage the OLT.

Table 288 Remote Management Commands

COMMAND	DESCRIPTION	M	P
show remote-management	Displays all IPv4 trusted host information.	E	3
show remote-management <index>	Displays all secured client information or, optionally, a specific group of secured clients. <i>index</i> : 1-4	E	3
remote-management <index>	Enables the specified group of trusted computers.	C	13
no remote-management <index>	Disables the specified group of trusted computers.	C	13
remote-management <index> start-addr <ip> end-addr <ip> service <[telnet] [ftp] [http] [icmp] [snmp] [ssh] [https]>	Specifies a group of trusted computer(s) from which an administrator may use the specified service(s) to manage the OLT. Group 0.0.0.0 - 0.0.0.0 refers to every computer.	C	13
no remote-management <index> service <[telnet] [ftp] [http] [icmp] [snmp] [ssh] [https]>	Disables the specified service(s) for the specified group of trusted computers.	C	13

78.17 Remote Management Command Example

This example allows computers in subnet 172.16.37.0/24 to access the OLT through any service except SNMP, allows the computer at 192.168.10.1 to access the OLT only through SNMP, and prevents other computers from accessing the OLT at all.

```
sysname# configure
sysname(config)# remote-management 1 start-addr 172.16.37.0 end-addr
--> 172.16.37.255 service telnet ftp http icmp ssh https
sysname(config)# remote-management 2 start-addr 192.168.10.1 end-addr
--> 192.168.10.1 service snmp
sysname(config)# exit
```

CHAPTER 79

Diagnostics

This chapter describes how to check the OLT's system status.

79.1 Diagnostics Commands

Use these commands to check system logs, ping IP addresses or perform port tests.

Table 289 Diagnostic Commands

COMMAND	DESCRIPTION	M	P
interface transceiver-ddmi <aid>	Enters sub-command mode for configuring the interface transceiver threshold settings. aid: <pon eth>-<port>	C	13
tlimit [alarm <high> <low>] [warn <high> <low>]	Sets the temperature alarm and/or warning threshold. value range <-128 ~ 128> Units: degrees Celsius C	C	13
vlimit [alarm <high> <low>] [warn <high> <low>]	Sets the voltage alarm and/or warning threshold. value range <0 ~ 6.55> Units: volts	C	13
blimit [alarm <high> <low>] [warn <high> <low>]	Sets the bias current alarm and/or warning threshold. value range <0 ~ 131> Units: mA	C	13
txlimit [alarm <high> <low>] [warn <high> <low>]	Sets the transmission power alarm and/or warning threshold. value range <-40 ~ 8.2> Units: dbm	C	13
rxlimit [alarm <high> <low>] [warn <high> <low>]	Sets the receive power alarm and/or warning threshold. value range <-40 ~ 8.2> Units: dbm	C	13
no inactive	Activates the interface transceiver threshold configuration.	C	13
inactive	Disables the interface transceiver threshold configuration.	C	13
no interface transceiver-ddmi <aid>	Deletes the interface transceiver threshold configuration for the specified port. aid: <pon eth>-<port>	C	13
no interface transceiver-ddmi all	Deletes all interface transceiver threshold configuration.	C	13

Table 289 Diagnostic Commands (continued)

COMMAND	DESCRIPTION	M	P
hardware-alarm-setting cpu-utilization <1 - 100>	Sets the CPU utilization alarm threshold.	C	13
hardware-alarm-setting memory-usage <1 - 100>	Sets the memory usage alarm threshold.	C	13
no hardware-alarm-setting cpu-utilization	Removes the CPU utilization alarm threshold setting.	C	13
no hardware-alarm-setting memory-usage	Removes the memory usage alarm threshold setting.	C	13
ping <ip host-name> <cr>	Sends Ping packets to the specified Ethernet device.	E	0
ping <ip host-name> [in-band out-of-band] [size <0-1472>] [-t]	Sends Ping packets to the specified Ethernet device. size <0-1472>: Specifies the size of the Ping packet. -t: Sends Ping packets to the Ethernet device indefinitely. Press [CTRL]+C to terminate the Ping process.	E	0
ping help	Provides more information about the specified command.	E	0
ping6 <ipv6-addr>	Sends IPv6 ping packets to the specified Ethernet device.	E	0
test interface olt rogue <aid>	Uses this command to discover rogue ONTs, especially when you receive reports from multiple ONTs not being able to transmit traffic. aid: <pon eth>-<port>	E	13
start	Enables rogue ONT detection on the specified PON port. The ONTs connected to the specified PON port will be disabled temporarily, so the OLT can perform rogue detection on the ONTs.	E	13
stop	Disables rogue ONT detection on the specified PON port.	E	13
Exit	Leaves the configure rogue mode.	E	13
show alarm-status	Displays alarm status.	E	0
show cpu-utilization	Displays the CPU utilization statistics on the OLT.	E	0
show hardware-alarm-setting	Displays the CPU and memory alarm thresholds.	E	13
show hardware-monitor <C F>	Displays current hardware monitor information with the specified temperature unit (Celsius C or Fahrenheit F).	E	0
show memory	Displays the memory utilization statistics on the OLT.	E	0
show interfaces transceiver <aid>	Displays real-time SFP (Small Form Factor Pluggable) transceiver information and operating parameters on specified SFP port(s). The parameters include, for example, module temperature, module voltage, transmitting and receiving power. aid: <pon eth>-<port> ont-<port>-<ont>	E	3

Table 289 Diagnostic Commands (continued)

COMMAND	DESCRIPTION	M	P
show interfaces transceiver <aid> user-define	Displays user-defined parameters on specified SFP port(s). aid: <pon eth>-<port> ont-<port>-<ont>	E	3
show system-information	Displays general system information.	E	0
show version flash	Display the version of the currently running firmware on the OLT. Optionally, display the versions of the currently installed firmware images on the flash memory.	E	0
traceroute <ip host-name> <cr>	Displays the path a packet takes to the specified Ethernet device with an IPv4 address.	E	0
traceroute <ip host-name> [in-band out-of-band] [ttl <1-255>] [wait <1-60>] [queries <1-10>]	Determines the path a packet takes to the specified Ethernet device. ttl <1-255>: Specifies the Time To Live (TTL) period. wait <1-60>: Specifies the time period to wait. queries <1-10>: Specifies how many times the OLT performs the traceroute function.	E	0
traceroute help	Provides more information about the specified command.	E	0

79.2 Diagnostics Commands Examples

This example sends Ping requests to an Ethernet device with IP address 172.16.37.254.

```
sysname# ping 172.16.37.254
Resolving 172.16.37.254... 172.16.37.254
  sent   rcvd   rate      rtt      avg      mdev      max      min    reply from
    1       1   100        0        0        0        0        0  172.16.37.254
    2       2   100        0        0        0        0        0  172.16.37.254
    3       3   100       10        1        3       10        0  172.16.37.254
```

The following table describes the labels in this display.

Table 290 ping

LABEL	DESCRIPTION
sent	This field displays the sequence number of the ICMP request the OLT sent.
rcvd	This field displays the sequence number of the ICMP response the OLT received.
rate	This field displays the percentage of ICMP responses for ICMP requests.
rtt	This field displays the round trip time of the ping.
avg	This field displays the average round trip time to ping the specified IP address.
mdev	This field displays the standard deviation in the round trip time to ping the specified IP address.
max	This field displays the maximum round trip time to ping the specified IP address.
min	This field displays the minimum round trip time to ping the specified IP address.
reply from	This field displays the IP address from which the OLT received the ICMP response.

This example shows the current alarm LED status for each slot in the OLT. It also lists the type of alarm detected when the alarm LED is on.

```
sysname# show alarm-status
alarmMask= Voltage, Temperature, Fan, Ext Alarm, SFP
index   name    AlmLED  AlmItem(s)
-----  -----
1       system  OFF     -
```

This example shows the current and recent CPU utilization.

```
sysname# show cpu-utilization
CPU usage status:
  baseline 1715384 ticks
    sec   ticks   util sec   ticks   util sec   ticks   util sec   ticks
util
  -----  -----  -----
  0   657543  61.67  1   255118  85.13  2   394329  77.01  3   620008
63.85
  4   195580  88.60  5   791000  53.89  6   137625  91.98  7   508456
70.36
----- SNIP -----
```

The following table describes the labels in this display.

Table 291 show cpu-utilization

LABEL	DESCRIPTION
baseline	This field displays the number of CPU clock cycles per second.
sec	This field displays the historical interval. Interval 0 is the time starting one second ago to the current instant. Interval 1 is the time starting two seconds ago to one second ago. Interval 2 is the time starting three seconds ago to two seconds ago.
ticks	This field displays the number of CPU clock cycles the CPU was not used during the interval.
util	This field displays the CPU utilization during the interval. $\text{util} = [(\text{baseline} - \text{ticks}) / \text{baseline}] * 100$

CHAPTER 80

Syslog

This chapter introduces the syslog feature of the OLT.

80.1 Syslog Overview

Use the syslog feature to send logs to an external syslog server. 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. See [Section 104.2 on page 662](#) for more information on the OLT's logs.

80.2 Syslog Commands

Use these commands to configure the device's system logging settings and to configure the external syslog servers.

Table 292 Syslog Commands

COMMAND	DESCRIPTION	M	P
syslog	Enables syslog logging.	C	13
no syslog	Disables syslog logging.	C	13

Table 293 Syslog Server Commands

COMMAND	DESCRIPTION	M	P
syslog server <ip-address> level <level>	Sets the IP address of the syslog server and the severity level. level: 0-7	C	13
no syslog server <ip-address>	Deletes the specified syslog server.	C	13
syslog server <ip-address> inactive	Disables syslog logging to the specified syslog server.	C	13
no syslog server <ip-address> inactive	Enables syslog logging to the specified syslog server.	C	13
show syslog server	Displays the syslog server settings.	E	3

Table 294 Syslog Type Commands

COMMAND	DESCRIPTION	M	P
syslog type <type>	Enables syslog logging for the specified log type. <i>type:</i> system, interface, switch, aaa, ip	C	13
syslog type <type> facility <0-7>	Sets the file location for the specified log type.	C	13
no syslog type <type>	Disables syslog logging for the specified log type.	C	13
show syslog type <cr>	Displays the status of the log types.	E	3

Table 295 Syslog Upload Commands

COMMAND	DESCRIPTION	M	P
syslog upload	Enables uploading the file with log messages to an external syslog server.	C	13
no syslog upload	Disables uploading the file with log messages to an external syslog server.	C	13
syslog upload server <ip-address> inactive	Disables the syslog server that the file with log messages will be uploaded to.	C	13
no syslog upload server <ip-address>	Clears the syslog server IP address.	C	13
no syslog upload server all	Clears all syslog servers' information.	C	13
no syslog upload server <ip-address> inactive	Enables the syslog server that the file with log messages will be uploaded to.	C	13
syslog upload time <time>	Sets the time that you want the OLT to upload the file with log messages.	C	13
no syslog upload time	Clears the time that you want the OLT to upload the file with log messages.	C	13
syslog upload server <ip-address> username <name> password <pwd>	Enters the username and password of the specified syslog server.	C	13
syslog upload server <ip-address> username <name> password <pwd> filepath <filepath>	Enter the location of the syslog server that you want the file with log messages to be uploaded to.	C	13
show syslog upload	Displays the following information: • If syslog uploading is enabled. • The time that the file with log messages will be uploaded to the external syslog server. • Syslog server information	E	3
show syslog upload server	Displays the syslog server information.	E	3

CHAPTER 81

MAC Address

This chapter introduces the MAC address commands.

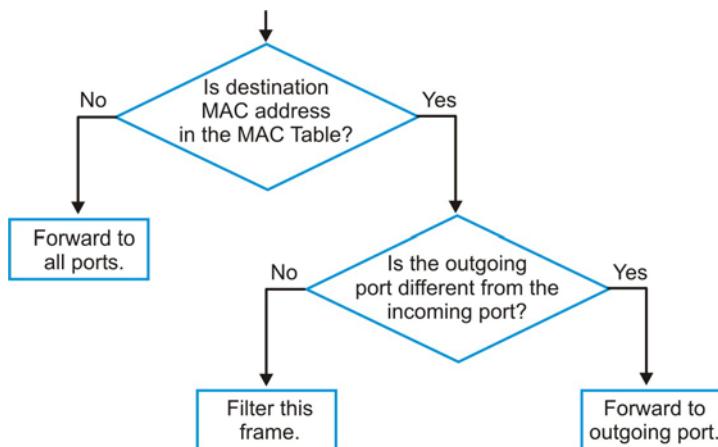
81.1 MAC Address Table Overview

The MAC Address table (a MAC table is also known as a filtering database) shows how frames are forwarded or filtered across the OLT's ports. When a device (which may belong to a VLAN group) sends a packet which is forwarded to a port on the OLT, the MAC address of the device is shown on the OLT's MAC table. It also shows whether the MAC address is dynamic (learned by the OLT) or static (manually entered by static MAC forwarding).

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

- 1 The OLT examines a received frame and learns the port from which this source MAC address came.
- 2 The OLT checks to see if the frame's destination MAC address matches a source MAC address already learned in the MAC table.
 - If the OLT has already learned the port for this MAC address, then it forwards the frame to that port.
 - If the OLT 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 OLT 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 244 MAC Address Table Flowchart



81.2 MAC Address Commands

Use these commands to look at the MAC address table and to configure MAC address learning. The OLT uses the MAC address table to determine how to forward frames.

Table 296 MAC Address Commands

COMMAND	DESCRIPTION	M	P
show mac-aging-time	Displays MAC learning aging time.	E	3
mac-aging-time <10-1000000>	Sets learned MAC aging time in seconds.	C	13
show mac address-table all [<sort>]	Displays MAC address table. You can sort by MAC address, VID or port. <i>sort</i> : MAC, VID, or PORT.	E	3
show mac address-table count Show mac-count	Displays the total number of MAC addresses in the MAC address table.	E	3
interface port-channel <aid>	Enters config-interface mode for configuring the specified port(s). <i>aid</i> : <pon eth>-<port>	C	13
pvid <1-4094>	Sets the specified interface's PVID.	C	13
frame-type <all tagged untagged>	Chooses to accept both tagged and untagged incoming frames (all), just tagged incoming frames (tagged) or just untagged incoming frames on a port (untagged).	C	13
max-frame-size <frame-size>	Sets the interface's maximum frame size. <i>frame-size</i> : 64 ~ 9216 bytes (Default: 9216)	C	13
no max-frame-size	Removes the interface's maximum frame size. <i>frame-size</i> : 64 ~ 9216 bytes (Default: 9216)	C	13
vlan <1-4094>	Sets the interface's VLAN. 1-4094: VLAN number	C	13
ingress-counter <aid>	Sets the ingress VLAN counter port. <i>aid</i> : <pon eth>-<port>	C	13
no ingress-counter <aid>	Removes the ingress VLAN counter port. <i>aid</i> : <pon eth>-<port>	C	13
show mac address-table port <aid T1 T2 ...T12>	Displays the MAC address table for the specified (trunk) port(s). <aid T1 T2...T12>: <i>aid</i> : <pon eth>-<port>, <T1 T2...T12>	E	3
show mac address-table port <aid T1 T2 ...T12> <sort>	Displays the MAC address table for the specified port(s). Sorted by MAC, Port or VID. <aid T1 T2...T12>: <i>aid</i> : <pon eth>-<port>, <T1 T2...T12> <i>sort</i> : MAC, VID, or PORT.	E	3
show mac address-table static	Displays the static MAC address table.	E	3
show mac address-table vlan <vlan-list> [<sort>]	Displays the MAC address table for the specified VLAN(s). Optionally, sorted by MAC, Port or VID. <i>sort</i> : MAC, VID, or PORT.	E	3
show mac address-table mac <mac-addr>	Displays a specified MAC entry.	E	3

Table 296 MAC Address Commands (continued)

COMMAND	DESCRIPTION	M	P
show mac address-table multicast	Displays the multicast MAC addresses learned by the OLT.	E	3
mac-flush [<port-num>]	Clears the MAC address table. Optionally, removes all learned MAC address on the specified port.	E	13

81.3 MAC Address Command Examples

This example shows the current MAC address table.

```
sysname# show mac address-table all
Port      VLAN ID      MAC Address        Type      Uniport-AID
GemFlow
CPU       1            5c:f4:ab:9c:e7:58  Static    N/A
N/A
CPU       2            5c:f4:ab:9c:e7:58  Static    N/A
N/A
total mac count:2
```

The following table describes the labels in this display.

Table 297 show mac address-table

LABEL	DESCRIPTION
Port	This is the port from which the above MAC address was learned. Drop: The entry is created from a filtering rule.
VLAN ID	This is the VLAN group to which this frame belongs.
MAC Address	This is the MAC address of the device from which this frame came.
Type	This shows whether the MAC address is dynamic (learned by the OLT) or static (manually entered using <code>mac-forward</code> commands, see Chapter 52 on page 411).
Uniport-AID	If the MAC address is learnt via a remote ONT and PON link, the MAC address table shows its UNI port Access ID here.
GemFlow	If the MAC address is learnt via a remote ONT and PON link on the OLT, the MAC address table shows its GEM (GPON Encapsulation Mode) flow ID here.

CHAPTER 82

ARP Table

This chapter introduces ARP Table.

82.1 ARP Table Overview

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.

82.1.1 How ARP Works

When an incoming packet destined for a host device on a local area network arrives at the OLT, the OLT's ARP program looks in the ARP Table and if it finds the address, it 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 OLT 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 OLT puts all ones in the target MAC field (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.

82.2 ARP Commands

The following section lists the commands for this feature.

Table 298 ARP Commands

COMMAND	DESCRIPTION	M	P
show ip arp	Displays the ARP table.	E	3
clear ip arp	Removes all of the dynamic entries from the ARP table.	E	13
clear ip arp interface port-channel <port-list>	Removes the dynamic entries learned on the specified port.	E	13

Table 298 ARP Commands (continued)

COMMAND	DESCRIPTION	M	P
clear ip arp ip <ip-address>	Removes the dynamic entries learned with the specified IP address.	E	13
no arp	Flushes the ARP table entries.	E	13

82.3 ARP Command Examples

This example shows the ARP table.

```
sysname# show ip arp
Index   IP           MAC          VLAN  Port    Age(s)  Type
 1      192.168.1.1  00:19:cb:00:00:02  1       CPU     0       static
```

The following table describes the labels in this display.

Table 299 show ip arp

LABEL	DESCRIPTION
Index	This field displays the index number.
IP	This field displays the learned IP address of the device.
MAC	This field displays the MAC address of the device.
VLAN	This field displays the VLAN to which the device belongs.
Port	This field displays the number of the port from which the IP address was learned. CPU indicates this IP address is the OLT's management IP address.
Age(s)	This field displays how long the entry remains valid.
Type	This field displays how the entry was learned. dynamic : The OLT learned this entry from ARP packets.

CHAPTER 83

Routing Table

This chapter introduces the routing table.

83.1 Routing Table Overview

The routing table contains the route information to the network(s) that the OLT can reach. The OLT automatically updates the routing table with the RIP information received from other Ethernet devices.

83.2 Routing Table Commands

The following section lists the commands for this feature.

Table 300 Routing Table Commands

COMMAND	DESCRIPTION	M	P
<code>interface route-domain <ip-address>/<mask-bits></code>	Configures a route-domain setting and enters the sub-commands for configuring it. <i>ip-address</i> : the IP address already created. <i>mask-bits</i> : the mask bits of the IP address, 0-32.	C	13
<code>exit</code>	Leaves from the configuration mode for an IPv4 or IPv6 routing domain.	C	13
<code>show ip route</code>	Displays the IP routing table.	E	3

83.3 Routing Table Command Examples

This example shows the current routing table.

```
sysname# show ip route
Terminology:
  L - this route is local interface          R - this route is reported by RIP
  B - this route is reported by BGP           O - this route is reported by OSPF
  S - this route is reported by Static Route

Route table in VPS00

Destination/Maskbits  Interface      Gateway      Metric  Type   Timer
-----  -----  -----  -----  -----  -----  -----
192.168.0.0/24        192.168.0.1    192.168.0.1    1       L     0
127.0.1.0/24          127.0.1.253   127.0.1.253   1       L     0

Route table in VPS01

Destination/Maskbits  Interface      Gateway      Metric  Type   Timer
-----  -----  -----  -----  -----  -----  -----
192.168.1.0/24        192.168.1.1    192.168.1.1    1       L     0
192.168.10.0/24       192.168.1.1    192.168.1.1    1       S     0
127.0.0.0/16           127.0.0.1      127.0.0.1      1       L     0

Route table in VPS02

Destination/Maskbits  Interface      Gateway      Metric  Type   Timer
-----  -----  -----  -----  -----  -----  -----
127.168.0.0/24        127.168.0.100  127.168.0.100  1       L     0
```

The following table describes the labels in this display.

Table 301 show ip route

LABEL	DESCRIPTION
Destination	This field displays the destination IP routing domain.
Maskbits	This field displays the number of bits in the subnet mask.
Interface	This field displays the IP address of the interface.
Gateway	This field displays the IP address of the gateway device.
Metric	This field displays the routing cost of the route.
Type	This field displays the method used to learn the route. L - this route is for a local interface R - this route is reported by RIP B - this route is reported by BGP O - this route is reported by OSPF S - this route is reported by Static Route
Timer	This field displays the number of remaining seconds this entry remains valid. It displays 0 if the entry is always valid.

CHAPTER 84

Running Configuration

Use these commands to manage the running configuration file. You can also copy settings between ports.

84.1 Running Configuration File

When you configure the OLT, the settings are saved as a series of commands in a configuration file on the OLT called `running-config`. You can perform the following with a configuration file:

- Back up OLT configuration once the OLT is set up to work in your network.
- Restore a previously-saved OLT configuration.
- Use the same configuration file to set all OLTs in your network to the same settings.

You may also edit a configuration file using a text editor. Make sure you use valid commands.

Note: The OLT rejects configuration files with invalid or incomplete commands.

84.2 Running Configuration Commands

The following table describes user-input values available in multiple commands for this feature.

Table 302 Running Configuration Commands User-input Values

COMMAND	DESCRIPTION
<code>options</code>	Possible values: active, name, speed-duplex, bpdu-control, flow-control, intrusion-lock, vlan1q, vlan1q-member, bandwidth-limit, vlan-stacking, port-security, broadcast-storm-control, mirroring, port-access-authenticator, queuing-method, igmp-filtering, spanning-tree, protocol-based-vlan, port-based-vlan, mac-authentication, trtcn, ethernet-oam, loopguard, arp-inspection, dhcp-snooping, l2protocol-tunnel, lldp, sFlow, pppoe-ia, arp-learning, cpu-protection, MSTP-operEdge, uni-port, olt, test, ip-mac-anti-spoofing.

The following section lists the commands for this feature.

Table 303 Running Configuration Commands

COMMAND	DESCRIPTION	M	P
<code>show running-config</code>	Displays the current configuration file. This file contains the commands that change the OLT's configuration from the default settings to the current configuration.	E	3
<code>show running-config interface port-channel <aid> [<options> [<...>]]</code>	Displays the current configuration that applies to the specified port. <code>aid: <pon eth>-<port></code>	E	3
<code>show running-config help</code>	Provides more information about the specified command.	E	3
<code>show running-config page</code>	Displays the current configuration file page by page.	E	3
<code>show running-config vlanAID</code>	Displays the current configuration file and lists the port membership of each VLAN.	E	3
<code>copy tftp config <index> <ip> <remote-file></code>	Restores configuration with the specified filename from the specified TFTP server to the specified configuration file on the OLT. <code>index: 1 or 2</code> Use <code>reload config <1 2></code> to restart the OLT and use the restored configuration. Note: This overwrites the configuration on the OLT with the file from the TFTP server.	E	13
<code>copy tftp flash <ip> <remote-file> <1 2></code>	Restores firmware via TFTP.	E	13
<code>copy running-config interface port-channel <port> <port-list></code>	Clones (copies) the attributes from the specified port to other port.	E	13
<code>copy running-config help</code>	Provides more information about the specified command.	E	13
<code>copy running-config tftp <ip> <remote-file></code>	Uses TFTP to back up the OLT's current configuration file to the TFTP server at the IP address you specify. Specify the name to use for the copied file.	E	13
<code>erase running-config</code>	Resets the OLT to the factory default settings.	E	13
<code>erase running-config ext</code>	Resets the OLT to the factory default settings except the management IP address.	E	13
<code>erase running-config interface port-channel <aid></code>	Resets the specified port to the factory default settings. <code>aid: <pon eth>-<port></code>	E	13
<code>erase running-config interface port-channel <aid> [<options> [<...>]]</code>	Resets the specified port to the factory default settings and optionally on a per-feature configuration basis. <code>aid: <pon eth>-<port></code>	E	13
<code>erase running-config help</code>	Provides more information about the specified command.	E	13

84.3 Running Configuration Command Examples

This example resets the OLT to the factory default settings.

```
sysname# erase running-config  
sysname# write memory
```

This example copies all attributes of port 1 to port 2 and copies selected attributes (active, bandwidth limit and STP settings) from port 1 to ports 5-8.

```
sysname# copy running-config interface port-channel pon-1 pon-2  
sysname# copy running-config interface port-channel pon-1 eth-5-eth-8  
active bandwidth-limit spanning-tree
```

CHAPTER 85

OLT Configuration

Use these commands to configure settings on the OLT.

85.1 OLT Configuration Commands

This table lists commands for OLT settings.

Table 304 OLT Configuration Commands

COMMAND	DESCRIPTION	M	P
<code>interface olt <aid></code>	Sets OLT configuration for the specified interface. <code>aid: pon-<port></code>	C	13
<code>07-state <sn></code>	Has the ONT with the specified serial number enter Emergency Stop State (07). Emergency Stop State is a ONU state defined in ITUT G.983. In this state, ONU will stop its transceiver output until the OLT requests it to exit from the state. <code>sn:</code> ONT serial number, 16 characters.	C	13
<code>fec</code>	Enables the Forward Error Correction (FEC) feature.	C	13
<code>no fec</code>	Disables the Forward Error Correction (FEC) feature.	C	13

Table 304 OLT Configuration Commands (continued)

COMMAND	DESCRIPTION	M	P
<pre>fec threshold [fec-code-word-th <value>][fec-corr-byte-th <value>][fec-corr-code-word-th <value>][fec-uncorr-code-word-th <value>][bip-byte-th <value>][bip-err-th <value>][rx-ploams-crc-err-th <value>][rx-ploams-nonidle-th <value>][positive-drift-th <value>][negative-drift-th <value>][rx-omci-packet-th <value>][rx-omci-packet-crc-err-th <value>][rei-counter-th <value>][unreceived-burst-th <value>][lcdgi-err-th <value>] [rdi-err-th <value>]</pre>	<ul style="list-style-type: none"> fec-code-word-th <value>: Enters the threshold of codewords that can be received in the Forward Error Correction (FEC) process. value: 0~4294967295 fec-corr-byte-th <threshold>: Enter the threshold of bytes that can be corrected by Forward Error Correction (FEC) feature. value: 0~4294967295 fec-corr-code-word-th <value>: Enter the threshold of codewords that can be corrected by Forward Error Correction (FEC) feature. value: 0~4294967295 fec-uncorr-code-word-th <value>: Enter the threshold of codewords that are allowed not to be corrected by Forward Error Correction (FEC) feature. value: 0~4294967295 bip-byte-th <value>: Enter the threshold of Bit Interleaved Parity (BIP) bytes that can be received. value: 0~4294967295 bip-err-th <value>: Enter the threshold of Bit Interleaved Parity (BIP) errors that are allowed. value: 0~4294967295 rx-ploams-crc-err-th <value>: Enter the threshold of Cyclic Redundancy Check (CRC) errors that are allowed in a received Physical Layer OAM Operations, Administrations and Maintenance (PLOAM) message. value: 0~4294967295 rx-ploams-nonidle-th <value>: Enter the threshold of non-idle PLOAM messages that can be received. value: 0~4294967295 positive-drift-th <value>: Enter the threshold of positive drifts that are allowed to increase the values of equalization delays. value: 0~4294967295 negative-drift-th <value>: Enter the threshold of negative drifts that are allowed to decrease the values of equalization delays. value: 0~4294967295 	C	13

Table 304 OLT Configuration Commands (continued)

COMMAND	DESCRIPTION	M	P
	<ul style="list-style-type: none"> <code>rx-omci-packet-th <value></code>: Enter the threshold of OMCI (Optical Network Unit Management and Control Interface) packets that can be received. <i>value</i>: 0~4294967295 <code>rx-omci-packet-crc-err-th <value></code>: Enter the threshold of Cyclic Redundancy Check (CRC) errors that are allowed in a received OMCI packet. <i>value</i>: 0~4294967295 <code>rei-counter-th <value></code>: Enter the threshold of Remote Error Indication (REI) counters for BER (Bit Error Rate) reports. <i>value</i>: 0~4294967295 <code>unreceived-burst-th <value></code>: Enter the threshold of burst that are allowed to be dropped. <i>value</i>: 0~4294967295 <code>lcdgi-err-th <value></code>: Enter the threshold of LCDGI/LCDGi (Loss of GEM Channel Delineation) errors that are allowed. <i>value</i>: 0~4294967295 <code>rdi-err-th <value></code>: Enter the threshold of RDI (Remote Defect Indication) errors that are allowed. <i>value</i>: 0~4294967295 	C	13
<code>no fec threshold</code>	Clears the fec thresholds values.	C	13
<code>fec threshold help</code>	Provides more information about the specified command.	C	13
<code>inactive</code>	Inactivates the OLT PON port.	C	13
<code>no 07-state <sn></code>	Disables Emergency Stop State (07) on the ONT with the specified serial number. <i>sn</i> : ONT serial number, 16 characters.	C	13
<code>no inactive</code>	Enables the OLT PON port.	C	13
<code>no ont-template</code>	Disables the ONT template.	C	13
<code>no ranging-distance</code>	Resets the ranging distance to default.	C	13
<code>ont-template</code>	Enables the ONT template.	C	13
<code>ranging-distance <max></code>	Configures the maximum ranging distance. <i>max</i> : The maximum distance is between 20 to 60 km	C	13
<code>register-method A</code>	Sets the OLT PON port's register method to A. Requires the serial number and password the ONT sends to match the ones you configure on the OLT.	C	13
<code>register-method C</code>	Sets the OLT PON port's register method to C. Requires the physical layer operations and maintenance (PLOAM) password the ONT sends to match what you configure on the OLT.	C	13
<code>register-method C-autolock</code>	Sets the OLT PON port's register method to C-autolock. Requires the serial number the ONT sends to match the one you configure on the OLT.	C	13

Table 304 OLT Configuration Commands (continued)

COMMAND	DESCRIPTION	M	P
register-method D	Sets the OLT PON port's register method to D. Automatically registers the ONT by template (onu-121~128) and brings it into service without checking the serial number or password.	C	13
register-method E	Sets the OLT PON port's register method to E. Non-volatile auto provision by template (onu-121~128).	C	13
register-method template-option <template-number>	Creates an olt OLT PON register method template (onu-121~128). <i>template-number</i> : 121~128	C	13
transceiver <type>	Sets the PON link's transceiver type (12). Transceiver type: 12: LIGENT_C	C	13
tx-disable <0 1>	Disables the PON link transceiver's transmission. 0: enable 1: disable	C	13
no rogue-onu-detection	Stops the rogue detection process.	C	13
rogue-onu-detection <cr>	Enables rogue ONT detection on the specified PON port, and the ONTs connected to the specified PON port will be still functioning.	C	13
rogue-onu-detection mode <prev-used full-scan>	Selects a mode for rogue ONT detection. <i>prev-used</i> : Selects this to scan the assigned Alloc-IDs (Allocation ID) that are unused. <i>full-scan</i> : Selects this to scan the assigned Alloc-IDs (Allocation ID) that are used unused.	C	13
exit	Leaves from the configuration commands.	C	13
no interface olt <aid>	Removes an OLT configuration for the specified interface. <i>aid</i> : pon-<port>	C	13
no interface olt all	Removes all OLT configurations.	C	13

CHAPTER 86

PON Port Status

This chapter introduces the PON port status commands.

86.1 PON Port Status Commands

Use these commands to display information about the PON ports.

Table 305 PON Port Commands

COMMAND	DESCRIPTION	M	P
show interfaces olt <aid> bandwidth	Displays the specified PON port's available bandwidth. <i>aid: pon-<pon></i>	E	3
show interfaces olt <aid> status	Displays the status of the specified PON port. <i>aid: pon-<pon></i>	E	3
show interfaces olt <aid> counter	Displays the specified PON port's counters. <i>aid: pon-<pon></i>	E	3
show interfaces olt <aid> rssи	Displays the specified PON port's RSSI (received signal strength indication) information. <i>aid: pon-<pon></i>	E	3
show interfaces olt <aid> fec	Displays the specified PON port's FEC (Forward Error Correction) information. <i>aid: pon-<pon></i>	E	3
show interfaces olt <aid> trafficmanagement	Displays the specified PON port's traffic management information. <i>aid: pon-<pon></i>	E	3
show interfaces olt <aid> registration	Displays the specified PON port's registration information. <i>aid: pon-<pon></i>	E	3
show interfaces olt <aid> unreg	Displays the specified PON port's unregistered ONT status. <i>aid: pon-<pon></i>	E	3
show interfaces olt <aid> ponbw-show	Displays the specified PON port's realtime bandwidth allocation. <i>aid: pon-<pon></i>	E	3

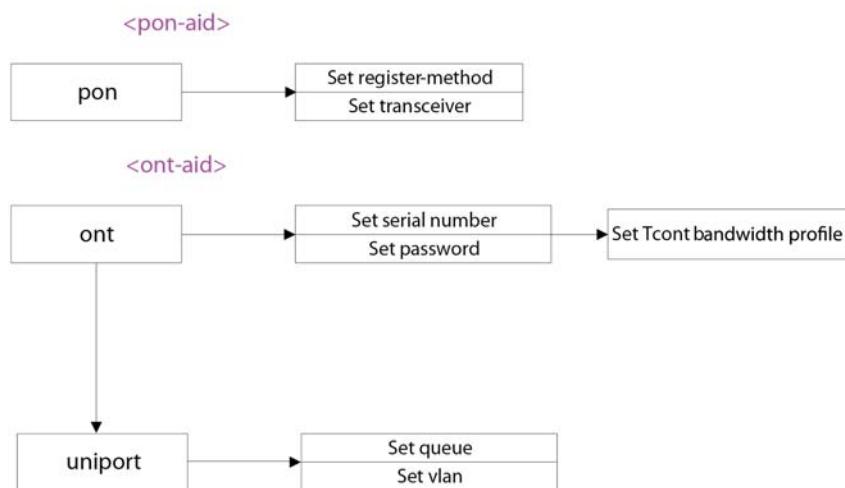
CHAPTER 87

Remote ONT

This chapter gives details on configuring remote ONTs. See [Chapter 51 on page 366](#) for basic examples of provisioning subscriber interfaces on an ONT or MDU.

87.1 Remote ONT Configuration Overview

Figure 245 Remote ONT Configuration Flow



A GPON network contains mainly active transmission equipment, namely the Optical Line Termination (OLT) at the service provider's central office and the Optical Network Unit (ONU) or Optical Network Termination (ONT) near end users.

87.2 ONT

The OLT supports registering a remote ONT when the PON link state is active. You can set the OLT to activate a remote ONT according to its serial number and password.

The following table introduces commands for configuring remote ONTs.

Table 306 Remote ONT Commands

COMMAND	DESCRIPTION	M	P
<code>remote ont <aid></code>	Configures remote ONT settings. <i>aid: ont-<pon>-<cont></i>	C	13
<code>alarm-profile <name-str></code>	Creates an ONT alarm profile to monitor the DDMI status of the ONT transceiver under configure mode. <i>name-str:</i> ONT alarm profile name. Use the following commands to create an ONT alarm profile: <code>sysname(config)# ont-alarm-profile TEST</code> <code>sysname(config-ont-alarm-profile)#{</code> Specify the lower and upper bounds for the laser bias current threshold, temperature threshold and power feed voltage threshold. Then apply the alarm threshold profile to an ONT. The default alarm profile monitors no DDMI information.		
<code>anti-mac-spoofing inactive</code>	Disables anti-MAC spoofing for the remote ONT.	C	13
<code>no anti-mac-spoofing inactive</code>	Enables anti-MAC spoofing for the remote ONT.	C	13
<code>bwgroup <id> usbwprofname <usbwprofname> dsbwprofname <dsbwprofname></code>	Sets the bandwidth group profile for the remote ONT. <i>id:</i> 1-40 <i>usbwprofname:</i> Upstream bandwidth profile name <i>dsbwprofname:</i> Downstream bandwidth profile name	C	13
<code>no bwgroup <id all></code>	Deletes bandwidth group profiles for the remote ONT. <i>id:</i> 1-40, delete the specified bandwidth group. <i>all:</i> Delete all bandwidth groups in the remote ONT.	C	13
<code>exit</code>	Exits from ONT configuration.		
<code>full-bridge <enable disable></code>	Enables full-bridge mode to allow the traffic of all four UNI ports once any one of them is configured.	C	13
<code>description <string></code>	Adds in a description for the ONT.	C	13
<code>inactive</code>	Turns off the ONT. You can configure more information such as a sequence number, password, or model name.	C	13
<code>loopback-test</code>	Executes a loopback test between the OLT and an ONT. The console displays whether the loopback test succeeded or failed.	C	13
<code>no inactive</code>	Activates on the ONT.	C	13
<code>password <password></code>	Sets the ONT password. <i>password:</i> ASCII characters (20 hex numbers).	C	13

Table 306 Remote ONT Commands (continued)

COMMAND	DESCRIPTION	M	P
plan-version <version>	Sets the ONT planned version to check if the current ONT setting is synchronized with the MIB database. <i>version</i> : The planned version is the firmware ID of the firmware that you want the ONT to use. Enter a string of up to 14 characters. Note: Use the <version> value of the mgmt-ont-img set image-version <version> command to set the ONT planned version. If the <version> values match, the connected ONTs can download firmware via the OLT.	C	13
plan-version <cr>	Clears the ONT planned version.	C	13
sn <sn>	Sets the ONT serial number in 8 hexadecimal characters (16 characters).	C	13
wan help	Provides more information about the specified command.	C	13
wan <id> [vlan <vid>] [priority <priority>] nat <disable enable>] [username <name>] [password <password>]	Sets the WAN profile settings for the remote ONT. <i>id</i> : 1-8 <i>vid</i> : 1-4094 <i>priority</i> : 0-7 <i>nat</i> : enable or disable the NAT feature <i>name</i> : username of PPPoE account, up to 50 ASCII characters <i>password</i> : password of PPPoE account, up to 50 ASCII characters	C	13
no wan <id all>	Removes ONT WAN configuration. <i>id</i> : 1-4 <i>all</i> : removes all ONT WAN configuration.	C	13
template-description <string>	Sets the ONT template description. <i>string</i> : up to 32 ASCII characters	C	13
option82 disable dhcp	Disables DHCP on the specified ONT.	C	13
option82 disable pppoe	Disables PPPoE on the specified ONT.	C	13
option82 pass-through dhcp	Disables DHCP passthrough.	C	13
option82 pass-through pppoe	Disables PPPoE passthrough.	C	13
fec <enable disable>	Enables or disables the ONT upstream Forward Error Correction (US FEC) mode.	C	13
no description	Clears the descriptions for all ONTs.	C	13
no option82 disable dhcp	Enables DHCP on the specified ONT.	C	13
no option82 disable pppoe	Enables PPPoE on the specified ONT.	C	13
no option82 pass-through dhcp	Enables DHCP passthrough.	C	13

Table 306 Remote ONT Commands (continued)

COMMAND	DESCRIPTION	M	P
no option82 pass-through pppoe	Enables PPPoE passthrough.	C	13
no plan-version	Removes the ONT planned version (14 characters) for checking if the current ONT setting is synchronized with the MIB database.	C	13
no template-description	Clears the template descriptions for all ONTs.	C	13
wan <wan-id> [vlan <vid>][priority <priority>][nat <disable enable>][username <name>][password <password>]	<p>Configures the following settings on the specified WAN connection:</p> <ul style="list-style-type: none"> • VLAN group • Priority level • NAT • Internet information <p>wan-id: You can check the WAN ID of the WAN connection that you want to configure in the Advanced Application > ONT Quick Setup > Wan screen.</p> <p>vid: Enters an ID of the VLAN group that you want the WAN connection to belong to.</p> <p>username <name>: Enters the username for the specified WAN connection.</p> <p>password <password>: Enters the password for the specified WAN connection.</p>	C	13
ont-alarm-profile <name>	Enters the sub-command mode for configuring an alarm profile for remote ONT DDMI threshold settings.	C	13
exit	Leaves the alarm profile configuration sub-command mode.	C	13
low-curr-thresh <0~79 N/A>	Specifies the low laser bias current threshold in mA. Use N/A to have the profile not check this parameter and let the ONU use its internal policy for it.	C	13
low-rxpower-thresh <-127~0 N/A>	Specifies the low received power threshold in dBm. Use N/A to have the profile not check this parameter and let the ONU use its internal policy for it.	C	13
low-temp <-40~100 N/A>	Specifies the low temperature threshold in degrees Celsius. Use N/A to have the profile not check this parameter and let the ONU use its internal policy for it.	C	13
low-txpower-thresh <-15.3~6.5 N/A>	Specifies the low transmission power threshold in dBm. Use N/A to have the profile not check this parameter and let the ONU use its internal policy for it.	C	13
low-volt-thresh <2.80~3.59 N/A>	Specifies the low power feed voltage threshold in volts. Use N/A to have the profile not check this parameter and let the ONU use its internal policy for it.	C	13
up-curr-thresh <0~79 N/A>	Specifies the upper laser bias current threshold in mA. Use N/A to have the profile not check this parameter and let the ONU use its internal policy for it.	C	13

Table 306 Remote ONT Commands (continued)

COMMAND	DESCRIPTION	M	P
up-rxpower-thresh <-127~0 N/A>	Specifies the upper received power threshold in dBm. Use N/A to have the profile not check this parameter and let the ONU use its internal policy for it.	C	13
up-temp <-40~100 N/A>	Specifies the upper temperature threshold in degrees Celsius. Use N/A to have the profile not check this parameter and let the ONU use its internal policy for it.	C	13
up-txpower-thresh <-15.3~6.5 N/A>	Specifies the upper transmission power threshold in dBm. Use N/A to have the profile not check this parameter and let the ONU use its internal policy for it.	C	13
up-volt-thresh <2.80~3.59 N/A>	Specifies the upper power feed voltage threshold in volts. Use N/A to have the profile not check this parameter and let the ONU use its internal policy for it.	C	13
onu-model name <14 char> model-ID <0~8> vendor-version <14 char> [software-version <14 char>][card1 <1~254>...]	Creates an ONT model name, and configures the following settings for the ONT: <ul style="list-style-type: none"> • Model ID • Vendor Version • Software Version • Card ID 	C	13
no onu-model all	Returns all connected ONTs to the default settings.	C	13
no onu-model name <14 char> <cr>	Returns the specified ONT to the default settings.	C	13
no onu-model name <14 char> [card1 card2...]	Returns the card settings of the specified ONT to default settings.	C	13
onu-model help	Provides more information about the specified command.	C	13
no ont-alarm-profile <cr>	Clears all unused ONT alarm threshold profiles.	C	13
no ont-alarm-profile <profile-name>	Clears the specified ONT alarm threshold profile.	C	13
show interfaces olt <aid> ont-template aid: pon-<port>	Displays the ont template status on the specified pon port.	E	3
show onu-model <cr>	Displays the following information of Zyxel ONT products. <ul style="list-style-type: none"> • Vendor Version • Software Version • Entity ID 	E	3
remote ont <aid> onu-reboot <cr> <1> <2> aid: ont-<pon>-<cont> pon-<pon>	Restarts the ONT with the current image or the specified image 1 or 2.	E	13

Table 306 Remote ONT Commands (continued)

COMMAND	DESCRIPTION	M	P
<code>remote ont <aid> download <file uri> <local file name> <user name> <password></code>	<p>Initiates file download from a URL or FTP server to the ONT.</p> <p><i>aid</i>: ont-<pon>-<ont> pon-<pon></p> <p><i>file uri</i>: server URI (for example <code>ftp://a.b.c/dir/config.xml</code>), length 1-100 characters.</p> <p><i>local file name</i>: local file name in the ONU (for example <code>config.xml</code>), length 1-25 characters.</p> <p><i>user name</i>: for the server, length 1-25 characters.</p> <p><i>password</i>: for the server, length 1-25 characters.</p>	E	13
<code>remote ont <aid> upload <local file name> <file uri> <user name> <password></code>	<p>Initiates upload of a local file from the ONT to a URL or FTP server.</p> <p><i>aid</i>: ont-<pon>-<ont> pon-<pon></p> <p><i>local file name</i>: Local file name in the ONU (for example <code>config.xml</code>), length 1-25 characters.</p> <p><i>file uri</i>: server URI (for example <code>ftp://a.b.c/dir/config.xml</code>), length 1-100 characters.</p> <p><i>user name</i>: for the server, length 1-25 characters.</p> <p><i>password</i>: for the server, length 1-25 characters.</p>	E	13
<code>remote ont <aid> restore-time</code>	<p>Displays how long it has been since the ONT restored configuration the last time.</p> <p>Note: The ONT must support this feature as well to use this command.</p>	E	13
<code>show remote pat-binds</code>	<p>Displays the port address translation binding table.</p> <p>For your convenience, the OLT binds specific socket ports to designated ONTs so that clicking the ONT's ONT AID link in the OLT Web Configurator's Advanced Application > ONT Quick Setup screen redirects to the ONT's Web Configurator.</p> <p>The IP binding is automatically assigned when you refresh the ONT Quick Setup Web Configurator screen.</p> <p>The ONT must have Web Configurator access privileges for the WAN interface enabled first.</p>	E	13
<code>ont-copy source-ont <aid> dest-ont <aid></code>	Copies the specified ONT template configuration to the specified ONT(s).	E	13
	<p><i>source-ont <aid></i>: ont-<pon>-<ont></p> <p><i>dest-ont <aid></i>: ont-<pon>-<ont></p>		

Table 306 Remote ONT Commands (continued)

COMMAND	DESCRIPTION	M	P
no remote ont <aid>	Removes ONT configuration for specified ONT. The related ontcard/ontenet/ontvDSL/ontvenet/ontpots/ontvideo/uniport configuration will be also removed. aid: ont-<pon>-<ont> pon-<pon>	C	13
no remote ont all	Removes all ONT configuration. The related ontcard/ontenet/ontvDSL/ontvenet/ontpots/ontvideo/uniport configuration will be also removed.	C	13
no remote ont password <password>	Removes an ONT using its GPON password.	C	13
no remote ont sn <sn>	Removes an ONT using its serial number.	C	13
show remote ont password <password>	Displays the information of an ONT using its GPON password.	E	3
show ont-alarm-profile	Displays the configuration of all the ONT alarm profiles.	E	13
show ont-alarm-profile <profile-name>	Displays the configuration of the specified ONT alarm profile.	E	13
show remote ont <aid>	Show the specified ONT's information. aid: ont-<pon>-<ont>	E	3
show remote ont <aid> alarm-indication	Displays the specified ONT's alarm indication. aid: ont-<pon>-<ont>	E	13
show remote ont <aid> bwgroup	Displays the specified ONT's bandwidth group information. aid: ont-<pon>-<ont>	E	13
show remote ont <aid> option82	Displays the specified ONT's option 82 information. aid: ont-<pon>-<ont>	E	13
show remote ont <aid> counter	Displays the specified ONT's counters. aid: ont-<pon>-<ont>	E	13
show remote ont <aid> dDMI current	Displays the specified ONT's current DDMI information. aid: ont-<pon>-<ont>	E	13
show remote ont <aid> dDMI history	Displays the specified ONT's historical DDMI information for 15 minute periods over the past day. aid: ont-<pon>-<ont>	E	13
show remote ont <aid> config	Displays the specified ONT's configuration information. aid: ont-<pon>-<ont>	E	3
show remote ont sn <sn>	Displays the configuration information of an ONT using its serial number.	E	3
show remote ont <cr>	Displays all ONT information.	E	3

Table 306 Remote ONT Commands (continued)

COMMAND	DESCRIPTION	M	P
<code>show remote ont filter < pon-<aid> <serial number> is oos-nr .. ></code>	<p>Displays the status of ONTs matching the filter you specify.</p> <p><code>pon-<aid></code>: Show ONT information by PON port.</p> <p><code>is</code>: Show ONTs with an IS (In Service) status.</p> <p><code>oos</code>: Show ONTs with an OOS (Out Of Service) status.</p> <p><code>oos-lo</code>: Show ONTs with a Line Card Out Of Service status.</p> <p><code>oos-nr</code>: Show ONTs with an Out Of Service Not Registered status.</p> <p><code>oos-cd</code>: Show ONTs with an Out Of Service OMCC Down status.</p> <p><code>oos-np</code>: Show ONTs with an Out Of Service Not Provisioned status.</p> <p><code>oos-ad</code>: Show ONTs with an Out Of Service Admin Down status.</p> <p><code>oos-op</code>: Show ONTs with an Out Of Service Operation Down status.</p>	E	3
<code>show remote ont summary</code>	Displays a summary of ONT status.	E	3
<code>show remote ont unreg</code>	Displays unregistered ONT status information.	E	3
<code>show remote ont template <aid></code>	<p>Displays ONT template information for the specified template.</p> <p><code>aid: pon-<pon> ont-<pon>-<121~128></code></p>	E	13
<code>show remote ont template</code>	Displays all ONT template information.	E	3
<code>show remote ont <aid> status-history</code>	Displays the ONU status history.	E	13
<code>show remote ont <aid> wan-status</code>	Displays the ONT WAN status.	E	13
<code>remote ont <aid> onu-reset[<cr> <1> <2>]</code>	<p>Resets the ONU.</p> <p>1: Load factory default</p> <p>2: Reset default</p> <p><code>aid: ont-<pon>-<ont> / pon-<pon></code></p>	E	13
<code>remote ont <aid> config-status</code>	Gets the ONT's current configuration status.	E	13

See [Section 6.6 on page 75](#) for more information on how to upgrade ONTs to the latest firmware via the OLT.

Table 307 Remote ONT Firmware Upgrade Commands

COMMAND	DESCRIPTION	M	P
mgmt-ont-img	Enter manager ONT image mode.	E	13
clear image-version	Clears the firmware version of the ONT firmware file uploaded to the OLT.	E	13
clear upgrade-status <aid> <cr>	Clears the firmware upgrades' status of the ONTs connect to the specified port. Clears the firmware upgrade status of the specified ONT. aid: pon-<pon> ont-<pon>-<ont>	E	13
clear upgrade-status <cr>	Clears the firmware upgrades' status of all connected ONTs.	E	13
clear waiting-queue <aid> <cr>	Clears the waiting queue for firmware upgrades on the specified port. aid: pon-<pon> ont-<pon>-<ont>	E	13
clear waiting-queue <cr>	Clears the waiting queue for firmware upgrades on all ports.	E	13
disp auto-reboot <cr>	Displays if all connected ONTs will reboot automatically after firmware upgrades.	E	13
disp image-info	Displays the firmware information of the ONT firmware file uploaded to the OLT.	E	13
disp queue <cr>	Displays the waiting queue' status for firmware upgrades.	E	13

COMMAND	DESCRIPTION	M	P
disp upgrade-status <aid> <cr>	<p>Displays the firmware upgrades' status of:</p> <ul style="list-style-type: none"> The ONTs that connect to the specified port The specified ONT <p>Displays the firmware upgrade status of the specified ONT.</p> <p>aid: pon-<pon> ont-<pon>-<ont></p> <p>One of the following results appears:</p> <ul style="list-style-type: none"> MATCHED: The ONT's planned version and running firmware version are identical. Downloading: The ONT is downloading the latest firmware from the OLT. The image version of the ONT firmware file uploaded to the OLT and the ONT's planned version are identical. Failed: The ONT didn't upgrade firmware successfully. Failed with ONU Down: The ONT didn't upgrade firmware successfully, because the optical network of the ONT is down. Not found the matching image: The ONT didn't upgrade firmware successfully, because the image version of the ONT firmware file uploaded to the OLT and the ONT's planned version are not identical. No planned version: The ONT's planned version hasn't configured yet. Timeout: The ONT didn't upgrade firmware successfully, because there was no response from the OLT. ONU not ready: The ONT didn't upgrade firmware successfully, because the ONT is not ready. SWDL queue full: The ONT didn't upgrade firmware successfully, because the waiting queue is full. In waiting queue: The ONT is in the waiting queue, and waiting for the firmware upgrade process to begin. Change to image(1)/(2): Image 1/2 is in use now for the ONT's running firmware, because the ONT's planned version and image 1/2 firmware version are identical. No Image: No ONT firmware file is uploaded to the OLT. Already successful: This message only appears when you're checking the ONTs firmware upgrades status of the specified port. An ONT has already upgraded firmware successfully. Already changed to image (1)/(2): This message only appears when you're checking the ONTs firmware upgrades status of the specified port. Image 1/2 is in use now for the ONT's running firmware, because the ONT's planned version and image 1/2 firmware version are identical. 	E	13
disp upgrade-status <cr>	Displays the firmware upgrades' status of all connected ONTs.	E	13
release-image <cr>	Removes the ONT firmware file uploaded to the OLT. This will release more volatile memory on the OLT.	E	13
set auto-reboot <enable disable> <cr>	Reboots or not reboots all connected ONTs after the firmware upgrade process is complete.	E	13

COMMAND	DESCRIPTION	M	P
set image-version <version>	<p>Sets the image version of the ONT firmware file uploaded to the OLT. Enter a string of up to 14 characters.</p> <p>Note: Use the firmware ID provided by the ONT vendor.</p> <p>If the <version> values of the following commands match, the connected ONTs can download firmware via the OLT.</p> <ul style="list-style-type: none">• This command• remote ont <aid> plan-version <version> command	E	13

COMMAND	DESCRIPTION	M	P
exit	Leaves from the configuration commands.	E	13
remote ont <aid> check-version	<p>Checks the ONT version and performs software download.</p> <p>aid: ont-<pon>-<ont> pon-<pon></p> <p>Up to three ONTs can upgrade firmware via the OLT at the same time.</p> <p>The standby firmware of the ONT will be updated when the ONT is downloading firmware via the OLT.</p> <p>One of the following results appears:</p> <ul style="list-style-type: none"> • MATCHED: The ONT's planned version and running firmware version are identical. • Downloading: The ONT is downloading the latest firmware from the OLT. The image version of the ONT firmware file uploaded to the OLT and the ONT's planned version are identical. • Failed: The ONT didn't upgrade firmware successfully. • Failed with ONU Down: The ONT didn't upgrade firmware successfully, because the optical network of the ONT is down. • Not found the matching image: The ONT didn't upgrade firmware successfully, because the image version of the ONT firmware file uploaded to the OLT and the ONT's planned version are not identical. • No planned version: The ONT's planned version hasn't configured yet. • Timeout: The ONT didn't upgrade firmware successfully, because there was no response from the OLT. • ONU not ready: The ONT didn't upgrade firmware successfully, because the ONT is not ready. • SWDL queue full: The ONT didn't upgrade firmware successfully, because the waiting queue is full. • In waiting queue: The ONT is in the waiting queue, and waiting for the firmware upgrade process to begin. • Change to image(1)/(2): Image 1/2 is in use now for the ONT's running firmware, because the ONT's planned version and image 1/2 firmware version are identical. • No Image: No ONT firmware file is uploaded to the OLT. • Already successful: This message only appears when you're checking the ONTs firmware upgrades status of the specified port. An ONT has already upgraded firmware successfully. • Already changed to image (1)/(2): This message only appears when you're checking the ONTs firmware upgrades status of the specified port. Image 1/2 is in use now for the ONT's running firmware, because the ONT's planned version and image 1/2 firmware version are identical. 	E	13

87.3 UNI Port Settings

Use these commands to configure settings on individual UNI ports (ports on the subscriber devices). See [Section 73.5 on page 515](#) and [Section 73.6 on page 516](#) for UNI port VoIP commands.

87.3.1 UNI Port General Commands

These commands apply to any UNI port.

Table 308 UNI Port General Command Parameters

LABEL	DESCRIPTION	M	P
no remote uniport all	Removes all UNI port configuration.	C	13
no remote uniport <aid>	Removes UNI port configuration for the specified UNI port. <i>aid: uniport-<pon>-<ont>-<card>-<port></i>	C	13
remote uniport <aid>	Configures UNI port settings. <i>aid: uniport-<pon>-<ont>-<card>-<port></i>	C	13
inactive	Deactivates the specified UNI port.	C	13
no inactive	Activates the specified UNI port.	C	13
pmenable <cr>	Enables PM (performance monitoring) to get counters on the specified UNI port.	C	13
pmenable 32-bit	Enables PM (performance monitoring) to get 32-bit counters on the specified UNI port.	C	13
pmenable 64-bit	Enables PM (performance monitoring) to get 64-bit counters on the specified UNI port.	C	13
no pmenable	Disables PM (performance monitoring) to get counters on the specified UNI port.	C	13
port-speed <auto 10-full 100-full 1000-full 2.5G-full>	Sets the auto detection configuration attribute in the physical path termination point Ethernet UNI ME as defined in G984.4. Use auto ora specific rate and duplex mode.	C	13
exit	Leaves the slot configuration sub-commands.	C	13
show remote uniport <aid> pm-counter <cr>	Displays the specified UNI port's PM (performance monitoring) counter. <i>aid: uniport-<pon>-<ont>-<card>-<uniport></i>	E	13
show remote uniport <aid> pmenable <cr>	Displays if PM (performance monitoring) is enabled or disabled on the specified UNI port. <i>aid: uniport-<pon>-<ont>-<card>-<uniport></i>	E	13

87.3.2 UNI Port Queue Settings

Use the `queue` command to configure a UNI port traffic class.

Table 309 UNI Port QoS Queue Command Parameters

LABEL	DESCRIPTION	M	P
<code>remote uniport <aid></code>	<p>Configures UNI port settings.</p> <p><i>aid: uniport-<pon>-<ont>-<card>-<port></i></p> <p>Please select the corresponding card ID according to the desired card type.</p> <p>Card 1: 10_100_1000Baset</p> <p>Card 2: VEIP</p> <p>Card 3: POTS</p> <p>Card 4: VIDEO</p> <p>Card 5: 10_100Baset</p> <p>Card 6: 10_100_1000Baset_VEIP</p>	C	13
<code>queue tc <tc> priority <priority> weight <weight></code> <code>usbwprofilename <usbwprofilename></code> <code>dsbwprofilename <dsbwprofilename></code> <code>dsoption <dsoption></code> <code>bwsharegroupid <bwsharegroupid></code> <code>[<dsbwsharegroupid>]</code>	<p>Configures a UNI port QoS queue.</p> <p><i>tc:</i> The IEEE 802.1P QoS traffic class 0~7 of traffic to which to apply this queue.</p> <p><i>priority:</i> 0~7. This is reserved for future development since the ONT does not support this QoS feature now.</p> <p><i>weight:</i> Queue weight: 0~255. You can configure different queues with the same queue priority level. The OLT then uses Weighted Round Robin (WRR) scheduling to service these queues on a rotating basis based on their queue weight. The higher a queue's weight, the more service it gets. This is reserved for future development since the ONT does not support this QoS feature now.</p>	C	13

Table 309 UNI Port QoS Queue Command Parameters (continued)

LABEL	DESCRIPTION	M	P
	<p><i>usbwprofname</i>: The upstream bandwidth profile to use for the traffic class.</p> <p><i>dsbwprofname</i>: The downstream bandwidth profile to use for the traffic class.</p> <p><i>dsoption</i>: olt ont. Set whether to apply the downstream rate limit function to the OLT (olt) or the ONT (ont).</p> <p><i>bwsharegroupid</i>: Specify the ID (1-40) of the bandwidth group on this ONT to put the QoS queues into. You created the bandwidth group when you configured the ONT setup. The UNI port will share the bandwidth defined by the bandwidth group.</p> <p><i>dsbwsharegroupid</i>: Specify the ID (1-40) of the downstream bandwidth group on this ONT to put the QoS queues into. You can use this when the <i>dsoption</i> is olt. You created the bandwidth group when you configured the ONT setup. The UNI port will share the downstream bandwidth defined by the bandwidth group. The OLT uses <i>bwsharegroupid</i> as the default value.</p>	C	13
queue help	Provides more information about the specified command.	C	13
no queue <cr>	Deletes all QoS queue setting from the UNI port.	C	13
no queue tc <0-7>	Deletes the specified QoS queue setting from the UNI port.	C	13
show remote uniport <aid> queue	<p>Displays the specified UNI port queue.</p> <p>aid: uniport-<pon>-<ont>-<card>-<uniport></p>	E	13

This example creates a traffic class mapping rule. The traffic class allocates bandwidth which will be used for the UNI port vlan.

Before creating the traffic class rule, create the QoS bandwidth profile that controls the upstream and downstream rates of the UNI port VLAN.

Qos bandwidth example:

```

qos bwprof 0MSir_0MAir_1GPir sir 0 air 0 pir 1200000
qos bwprof 20m sir 1024 air 2048 pir 20000
qos bwprof 40m sir 1024 air 2048 pir 40000

```

Before creating traffic class rule, create a bandwidth group ID when you create the ONT. The traffic class references the bandwidth group ID.

```

remote ont ont-1-3
  sn 5A59584503005457
  password 44454641554C542D3100
  full-bridge disable
  no inactive
  bwgroup 1 usbwprofname 0MSir_0MAir_1GPir dsbwprofname 0MSir_0MAir_1GPir

```

This example creates 2 traffic classes (tc3 and tc4) on uniport-1-1 of ONT-1-3.

- Tc3 limits upstream and downstream rates to 20 Mbps.
- Tc4 limits upstream and downstream rates to 40 Mbps.

```
sysname (config)# remote uniport uniport-1-3-1-1
sysname (config-remote-uniport)# queue tc 3 priority 3 weight 0 USbwprofilename 20m
DSBwprofilename 20m dsoption olt bwsharegroupid 1
sysname (config-remote-uniport)# queue tc 4 priority 4 weight 0 USbwprofilename 40m
DSBwprofilename 40m dsoption olt bwsharegroupid 1
```

This example removes traffic class "3".

```
sysname (config)# remote uniport uniport-1-3-1-1
sysname (config-remote-uniport)# no queue tc 3
```

This example removes all traffic classes on uniport-1-1 of ONT-1-3.

```
sysname (config)# remote uniport uniport-1-3-1-1
sysname (config-remote-uniport)# no queue tc
```

This example shows the protocol base VLAN rules on uniport-1-1 of ONT-1-3.

```
sysname# show remote uniport uniport-1-3-1-1 protocol-based
Uniport Ether type Vlan Priority
----- ----- ---- -----
uniport-5-1-3-1-1    3      3      0
uniport-5-1-3-1-1    4      4      0
```

87.3.3 UNI Port VLAN Settings

Use the `vlan` command to configure VLAN flow settings for the subscriber port on the remote ONT. See [Figure 233 on page 484](#) for where the VLAN IDs in the UNI port VLAN command fit in the reference configuration defined in ITU-T G.984.1.

Table 310 UNI Port VLAN Command Parameters

LABEL	DESCRIPTION	M	P
<code>remote uniport <aid></code>	Configures UNI port settings. <code><aid></code> : <code>uniport-<pon>-<ont>-<card>-<port></code>	C	13
<code>vlan <UNIVID SVID:CVID> [network <VID SVID[/SPRI]:CVID>] [txtag <tag untag priotag>] [pbitprof <prof>] [gemport <gem-port>] [ingprof <name>] [aesencrypt <enable disable>] [TR156 <enable disable>] [sharepri <0-7 off>] [macnum <1-6>] [active <on off>]</code>	Configures UNI port VLAN flow settings. UNIVID SVID:CVID: UNI VLAN ID (1~4094) of traffic on the UNI port to which to apply this command's VLAN, QoS ingress profile, and AES encryption settings. network: The Network Node Interface (NNI) VID to which the ONT translates the UNI VLAN ID before sending traffic to the OLT. Use a number different from the UNI VLAN to apply VLAN translation. txtag: Sets whether the ONT sends downstream traffic with a VLAN tag or untagged. <code>gem-port</code> : The GEM port to assign to the ONT VLAN (range is 256 ~). A GEM port ID represents a specific traffic flow or group of flows between the OLT and one or more ONUs. The GEM port ID is unique per GPON interface (see TR-156 for more information). <code>ingprof</code> : The QoS ingress profile to apply to the VLAN's traffic (IEEE 802.1p priority bit to TC mapping profile). <code>aesencrypt</code> : The UNI port VLAN to assign to the gem port. This setting enables gem port AES encryption. <code>TR156</code> : Reserved for future development. Use "disable" as the default. <code>sharepri</code> : The share priority in a downstream share group if the dsoption is olt. The value "off" means discard the downstream share group setting. If other VLANs have "0-7" set in the same downstream share group, the value cannot be set to "off". The priority value means the priority of VLAN of downstream rate limit and is unique in the same downstream bandwidth group. 7 has the highest priority. <code>macnum</code> : You can limit the maximum number of downstream traffic MAC addresses if the dsoption is olt. <code>active</code> : Turn the VLAN flow setting rule on or off on the UNI port.	C	13
<code>vlan help</code>	Provides more information about the specified command.	C	13
<code>no vlan <uni-vid></code>	Deletes the VLAN flow settings from the UNI port.	C	13

Table 310 UNI Port VLAN Command Parameters (continued)

LABEL	DESCRIPTION	M	P
no vlan all	Deletes all of the UNI port's VLAN flow settings.	C	13
show remote uniport <aid> vlan <uni-vid>	Displays the specified UNI port's VLAN flow settings for the specified VLAN. aid: uniport-<pon>-<ont>-<card>-<port>	E	13
show remote uniport <aid> vlan <cr>	Displays all of the specified UNI port's VLAN flow settings. aid: uniport-<pon>-<ont>-<card>-<port>	E	13

Before creating a VLAN rule, we need to create the tc (traffic class) that controls the VLAN's bandwidth.

In the previous section we created tc3 and tc4 as below.

```
remote uniport uniport-1-3-1-1
queue tc 3 priority 3 weight 0 USbwprofilename 20m DSbwprofilename 20m dsoption olt
bwsharegroupid 1
queue tc 4 priority 4 weight 0 USbwprofilename 40m DSbwprofilename 40m dsoption olt
bwsharegroupid 1
```

To map the IEEE 802.1p priority bit from a VLAN to a traffic class , we need to create an ingress profile to use when we create the UNI port VLAN.

```
qos ingprof Pbit3ToTc3 dot1p3tc 3
qos ingprof Pbit4ToTc4 dot1p4tc 4
```

This example creates VLAN 103 on the ONT with the following actions:

- The ONT sends downstream VLAN 103 traffic out untagged.
- The ONT assigns VLAN 103 traffic to gemport 256.
- The ONT assigns traffic with VLAN 103 and priority bit 3 to tc4 based on ingress profile Pbit3ToTc3. Tc3 limits the upstream and downstream traffic rates to 20 Mbps.
- The gem port 256 does not enable AES encryption.
- The uniport VLAN does not use TR156 mode.

```
sysname (config)# remote uniport uniport-1-3-1-1
sysname (config-remote-uniport)# vlan 103 txtag untag gempport 256 ingprof
Pbit3ToTc3 aesencrypt disable TR156 disable
```

This example creates VLAN 203 on the ONT with the following actions:

- The ONT sends downstream VLAN 203 traffic out untagged.
- The ONT assigns VLAN 203 traffic to gempport 257.
- The ONT assigns traffic with VLAN 103 and priority bit 4 to tc4 based on ingress profile Pbit4ToTc4. Tc4 limits the upstream and downstream traffic rates to 40 Mbps.
- The gem port 257 does not enable AES encryption.
- The uniport VLAN does not use TR156 mode.

```
sysname (config)# remote uniport uniport-1-3-1-1
sysname (config-remote-uniport)# vlan 203 txtag untag gempport 257 ingprof
Pbit4ToTc4 aesencrypt disable TR156 disable
```

This example deletes VLAN rules on uniport-1-1 of ONT-1-3.

```
sysname (config)# remote uniport uniport-1-3-1-1
sysname (config-remote-uniport)# no vlan 103
sysname (config-remote-uniport)# no vlan 203
```

This example shows the VLAN rules on UNI port-1-1 of ONT-1-3.

```
sysname# show remote uniport uniport-1-3-1-1 vlan
|AID          | UNI-VID Status   NNI-VID     Tag      PBit_Prof DSCP_to_PBIT      Ing_Prof TC
GemP AES_Ept  SP  MN
-----+-----+-----+-----+-----+-----+-----+-----+
v|uniport-1-3-1-1 |    103    Idle     103    untag      inactive      Pbit3ToTc3
3 256 disable of 1
-----+-----+-----+-----+-----+-----+-----+-----+
v|uniport-1-3-1-1 |    203    Idle     203    untag      inactive      Pbit4ToTc4
4 257 disable of 1
-----+-----+-----+-----+-----+-----+-----+-----+
```

87.3.4 UNI Port Protocol-based VLAN Settings

Use the `protocol-based` command to configure UNI port protocol-based VLAN.

Table 311 UNI Port Protocol-based VLAN Command Parameters

LABEL	DESCRIPTION	M	P
<code>remote uniport <aid></code>	Configures UNI port settings. <i>aid</i> : <code>uniport-<pon>-<ont>-<card>-<port></code>	C	13
<code>protocol-based <ipoe pppoe arp ipv6> [vlan <VID SVID:CVID>] [def-pbit <priority>] [active <on off>]</code>	Configures protocol-based VLAN flow settings for the UNI port. ipoe pppoe arp ipv6: IPoE packet ethertype = 0x0800 PPPoE packet ethertype = 0x8863 , 0x8864 ARP packet ethertype = 0x0806 IPv6 packet ethertype = 0x86DD vlan: The VLAN the ONT inserts in the protocol packet. def-pbit: The priority bit the ONT inserts in the protocol packet. active: Enable or disable the protocol packet rule.	C	13

Table 311 UNI Port Protocol-based VLAN Command Parameters (continued)

LABEL	DESCRIPTION	M	P
no protocol-based <ipoe pppoe arp ipv6>	Deletes the protocol-based vlan flow. ipoe pppoe arp ipv6: IPoE packet ethertype = 0x0800 PPPoE packet ethertype = 0x8863 , 0x8864 ARP packet ethertype = 0x0806 IPv6 paceket ethertype = 0x86DD	C	13
no protocol-based <cr>	Deletes all of the UNI port's protocol-based VLAN flow settings.	C	13
show remote uniport <aid> protocol-based <cr>	Displays the specified UNI port's protocol-based VLAN flow settings. <i>aid: uniport-<pon>-<ont>-<card>-<uniport></i>	E	13

This example creates 3 protocol-based VLAN rules on ONT-1-3 uniport-1-1 to have the ONT do the following:

- Insert vlan103 and pbit 4 in IPoE packets the ONT forwards to the OLT.
- Insert vlan103 and pbit 4 in ARP packets the ONT forwards to the OLT.
- Insert vlan203 and pbit 0 in PPPoE packets the ONT forwards to the OLT.

```
sysname (config)# remote uniport uniport-1-3-1-1
sysname (config-remote-uniport)# protocol-based ipoe vlan 103 pbit 4
sysname (config-remote-uniport)# protocol-based pppoe vlan 203 pbit 0
sysname (config-remote-uniport)# protocol-based arp vlan 103 pbit 4
```

This example deletes 3 protocol-based VLAN rules on ONT-1-3 uniport-1-1.

```
sysname (config-remote-uniport)# no protocol-based ipoe
sysname (config-remote-uniport)# no protocol-based pppoe
sysname (config-remote-uniport)# no protocol-based arp
```

This example shows protocol-based VLAN rules on ONT-1-3 uniport-1-1.

```
sysname# show remote uniport uniport-1-3-1-1 protocol-based
      Uniport   Ether type   Vlan   Priority
      -----   -----   ----   -----
uniport-1-3-1-1       ipoe     103        4
uniport-1-3-1-1       pppoe    203        0
uniport-1-3-1-1       arp      103        4
```

87.3.5 UNI Port PVID Settings

Use the `pvid` command to configure UNI port default VLAN settings.

Table 312 UNI Port PVID Command Parameters

LABEL	DESCRIPTION	M	P
<code>remote uniport <aid></code>	Configures UNI port settings. <i>aid: uniport-<pon>-<ont>-<card>-<port></i>	C	13
<code>pvid [VID SVID:CVID] [def-pbit <priority>] [active <on off>]</code>	Configures default VLAN settings for the UNI port. VID SVID:CVID: The default VLAN ID the ONT applies to untagged packets it receives from the subscriber ports. def-pbit: The priority bit (0~7) the ONT inserts in the packets to which it applies the PVID. active: Enable or disable the PVID rule.	C	13
<code>no pvid</code>	Deletes default VLAN settings for the UNI port.	C	13
<code>show remote uniport <aid> pvid <cr></code>	Displays the specified UNI port's default VLAN settings. <i>aid: uniport-<pon>-<ont>-<card>-<uniport></i>	E	13

This example sets up PVID on uniport-1-1 of ONT-1-3. Untagged packets from port 1 of ONT-1-3 will be tagged by the ONT with VID 203 and priority bit 2.

```
sysname (config)# remote uniport uniport-1-3-1-1
sysname (config-remote-uniport)# pvid 203 def-pbit 2 inactive
```

This example deletes the PVID on uniport-1-1 of ONT-1-3.

```
sysname (config)# remote uniport uniport-1-3-1-1
sysname (config-remote-uniport)# no pvid
```

This example shows the PVID setting on uniport-1-1 of ONT-1-3.

```
sysname # show remote uniport uniport-1-3-1-1 pvid
Active: Yes
port default vlan and priority:
pvid is 203
pri is 2
```

87.3.6 UNI Port IGMP Channel Settings

Use the `igmpchannel` command to configure a UNI port with multicast subscriber information.

Table 313 UNI Port IGMP Channel Commands

LABEL	DESCRIPTION	M	P
<code>remote uniport <aid></code>	Configures UNI port settings. <i>aid: uniport-<pon>-<ont>-<card>-<port></i>	C	13
<code>igmpchannel <uni-vid> <cr></code>	Creates an IGMP channel on this port. <i>uni-vid: The default VLAN ID for IGMP reports, that is Join and Leave packets. You must first create the VLAN using the <code>vlan</code> command under the <code>remote uniport</code> command. (Required.)</i>	C	13

Table 313 UNI Port IGMP Channel Commands (continued)

LABEL	DESCRIPTION	M	P
<code>igmpchannel <univid> [active <on off>] [version <IGMPv2 IGMPv3>] [cacprof <prof>] [maxgroup <0-512>] [maxmsg <0-64>] [signaling <on off>] [previewpkg <packages>] [fullviewpkg <packages>] [txtag <transparent untag replace <1~4094>>]</code>	<p>Configures a UNI port IGMP channel.</p> <p>active: Activates/deactivates this CLI configuration and, for the remote ONT UNI port, provisions OMCI to ONT. (Optional, default is on.)</p> <p>uni-vid: The default VLAN ID for IGMP reports, that is Join and Leave packets. You must first create the VLAN using the <code>vlan</code> command under the <code>remote uniport</code> command. (Required.)</p> <p>version: Configures the IGMP version to either IGMPv2 or IGMPv3. (Optional, default IGMPv2.)</p> <p>cacprof: Adapts a QoS CAC profile which contains multicast bandwidth settings and is created by the <code>qos cacprof</code> command. (Optional.)</p> <p>maxgroup: <0-512>. The maximum number of multicast groups a client can join concurrently. (Optional, default 64.)</p> <p>maxmsg: <0-255>. The maximum number of IGMP reports a client can send per second. (Optional, default 0.)</p> <p>signaling: <on off>. Enables the IGMP signaling mode. That is, it lets the OLT control and decide the multicast table of the ONT. The ONT must also support this feature. (Optional, default off.)</p> <p>previewpkg: Configures a list of package members with preview privilege. That is, IGMP clients can join groups in these package members only in a period of time. Use the <code>mcast-channel</code> command to create the package members. The ONT must also support this feature. (Optional.)</p> <p>fullviewpkg: Configures a list of package members with full view privilege. That is, IGMP clients can join to groups in these package members all the time. Use the <code>mcast-channel</code> command to create the package members. (Optional.)</p> <p>txtag: Sets whether the ONT sends multicast downstream traffic with a VLAN behavior. Use <code>transparent</code> if you want to follow the <code>uniport</code> VLAN txtag setting. Use <code>untag</code> for untagged VLAN. Use <code>replace</code> to replace the original VLAN with a specific VID.</p>	C	13
<code>no igmpchannel <cr></code>	Deletes the UNI port IGMP channel.	C	13

Table 313 UNI Port IGMP Channel Commands (continued)

LABEL	DESCRIPTION	M	P
show remote uniport <aid> igmpchannel <cr>	Displays the specified UNI port's IGMP channel settings. <i>aid: uniport-<pon>-<ont>-<card>-<port></i>	E	13
show remote uniport <aid> igmpchannel counter	Displays the specified UNI port's IGMP channel counter. <i>aid: uniport-<pon>-<ont>-<card>-<uniport></i>	E	13

Here are some example multicast channel packages:

Table 314 Example Multicast Channel Packages

ID	GROUP RANGE	DESCRIPTION
1	224.1.1.1 ~ 224.1.1.255	Basic channels
2	225.1.1.1 ~ 225.1.1.255	Financial channels
3	230.1.1.1 ~ 230.1.1.255	Sport channels
4	230.1.2.1 ~ 230.1.2.255	Movie channels

These example commands configure the multicast channels:

```
sysname (config)# mcast-channel 224.1.1.1 224.1.1.255 vlan 4001 pbit 4 package-member 1 preview-duration 60 preview-count 2 preview-blackout 10
sysname (config)# mcast-channel 225.1.1.1 225.1.1.255 vlan 4001 pbit 4 package-member 2 preview-duration 60 preview-count 2 preview-blackout 10
sysname (config)# mcast-channel 230.1.1.1 230.1.1.255 vlan 4001 pbit 4 package-member 3 preview-duration 60 preview-count 2 preview-blackout 10
sysname (config)# mcast-channel 230.1.2.1 230.1.2.255 vlan 4001 pbit 4 package-member 4 preview-duration 60 preview-count 2 preview-blackout 10
```

Now, suppose you want to allow subscribers to watch the channels as follows:

Table 315 Example Multicast Channel Package Subscribers

SUBSCRIBER	UNI PORT AID	PACKAGE PLAN
1	Uniport-1-1-1-1	Basic (fullview)
2	Uniport-1-2-1-1	Basic (fullview) + Financial (fullview)
3	Uniport-1-3-1-1	Basic (fullview) + Sport (preview)
4	Uniport-2-1-1-1	All (fullview)

These example commands configure IGMP channels for the ONT UNI ports:

```

sysname (config)# remote uniport uniport-1-1-1-1
sysname(config-remote-uniport)# igmpchannel 201 active on version IGMPv2 cacprof
mcast-100M maxgroup 64 maxmsg 10 signaling off fullviewpkg 1
sysname(config-remote-uniport)# exit
sysname (config)# remote uniport uniport-1-2-1-1
sysname(config-remote-uniport)# igmpchannel 202 active on version IGMPv2 cacprof
mcast-100M maxgroup 64 maxmsg 10 signaling off fullviewpkg 1,2
sysname(config-remote-uniport)# exit
sysname (config)# remote uniport uniport-1-3-1-1
sysname(config-remote-uniport)# igmpchannel 203 active on version IGMPv2 cacprof
mcast-100M maxgroup 64 maxmsg 10 signaling off fullviewpkg 1 previewpkg 3
sysname(config-remote-uniport)# exit
sysname (config)# remote uniport uniport-2-1-1-1
sysname(config-remote-uniport)# igmpchannel 211 active on version IGMPv2 cacprof
mcast-100M maxgroup 64 maxmsg 10 signaling off fullviewpkg 1-4
sysname(config-remote-uniport)# exit

```

87.3.7 UNI Port MAC Limit Settings

Use the `mac-limit` command to limit the number of MAC addresses a UNI port can learn.

Table 316 UNI Port MAC Limit Commands

LABEL	DESCRIPTION	M	P
<code>remote uniport <aid></code>	Configures UNI port settings. <i>aid: uniport-<pon>-<ont>-<card>-<port></i>	C	13
<code>mac-limit <number></code>	Limits the number of MAC addresses the UNI port can learn (1-128).	C	13
<code>no mac-limit <cr></code>	Disables the MAC limit function on the UNI port.	C	13
<code>show remote uniport <aid> mac-limit <cr></code>	Displays the specified UNI port's MAC limit configuration. <i>aid: uniport-<pon>-<ont>-<card>-<port></i>	E	13
<code>show remote uniport <aid> mac-address-table</code>	Displays the UNI port's MAC address table on the ONT. <i>aid: uniport-<pon>-<ont>-<card>-<port></i>	E	13

This example sets up a MAC limit number on uniport-1-1 of ONT-5-1-3.

```

sysname (config)# remote uniport uniport-1-3-1-1
sysname (config-remote-uniport)# mac-limit 128

```

This example disables the MAC limit on uniport-1-1 of ONT-1-3.

```

sysname (config)# remote uniport uniport-1-3-1-1
sysname (config-remote-uniport)#no mac-limit

```

This example shows the MAC limit setting on uniport-1-1 of ONT-1-3.

```
sysname # show remote uniport uniport-1-3-1-1 mac-limit
Mac Limit Active : YES
Mac Limit Number : 128
```

87.3.8 UNI Port CFM MEP Settings

Use the `cfm-mep` command to configure a maintenance association end point on a UNI port.

Table 317 UNI Port CFM MEP Commands

LABEL	DESCRIPTION	M	P
<code>remote uniport <aid></code>	Configures UNI port settings. <i>aid</i> : <code>uniport-<pon>-<ont>-<card>-<port></code>	C	13
	Configures IEEE 802.1ag CFM MEP for remote UNI port. <i>mep-index</i> : MEP's own identity in the MA. For a given MA, each MEP ID must be unique throughout the network defined by the MD. The MEP ID is defined in the range 1-8191. <i>ma-index</i> : Maintenance association index with which the MEP is associated. <i>priority</i> : CCM and CTM frames are transmitted according to this specified IEEE 802.1p priority. The priority is also used in LTR frames originating from this MEP.		
<code>no cfm-mep <cr></code>	Deletes the UNI port's CFM MEP configuration.	C	13
<code>show remote uniport <aid> cfm-mep <cr></code>	Displays the specified UNI port's CFM MEP configuration. <i>aid</i> : <code>uniport-<pon>-<ont>-<card>-<uniport></code>	E	13

CHAPTER 88

Port Protection Switching

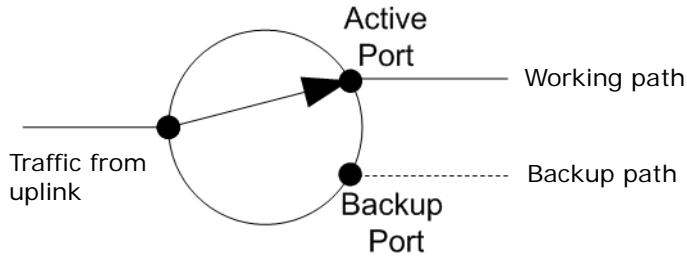
Port protection switching creates a protection path for traffic in case the working path fails.

88.1 Downlink Port Protection Switching

The port protection switching feature creates a working path (active port) and backup path (backup port) for uplink traffic.

Use protection groups to have active and backup uplink ports. You put 2 ports into a protection group. There are 3 groups for 6 ports. Each group has an active port and a backup port. Normally, the traffic uses the working path (traffic is sent out the active port). When the active port is down, the OLT sends out packets using the backup path (traffic is sent out the backup port).

Figure 246 Downlink Port Protection Switching



The following section lists the commands for this feature.

Table 318 Port Protection Switching Commands

COMMAND	DESCRIPTION	M	P
execution mode			
show protect-switch pon status	Displays the current status of the PON port protection switching operation.	E	3
switch-over pon <aid>	Triggers a PON port protection switch-over operation. aid: pon-<pon>	E	13
configure mode			
protect-switch pon pon-<port> pon-<port>	Assigns the specified PON ports as an active and backup pair. You can configure multiple pairs of PON ports, but each PON port can only be in one pair at a time.	C	13

Table 318 Port Protection Switching Commands (continued)

COMMAND	DESCRIPTION	M	P
no protect-switch pon all	Removes all of the protection groups.	C	13
no protect-switch pon pon-<port>	Enters the port number of an active port to remove the protection group that the active port belongs to.	C	13

CHAPTER 89

WRED

Weighted Random Early Detection (WRED) is a congestion avoidance technique that makes early detection of traffic congestion possible and provides queueing scheduling for multiple classes of traffic. It is an extension of the Random Early Detection (RED) algorithm where a single queue is assigned different drop thresholds.

This table lists the commands for this feature.

Table 319 WRED Commands

COMMAND	DESCRIPTION	M	P
execution mode			
show qos wred	Displays the QoS WRED status.	E	3
show qos ds-meter	Displays the downstream macro meter rate limit sharing mode.	E	3
configure mode			
qos wred	Enables QoS WRED.	C	13
no qos wred	Disables QoS WRED.	C	13
qos ds-meter macro-mode <pir cir>	Sets the downstream macro meter rate limit sharing mode. <i>pir</i> : the micro meter's Peak Information Rate (PIR) takes bandwidth first. <i>cir</i> : the micro meter's Committed Information Rate (CIR) takes bandwidth first.	C	13

CHAPTER 90

PPPoE IA

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

90.1 PPPoE Intermediate Agent Overview

- PPPoE allows ISPs to manage accounts access from dial-up Internet (such as ADSL).
- A PPPoE Intermediate Agent (PPPoE IA) is deployed between a PPPoE server and PPPoE clients.

Figure 247 PPPoE IA in Network



- PPPoE IA helps the PPPoE server identify and authenticate clients by adding subscriber line specific information to PPPoE discovery packets (PADI, PPPoE Active Discovery Initiation, and PADR, PPPoE Active Discovery Request) from clients on a per-port or per-port-per-VLAN basis before forwarding them to the PPPoE server.
- PPPoE Intermediate Agent is defined in "DSL Forum Technical Report 101-Migration to Ethernet-Based DSL Aggregation" (TR-101).
- If a PADI or PADR packet exceeds 1500 octets after adding the subscriber line specific information, the PPPoE IA does not send the packet to the PPPoE server but sends the packet with a Generic-Error TAG back to the sender (client).

90.1.1 Port State

Every port is either a trusted port or an untrusted port for the PPPoE intermediate agent. This setting is independent of the trusted/untrusted setting for DHCP snooping or ARP inspection. PPPoE IA inserts access loop identification in the packets sent from non-trusted ports to trusted ports. You can also specify the agent sub-options (Circuit ID and Remote ID) that the OLT adds to PADI and PADR packets from PPPoE clients.

Trusted ports are connected to PPPoE servers.

Note: The OLT will drop all PPPoE discovery packets if you enable the PPPoE intermediate agent and there are no trusted ports.

Untrusted ports are connected to subscribers.

90.2 PPPoE Intermediate Agent Commands

This table describes the commands.

Table 320 PPPoE Intermediate Agent Commands

COMMAND	DESCRIPTION	M	P
interface port-channel <aid>	Enters the sub-commands for configuring settings for the specified port. aid: <pon eth>-<port>	C	13
pppoe intermediate-agent trust	Sets the specified ports as PPPoE IA trusted ports.	C	13
no pppoe intermediate-agent trust	Sets the specified ports as PPPoE IA untrusted ports.	C	13
pppoe intermediate-agent <cr>	Activates PPPoE IA on the OLT.	C	13
pppoe intermediate-agent option circuit-id vlan <vid> option-info <info>	Enters a string of up to 127 ASCII characters that the OLT adds into the Agent Circuit ID sub-option for PPPoE discovery packets received in the VLAN group. <info>: The string should be composed of the following special characters. The special characters listed in the brackets [~!@#\$^*&()] are not allowed except % and space. <ul style="list-style-type: none"> • %%: character % • %space: character space • %mac: client source mac • %hname: host device name • %pid: pon port index • %oid: ONT index • %ocid: ONT card index • %upid: uniport index • %nnisvlan: SVLAN ID on network-network interface • %snisvlan: SVLAN ID on service-network interface • %snicvlan: CVLAN ID on service-network interface • %sn: serial number of remote ONT • %ontname: will be translated into ONT model name • %ontdesc: will be translated into ONT description • %ontpasswd: will be translated into ONT password Note: If the string is composed of more than 127 characters, the string will be truncated to the maximum number of characters allowed when the OLT transforms the string into the Circuit ID.	C	13
no pppoe intermediate-agent option circuit-id vlan <vid> <cr>	Clears the string that the OLT adds into the Agent Circuit ID sub-option for PPPoE discovery packets received in the VLAN group.	C	13

Table 320 PPPoE Intermediate Agent Commands (continued)

COMMAND	DESCRIPTION	M	P
<code>pppoe intermediate-agent option remote-id vlan <vid> option-info <info></code>	<p>Enters a string of up to 95 ASCII characters that the OLT adds into the Agent Remote ID sub-option for PPPoE discovery packets received in the VLAN group.</p> <p><info>: The string should be composed of the following special characters. The special characters listed in the brackets [~`!@#\$^&*()]) are not allowed except % and space.</p> <ul style="list-style-type: none"> • %: character % • %space: character space • %mac: client source mac • %hname: host device name • %pid: pon port index • %oid: ONT index • %ocid: ONT card index • %upid: uniport index • %nnisvlan: SVLAN ID on network-network interface • %snisvlan: SVLAN ID on service-network interface • %snicvlan: CVLAN ID on service-network interface • %sn: serial number of remote ONT • %ontname: will be translated into ONT model name • %ontdesc: will be translated into ONT description • %ontpasswd: will be translated into ONT password <p>Note: If the string is composed of more than 95 characters, the string will be truncated to the maximum number of characters allowed when the OLT transforms the string into the Remote ID.</p>	C	13
<code>no pppoe intermediate-agent option remote-id vlan <vid> <cr></code>	Clears the string that the OLT adds into the Agent Remote ID sub-option for PPPoE discovery packets received in the VLAN group.	C	13
<code>pppoe intermediate-agent option vlan <vid> <cr></code>	Enables the PPPoE intermediate agent option on the specified VLAN.	C	13
<code>no pppoe intermediate-agent option vlan <vid> <cr></code>	Disables the PPPoE intermediate-agent option on the specified VLAN.	C	13
<code>pppoe intermediate-agent vlan <vlan-list></code>	Activates PPPoE IA on the specified VLAN.	C	13
<code>pppoe intermediate-agent vlan <vlan-list> circuit-id</code>	Enables a PPPoE IA Circuit ID for the specified VLAN.	C	13
<code>pppoe intermediate-agent vlan <vlan-list> remote-id</code>	Enables a PPPoE IA Remote ID for the specified VLAN.	C	13
<code>no pppoe intermediate-agent <cr></code>	Turns off PPPoE IA on the OLT.	C	13
<code>no pppoe intermediate-agent vlan <vlan-list></code>	Removes the PPPoE IA on the specified VLAN.	C	13

Table 320 PPPoE Intermediate Agent Commands (continued)

COMMAND	DESCRIPTION	M	P
no pppoe intermediate-agent vlan <vlan-list> circuit-id	Removes the PPPoE IA Circuit ID for the specified VLAN.	C	13
no pppoe intermediate-agent vlan <vlan-list> remote-id	Removes the PPPoE IA Remote ID for the specified VLAN.	C	13
show pppoe intermediate-agent	Displays the PPPoE IA settings.	E	3
show pppoe intermediate-agent vlan <vlan/*>	Displays the option 82 Circuit ID and Remote ID information on the specified VLAN or all VLANs.	E	1
show pppoe intermediate-agent statistic	Displays the PPPoE IA statistics.	E	3
show pppoe intermediate-agent statistic vlan <vlan-list>	Displays the PPPoE IA statistics for the specified VLAN.	E	13
clear pppoe intermediate-agent statistics	Deletes the PPPoE IA statistics.	E	13
clear pppoe intermediate-agent statistics vlan <vlan-list>	Deletes the PPPoE IA statistics for the specified VLAN.	E	13

Table 320 PPPoE Intermediate Agent Commands (continued)

COMMAND	DESCRIPTION	M	P
<code>test pppoe-client start <aid></code> <code>username <username> password <password></code> <code>vlan <sniivid> [snicvid <1-4094>] [nnisvid <1-4094>] [</code> <code>univid <1-4094>] [ontid <1-128>] [</code> <code>ontcardid <1-16>] [uniport <1-128>] [ontsn <16 hex numbers>] [</code> <code>timeout <10-300>]</code>	<p>Starts a PPPoE client test to simulate the ONT creating a PPPoE session and getting an IP address from the PPPoE server. Up to 1 session can be simulated at a time.</p> <p><i>aid</i>: <ge pon>-<slot>-<port></p> <p><i>username</i>: the user name of the PPPoE account, length 1-32</p> <p><i>password</i>: the password of the PPPoE account, length 1-32</p> <p><i>sniivid</i>: Choose SNI SVID on subscriber port (ONT), 1-4094. This is the outer VLAN on the service node interface.</p> <p><i>snicvid</i>: SNI CVID setting on subscriber port (ONT), 1-4094. If not set and PPPoE IA needs this value, it will show 4096. This is the inner VLAN on the service node interface.</p> <p><i>nnisvid</i>: NNI SVID setting on subscriber port (ONT), 1-4094. If not set and PPPoE IA needs this value, it will show 4096. This is the outer VLAN on the network to network interface.</p> <p><i>univid</i>: UNI VID setting on subscriber port (ONT), 1-4094. If not set and PPPoE IA needs this value, it will show 4096. This is the (outer) VLAN on the user node interface.</p> <p><i>ontid</i>: ONT ID to be added to the PPPoE IA information, 1-128</p> <p><i>ontcardid</i>: ONTCARD ID to be added to the PPPoE IA information, 1-16</p> <p><i>uniport</i>: UNIPORT value to be added to the PPPoE IA information, 1-128</p> <p><i>ontsn</i>: ONT serial number to be added to the PPPoE IA information, 16 HEX characters long</p> <p><i>timeout</i>: timeout value for the simulation. 10-300 seconds, default value: 30 seconds</p>	E	13
<code>test pppoe-client start help</code>	Provides more information about the specified command.	E	13
<code>test pppoe-client status</code>	Displays the PPPoE client simulation results.	E	13
<code>test pppoe-client stop</code>	Stops the PPPoE client test.	E	13

90.3 PPPoE IA Configuration

90.3.1 Activating PPPoE IA

These commands activate PPPoE IA on the OLT.

```
sysname# config
sysname(config)# pppoe intermediate-agent
```

These commands activate PPPoE IA on a specific VLAN.

```
sysname#config
sysname(config)#pppoe intermediate-agent vlan <vlan-list>
```

Note: You must activate PPPoE IA for both the OLT system and the VLAN to use PPPoE IA.

These commands enable a PPPoE-IA Circuit ID or Remote ID in the specified VLAN.

```
sysname#config
sysname(config)#pppoe intermediate-agent vlan <vlan-list> circuit-id
sysname(config)#pppoe intermediate-agent vlan <vlan-list> remote-id
```

Note: You must activate PPPoE IA for the Circuit ID or Remote ID of the corresponding VLAN to insert the given access loop identification information

90.3.2 PPPoE IA Access Loop Identification Settings

The OLT handles PPPoE discovery-stage packets as follows:

- The OLT adds information to a PADI or PADR packet received from a non-trusted port and forwards it to a trusted port.
- The OLT drops a PADO or PADS packet received from a non-trusted port.
- The OLT forwards a PADI or PADR packet received from a trusted port to all trusted ports.
- In other cases besides those described above, the OLT forwards PPPoE discovery-stage packets.

Here are the PPPoE IA show commands.

```
sysname# show pppoe intermediate-agent
Switch PPPoE IA is disabled
PPPoE IA access-node-identifier string: OLT1404A
Operator configures the flexible syntax for PPPoE IA circuit-id: No
PPPoE IA is enabled in the following VLANs: None
PPPoE IA circuit-id is enabled in the following VLANs: 1-5
PPPoE IA remote-id is enabled in the following VLANs: None
PPPoE IA port setting is configured as following:
pon-1
    Trusted: No
pon-2
    Trusted: No
pon-3
    Trusted: No
pon-4
    Trusted: No
eth-1
    Trusted: No-----
-----
eth-20
    Trusted: No
sysname# show pppoe intermediate-agent statistic vlan 1
```

CHAPTER 91

Port Bridge

The port bridge feature enables the ONTs connected to the same PON port to communicate with each other. Use the port bridge feature to bridge multiple MAC addresses associated with the same port.

The port bridge feature only works on the PON ports of the OLT.

An ONT that doesn't support the port bridge feature may not function properly if the port bridge feature is enabled on the OLT.

91.1 Port Bridge Commands

This table describes the commands.

Table 321 Port Bridge Commands

COMMAND	DESCRIPTION	M	P
port-bridge	Enables the port bridge feature on the OLT.	C	13
port-bridge <aid>	Enables the port bridge feature on the specified port. aid: pon-<port>	C	13
no port-bridge	Disables the port bridge feature on the OLT.	C	13
no port-bridge <aid>	Disables the port bridge feature on the specified port. aid: pon-<port>	C	13
show port-bridge	Displays port bridge information for all ports.	E	3
show port-bridge <aid>	Displays port bridge information for the specified port. aid: pon-<port>	E	3

CHAPTER 92

IP and MAC Anti-Spoofing

92.1 IP and MAC Anti-Spoofing Overview

IP and MAC anti-spoofing protection lets you set inclusive or exclusive mode for specified source IP addresses or MAC addresses. This lets you allow or block packets from specific IP addresses or MAC addresses on specific ports. Here are some details about setting anti-spoofing entries:

- A port's anti-spoofing entries must all be exclusive or inclusive (not both).
- Set up to four entries per port.
- You can only apply anti-spoofing settings to subscriber ports.
- You can only add a specific MAC address or IP address in one entry on a port. (We do not want any two entries have confliction.)

The following tables describe the expected result for each type of anti-spoofing entry.

Table 322 Results for Inclusive Anti-Spoofing Entries

SETTING	RESULT
IP-Only (Inclusive)	The OLT allows non-IP packets and DHCP, but blocks other IP packets unless the source IP address is in the list.
MAC-Only (Inclusive)	The OLT blocks all packets unless the source MAC address is in the list.
IP-MAC (Inclusive)	The OLT allows non-IP packets and DHCP, but blocks other IP packets unless the source MAC address and source IP address are in the list.
OUI-MAC (Inclusive)	The OLT blocks all packets unless the source OUI-MAC is in the list.

However, if the IP-only entry and the MAC-only entry are both set at one port, the port allows all DHCP packets.

The OLT forwards packets from source IP addresses or MAC addresses listed in the inclusive entries and drops others.

Table 323 Results for Exclusive Anti-Spoofing Entries

SETTING	RESULT
IP-Only (Exclusive)	The OLT allows non-IP packets. The OLT also allows IP packets unless the source IP address is in the list.
MAC-Only (Exclusive)	The OLT allows all packets unless the source MAC address is in the list.
IP-MAC (Exclusive)	The OLT allows non-IP packets. The OLT also allows IP packets unless the source MAC address and source IP address are in the list.

The OLT drops packets from source IP addresses or MAC addresses listed in the exclusive entries and forwards others.

92.2 IP and MAC Anti-Spoofing Configuration

92.2.1 Activating IP and MAC Anti-Spoofing

These commands activate and de-activate anti-spoofing on the OLT.

```
sysname# config
sysname(config)# anti-spoofing
sysname(config)# no anti-spoofing
```

These commands activate and de-activate anti-spoofing on the specified port.

```
sysname#config
sysname(config)#interface port-channel <AID>
sysname(config-interface)# anti-spoofing
sysname(config-interface)# no anti-spoofing
```

Note: You must activate anti-spoofing on both the OLT and the port.

92.2.2 VLAN and MAC Spoofing Settings

These commands configure an anti-spoofing entry on a port-channel interface.

```
sysname#config
sysname(config)# interface port-channel <AID>
sysname(config-interface)# anti-spoofing <inclusive|exclusive> ip <ip> mac <mac-addr>
sysname(config-interface)# anti-spoofing <inclusive|exclusive> ip <ip>
sysname(config-interface)# anti-spoofing <inclusive|exclusive> mac <mac-addr>
sysname(config-interface)# anti-spoofing inclusive oui-mac <oui-mac-addr>
```

These commands delete the specified anti-spoofing entry on a port-channel interface.

```
sysname#config
sysname(config)# interface port-channel <AID>
sysname(config-interface)# no anti-spoofing ip <ip> mac <mac-addr>
sysname(config-interface)# no anti-spoofing ip <ip>
sysname(config-interface)# no anti-spoofing mac <mac-addr>
sysname(config-interface)# no anti-spoofing oui-mac <oui-mac-addr>
sysname(config-interface)# no anti-spoofing all-entry
```

These commands delete all the anti-spoofing entries for all ports.

```
sysname#config
sysname(config)# no anti-spoofing all-entry
```

These commands display the anti-spoofing entries for all ports or a specified port.

```
sysname# show anti-spoofing ?
      <cr>                      Show anti-spoofing settings of all ports
      pon-<port>                Show anti-spoofing settings of the given port
sysname# show anti-spoofing
Anti-Spoofing Active: NO
Port    Active   Mode       Setting
-----
sysname# show anti-spoofing pon-1
Anti-Spoofing Active: NO
Port    Active   Mode       Setting
-----
```

92.3 IP/MAC Anti-Spoofing Commands

This table describes the IP/MAC anti-spoofing commands.

Table 324 IP/MAC Anti-Spoofing Commands

COMMAND	DESCRIPTION	M	P
anti-spoofing	Enables IP/MAC anti-spoofing on the OLT.	C	13
no anti-spoofing	Disables IP/MAC anti-spoofing on the OLT.	C	13
no anti-spoofing all-entry	Removes all IP/MAC anti-spoofing entries for all ports.	C	13
show anti-spoofing	Displays the IP/MAC anti-spoofing settings for all ports.	E	3
show anti-spoofing pon-<port>	Displays the IP/MAC anti-spoofing settings for the specified port.	E	3
interface port-channel <aid>	Sets the IP/MAC anti-spoofing settings for the specified interface. aid: <pon>-<port>	C	13
anti-spoofing	Enables IP/MAC anti-spoofing on the specified interface.	C	13
anti-spoofing <inclusive exclusive> ip <ip>	Sets inclusive or exclusive mode for the specified source IP address.	C	13
anti-spoofing <inclusive exclusive> ip <ip> mac <mac-addr>	Sets inclusive or exclusive mode for the specified source IP address and MAC address.	C	13
anti-spoofing <inclusive exclusive> mac <mac-addr>	Sets inclusive or exclusive mode for the specified source MAC address.	C	13
anti-spoofing <inclusive exclusive> oui-mac <oui-mac-addr>	Sets inclusive or exclusive mode for the specified source OUI-MAC address.	C	13

Table 324 IP/MAC Anti-Spoofing Commands (continued)

COMMAND	DESCRIPTION	M	P
no anti-spoofing	Disables IP/MAC anti-spoofing on the specified interface.	C	13
no anti-spoofing <inclusive exclusive> ip <ip>	Removes the IP/MAC anti-spoofing entry of the specified source IP address.	C	13
no anti-spoofing <inclusive exclusive> ip <ip> mac <mac-addr>	Removes the IP/MAC anti-spoofing entry of the specified source IP address and MAC address.	C	13
no anti-spoofing <inclusive exclusive> mac <mac-addr>	Removes the IP/MAC anti-spoofing entry of the specified source MAC address.	C	13
no anti-spoofing <inclusive exclusive> oui-mac <oui-mac-addr>	Removes the IP/MAC anti-spoofing entry of the specified source OUI-MAC address.	C	13
no anti-spoofing all-entry	Removes all IP/MAC anti-spoofing entries.	C	13
exit	Leaves from the configuration commands.	C	13

92.4 Anti-MAC-Spoofing Commands

This table describes the anti-MAC-spoofing commands.

Table 325 Anti-MAC-Spoofing Commands

COMMAND	DESCRIPTION	M	P
anti-mac-spoof	Enables anti-MAC-spoofing on the OLT.	C	13
anti-mac-spoof <aid>	Sets the anti-MAC-spoofing settings for the specified interface. aid: pon-<port>	C	13
no anti-mac-spoof	Disables anti-MAC-spoofing on the OLT.	C	13
no anti-mac-spoof <aid>	Disables anti-MAC-spoofing for the specified interface. aid: <pon>-<port>	C	13
show anti-spoof	Displays the anti-MAC-spoofing settings for all ports.	E	3
show anti-mac-spoof <port-list>	Displays the anti-spoofing settings for the specified port.	E	3

CHAPTER 93

CPU Protection and DDoS

This chapter introduces the CPU protection and DDoS features of the OLT.

93.1 CPU Protection Overview

If the OLT receives large numbers of control packets, such as ARP, which are to be processed by the CPU, the CPU may become overloaded and be unable to handle regular tasks properly. The CPU protection feature allows you to limit the rate of ARP packets to be delivered to the CPU on a specific slot and port. This enhances the CPU efficiency and protects against potential DoS attacks or errors from other networks.

93.2 DDoS Overview

A distributed denial-of-service attack (DDoS attack) is an attempt to make a machine or network resource unavailable to its intended users. One common method of attack involves saturating the target machine with external communications requests, so much so that it cannot respond to legitimate traffic or responds so slowly as to be rendered essentially unavailable. Such attacks usually lead to a server overload. In general terms, DoS attacks are implemented by either forcing the targeted computer(s) to reset, or consuming its resources so that it can no longer provide its intended service or obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

93.3 DDoS Setup

The `show dos status` command displays the current DDoS configuration status:

Item	Name	Status
1	Source IP equal Destination IP	enable
2	MAC Source Addr equal MAC Destination Addr	enable
3	MAC Source Addr are zero	enable
4	TCP flags : SYN = 1 & ACK = 0 & SRC_Port < 1024	disable
5	TCP flags : All TCP flags = 0	disable
6	V4 first fragment check	disable
7	TCP flags : FIN = 1 & URG = 1 & PSH = 1	disable
8	TCP flags : SYN = 1 & FIN = 1	disable
9	TCP Source Port equal Destination Port	disable
10	UDP Source Port equal Destination Port	disable
11	TCP packets with not full TCP header	disable
12	TCP Header offset equals to 1 are dropped	disable
13	Enable ICMP size check	disable
14	Fragmented ICMP packets check	disable

You can use the `dos enable <item_number|all>` command to enable a specific item or all items, and the `no dos enable <item_number|all>` command to disable them.

93.4 CPU Protection and DDoS Commands

This table describes the CPU protection and DDoS commands.

Table 326 CPU protection and DDoS Commands

COMMAND	DESCRIPTION	M	P
<code>show cpu-protection interface port-channel <aid></code>	Displays the interface's CPU protection settings. <i>aid: <pon eth>-<port></i>	E	3
<code>clear cpu-protection interface port-channel <aid> cause <reason></code>	Clears the interface's CPU reason drop counter. <i>aid: <pon eth>-<port></i>	E	3
<code>CPU-limit ARP</code>	Enables the CPU to limit broadcast ARP packets.	C	13
<code>CPU-limit ARP inactive</code>	Disables the CPU to limit broadcast ARP packets.	C	13
<code>CPU-limit ARP rate <64 to 1,000,000 kbps></code>	Sets the limit of the ARP packet rate. <i>64 to 1,000,000 kbps, default: 64</i>	C	13
<code>interface port-channel <aid></code>	Enters the sub-commands for configuring the specified interface. <i>aid: <pon eth>-<port></i>	C	13

Table 326 CPU protection and DDoS Commands (continued)

COMMAND	DESCRIPTION	M	P
cpu-protection cause <reason> rate-limit <0-256>	Sets the maximum number of ARP, BPDU, IGMP, PPPoE, FTP, or ICMP packets that the specified ports are allowed to receive or transmit per second. <i>reason</i> : APR, BPDU, IGMP, PPPoE, FTP, or ICMP. Select the CPU protection reason. 0–256: Enter the reason rate-limit's setting. 0 means no rate limit.	C	13
cpu-protection cause help	Provides more information about the specified command.	C	13
dos enable <item_number / all>	Enables DDoS on a specific item or all items. Use show dos status to check the items.	C	13
no dos enable <item_number all>	Disables DDoS on a specific item or all items. Use show dos status to check the items.	C	13
show dos status	Displays the DoS status.	E	3
reset cpu-protection interface port-channel <aid> cause <reason>	Reset port reason settings on the specified port(s). <i>aid</i> : <pon eth>-<port>	E	13

CHAPTER 94

Error-Disable Recovery

94.1 Error-Disable Recovery Overview

Some features, such as loop guard or CPU protection, allow the OLT to shut down a port or discard specific packets on a port when an error is detected on the port. For example, if the OLT detects that packets sent out the port(s) loop back to the OLT, the OLT can shut down the port(s) automatically. After that, you need to enable the port(s) or allow the packets on a port manually via the web configurator or the commands. With error-disable recovery, you can set the disabled port(s) to become active or start receiving the packets again after the time interval you specify.

94.2 Error-Disable Recovery Commands

Use these commands to configure the error disable features on the OLT.

Table 327 Error Disable Recovery Commands

COMMAND	DESCRIPTION	M	P
errdisable detect cause <reason>	Sets the OLT to detect if the number of ARP, BPDU, IGMP, PPPoE, FTP, or ICMP packets exceeds the rate limit on port(s). <i>reason:</i> [ARP] [BPDU] [IGMP] [PPPoE] [FTP] [ICMP] [SNMP]	C	13
errdisable detect cause <reason> mode <mode>	Select the action that the OLT takes when the number of control packets exceed the rate limit on a port. <i><mode>:</i> <ul style="list-style-type: none">• inactive-port - The OLT disables the port on which the control packets are received.• inactive-reason - The OLT drops all the specified control packets (such as BPDU) on the port.• rate-limitation - The OLT drops the additional control packets the port(s) has to handle in every one second.	C	13
errdisable detect cause help	Sets the action that the OLT takes when the number of ARP, BPDU, IGMP, PPPoE, FTP, or ICMP packets exceeds the rate limit on port(s).	C	13
errdisable recovery cause <reason>	Enables the recovery timer for the specified feature that causes the OLT to shut down port(s).	C	13
errdisable recovery cause help	Sets how many seconds the OLT waits before enabling the port(s) which was shut down.	C	13
errdisable recovery cause <reason>	Enables the recovery timer on the OLT. <i>reason:</i> [ARP] [BPDU] [IGMP] [PPPoE] [FTP] [ICMP] [SNMP]	C	13

Table 327 Error Disable Recovery Commands (continued)

COMMAND	DESCRIPTION	M	P
no errdisable detect cause <reason>	Disables the recovery timer for the specified feature that causes the OLT to shut down a port. reason: [ARP] [BPDU] [IGMP] [PPPoE] [FTP] [ICMP] [SNMP]	C	13
errdisable recovery cause <reason> interval <30-2592000>	Sets how many seconds the OLT waits before enabling the port(s) which was shut down.	C	13
errdisable recovery	Turns on the disabled port recovery function on the OLT.	C	13
no errdisable recovery	Turns off the disabled port recovery function on the OLT.	C	13
no errdisable recovery cause <reason>	Disables the recovery timer for the specified feature that causes the OLT to shut down a port.	C	13
show errdisable	Displays which port(s) are detected (by Error Disable), the mode of the ports, and which packets are being detected.	E	3
show errdisable detect	Displays the Error Disable settings including the available protocol of packets, the current status (enabled or disabled), and the corresponding action the OLT takes when a detected port is handling packets over the limit.	E	3
show errdisable recovery	Displays the disabled port recovery settings and after how many seconds which port(s) will be activated.	E	3

CHAPTER 95

Battery

Use these commands to set up the OLT battery capacity and temperature threshold.

95.1 Battery Commands

The following section lists the commands for this feature.

Table 328 Battery Commands

COMMAND	DESCRIPTION	M	P
<code>battery alarm threshold <high-threshold> <low-threshold></code>	Enters the upper and lowest limits for the battery temperature. The OLT sends an alarm when the parameter values goes over or below the limits. The low-threshold value should be smaller than the high-threshold value. <high-threshold>/<low-threshold>: -15 ~ 50 Celsius	C	13
<code>no battery alarm threshold</code>	Sets the battery alarm temperature thresholds to the default values.	C	13
<code>battery info capacity <capacity></code>	Enters a value in the range of 7-18 Ah (ampere hour) for the battery capacity. This determines the amount of electric current that can be provided for a period of time.	E	13
<code>no battery info</code>	Sets the battery capacity to the default value.	C	13
<code>show battery</code>	Displays the battery capacity and alarm temperature thresholds of the connected battery.	E	13
<code>show battery status</code>	Displays the status of the connected battery.	E	13

CHAPTER 96

Additional Commands

Use these commands to configure or perform additional features on the OLT.

96.1 Command Summary

The following section lists the commands for this feature.

Table 329 Command Summary: Changing Modes or Privileges

COMMAND	DESCRIPTION	M	P
enable	Changes the session's privilege level to 14 and puts the session in enable mode (if necessary). The user has to provide the enable password. See Section 2.1.3.1 on page 14 .	E	0
enable <0-14>	Raises the session's privilege level to the specified level and puts the session in enable mode if the specified level is 13 or 14. The user has to provide the password for the specified privilege level. See Section 2.1.3.2 on page 14 .	E	0
disable	Changes the session's priority level to 0 and changes the mode to user mode. See Section 2.1.3.3 on page 15 .	E	13
configure	Changes the mode to config mode.	E	13
interface port-channel <aid> help	Enters config-interface mode for the specified port(s). aid: <pon eth>-<port>	C	13

Table 330 Command Summary: Additional Enable Mode

COMMAND	DESCRIPTION	M	P
baudrate <1 2 3 4 5>	Changes the console port speed. 1: 38400 bps 2: 19200 bps 3: 9600 bps 4: 57600 bps 5: 115200 bps	E	13
boot config	Restarts the system with the current active configuration file.	E	13
boot config <index>	Restarts the OLT (cold reboot) with the specified configuration file.	E	13
boot image <index>	The OLT supports dual firmware images, ras-0 and ras-1. Run this command, where <index> is 1 (ras-0) or 2 (ras-1) to specify which image is updated when firmware is loaded using the web configurator and to specify which image is loaded when the OLT starts up.	E	13

Table 330 Command Summary: Additional Enable Mode (continued)

COMMAND	DESCRIPTION	M	P
reload config	Reboots the OLT with stored configuration file.	E	13
reload config <index>	Restarts the system (warm reboot) with the specified configuration file. <index>: <1 2> 1: config-1 2: config-2	E	13
show version	Display the version of the currently running firmware on the OLT.	E	0
show version flash	Display the version of the currently running firmware on the OLT. Optionally, display the version of the currently installed firmware on the flash memory.	E	0
write memory	Saves current configuration in volatile memory to the configuration file the OLT is currently using or the specified configuration file.	E	13
write memory <index>	Saves current configuration in volatile memory to the specified configuration file.	E	13

Table 331 Command Summary: Additional Configure Mode

COMMAND	DESCRIPTION	M	P
default-management <in-band out-of-band>	Sets which traffic flow (in-band or out-of-band) the OLT sends packets originating from itself (such as SNMP traps) or packets with unknown source.	C	13
bcp-transparency <cr>	Enables Bridge Control Protocol (BCP) transparency on the OLT.		

CHAPTER 97

Product Specifications

97.1 System Specifications

The following tables list the OLT's system specifications. See [Section 97.2 on page 629](#) for power consumption specifications.

Table 332 System Specifications

dimensions	440 mm (width) x 250 mm (depth) x 44 mm (height); 1 U
Weight	4 Kg
Interfaces	<ul style="list-style-type: none">•• 1 fan module• 1 AC input• 1 battery input• 1 DC input• 1 MGMT port• 1CONSOLE port• 8 GE copper ports• 8 GE SFP ports• 4/8 GPON ports• 4 10G SFP+ ports• 1 ALARM port• 1 battery SENSOR port
Rack mounting	The OLT is 19-inch (482.6 mm) rack-mountable.
Operating environment	Temperature -40°C ~ 65°C (-40°F ~ 149°F); Humidity 5% - 95% RH (non-condensing)
Storage environment	Temperature: -40°C ~ 70°C (-40°F ~ 158°F) Humidity: 5% - 95% RH (non-condensing)
Reliability	MTBF (Mean Time Between Failure) > 44,000 hours
Fan module	Dimensions: 37 mm (W) x 253.6 mm (D) x 88.9 mm (H) Fans: 3 * 60 mm (W) x 60 mm (D) x 20 mm (H) Input Voltage: 12 V Maximum air flow per fan: 39.32 CFM, Speed Control: RPM adjusted based on temperature Hot swappable
Power	AC Input: 100 to -240 V AC, 50/60Hz, -1.6 Amps max. DC input: -36 VDC to -72 VDC, 2A max. (there is no tolerance for the DC input voltage.) Battery Input: +12VDC battery, 6A max.
Ground Wire Gauge	18 AWG or larger (green/yellow ground cable)

Table 332 System Specifications (continued)

Power Wire Gauge	18 AWG or larger
Certifications	<ul style="list-style-type: none"> • 2011/65/EU (RoHS 2) • 2012/19/EU (WEEE 2) • 2006/66/EC (Battery) • 94/62/EC (PPW, Packaging and Packaging Waste) • 1907/2006 (REACH, Registration, Evaluation, Authorization, and Restriction of Chemicals) <p>Safety</p> <ul style="list-style-type: none"> • EN62368-1 • IEC62368-1 <p>EMC</p> <ul style="list-style-type: none"> • FCC Part 15 Class A • ICES-003 Issue 6 Class A • EN 55032:2012/AC:2013 Class A • EN 55024:2010/A1:2015 • ETSI 300 386 V1.6.1 • AS/NZS CISPR 32:2013 • EN 61000-3-2:2014 • EN 61000-3-3:2013 • CNS 13438:2006 • <p>EE</p> <ul style="list-style-type: none"> • ETSI 300 019

97.2 Firmware Naming Conventions

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

Firmware Version: V4.00(AAVA.5)

"AAVA" is the model code.

"5" 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.

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/zxel_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

Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type/code numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

- **Name:** This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol:** This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **User-Defined**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s):** This value depends on the **Protocol**. Please refer to RFC 1700 for further information about port numbers.
 - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
 - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description:** This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 333 Commonly Used Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM/New-ICQ	TCP	5190	AOL's Internet Messenger service. It is also used as a listening port by ICQ.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for example www.zyxel.com) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.

Table 333 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic or routing purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
RExec	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	Simple File Transfer Protocol.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).

Table 333 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP	7000	Another videoconferencing solution.

APPENDIX C

Legal Information

Copyright

Copyright © 2018 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.

Federal Communications Commission (FCC) EMC Statement

- This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:
 - (1) This device may not cause harmful interference.
 - (2) This device must accept any interference received, including interference that may cause undesired operations.
- 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

- 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 store things on the device.
- Do not obstruct the device ventilation slots as insufficient airflow may harm your device. For example, do not place the device in an enclosed space such as a box or on a very soft surface such as a bed or sofa.
- 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.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- 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 an appropriate power adaptor or cord for your device. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- DO NOT remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- 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.
- CAUTION: RISK OF EXPLOSION IF BATTERY (on the motherboard) IS REPLACED BY AN INCORRECT TYPE. DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS. Dispose them at the applicable collection point for the recycling of electrical and electronic equipment. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.
- Use ONLY power wires of the appropriate wire gauge for your device. Connect it to a power supply of the correct voltage.
- Fuse Warning! Replace a fuse only with a fuse of the same type and rating.
- The POE (Power over Ethernet) devices that supply or receive power and their connected Ethernet cables must all be completely indoors.
- This equipment must be grounded by qualified service personnel. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact qualified service personnel if you are uncertain that suitable grounding is available.
- When connecting or disconnecting power to hot-pluggable power supplies, if offered with your system, observe the following guidelines:
 - Install the power supply before connecting the power cable to the power supply.
 - Unplug the power cable before removing the power supply.
 - If the system has multiple sources of power, disconnect power from the system by unplugging all power cables from the power supply.
- The following warning statements apply, where the disconnect device is not incorporated in the equipment or where the plug on the power supply cord is intended to serve as the disconnect device,
 - For PERMANENTLY CONNECTED EQUIPMENT, a readily accessible disconnect device shall be incorporated external to the equipment;
 - For PLUGGABLE EQUIPMENT, the socket-outlet shall be installed near the equipment and shall be easily accessible.
- CLASS 1 LASER PRODUCT
- APPAREIL A LASER DE CLASS 1
- PRODUCT COMPLIES WITH 21 CFR 1040.10 AND 1040.11.
- PRODUIT CONFORME SELON 21 CFR 1040.10 ET 1040.11.

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** Do not open the device. Opening or removing covers can expose you to dangerous high voltage points or other risks. Please contact your vendor for further information.
- 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**  Hazardous Moving Parts. Keep body parts away from fan blades.
- 6**  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** Ne pas ouvrir l'appareil, l'ouverture ou le retrait des couvercles peut vous exposer à des points comportant des tensions élevées ou à d'autres risques. Veuillez contacter votre vendeur pour plus d'informations.
- 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 connections téléphoniques.
- 5**  Mobilité des pièces détachées. S'assurer que les pièces détachées ne sont pas en contact avec les pales du ventilateur.
- 6**  Surface brûlante. Ne pas toucher.

Environment Statement

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 simbolo 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 innehåller 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

- 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。

About the Symbols

Various symbols are used in this product to ensure correct usage, to prevent danger to the user and others, and to prevent property damage. The meaning of these symbols are described below. It is important that you read these descriptions thoroughly and fully understand the contents.

Explanation of the Symbols

SYMBOL	EXPLANATION
	Alternating current (AC): AC is an electric current in which the flow of electric charge periodically reverses direction.
	Direct current (DC): DC is the unidirectional flow or movement of electric charge carriers.
	Earth; ground: A wiring terminal intended for connection of a Protective Earthing Conductor.
	Class II equipment: The method of protection against electric shock in the case of class II equipment is either double insulation or reinforced insulation.

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.

Index

Numbers

802.1P priority **94**

A

AAA **182, 417**
 accounting **183**
 authentication **182**
 authorization **182**
 external server **182**
 RADIUS **182**
 TACACS+ **182**
 AAA (Authentication, Authorization and Accounting) **182**
 access control
 limitations **308, 546**
 login account **313, 551**
 remote management **315**
 service port **314, 556**
 SNMP **316, 546**
 accessing the CLI **354**
 accounting
 setup **186**
 address learning, MAC **103, 105**
 Address Resolution Protocol (ARP) **344, 568**
 administrator password **313**
 aging time **89**
 alarm threshold **244, 247, 248**
 ARP
 how it works **568**
 ARP (Address Resolution Protocol) **344, 568**
 ARP inspection **193, 211**
 authentication
 setup **186**
 authentication, authorization and accounting **182**
 Authentication, Authorization and Accounting, see
 AAA **182**
 authorization
 privilege levels **187**

setup **186**
 auto-crossover **43**
 automatic VLAN registration **96**

B

back up, configuration file **304**
 Bandwidth Control **438**
 bandwidth control **131**
 egress rate **133**
 ingress rate **132**
 setup **131**
 basic settings **84, 370**
 basic setup tutorial **63**
 bias current **244, 247, 248**
 binding **192**
 binding table **192**
 building **193**
 BPDUs **117, 378**
 BPDUs (Bridge Protocol Data Units) **427**
 Bridge Protocol Data Units **378**
 Bridge Protocol Data Units (BPDUs) **117, 427**
 Broadcast Storm Control **441**
 broadcast storm control **134**

C

cable dust covers **44**
 CDR **493**
 certifications
 viewing **643**
 CFI **95**
 CFI (Canonical Format Indicator) **95, 400**
 changing the password **55**
 chassis
 installation **32**
 CIST **130, 430**

CIST (Common and Internal Spanning Tree) **428**
 classifier **148, 456**
 and QoS **148, 456**
 editing **152**
 example **153**
 overview **148, 456**
 setup **149, 152**
 viewing **152**
 command modes. See also modes **359**
 Common and Internal Spanning Tree (CIST) **428**
 Common and Internal Spanning Tree, See CIST **130, 430**
 config mode **360, 626**
 config-interface mode **360**
 config-mvr mode **360**
 configuration **285**
 change running config **303**
 saving **56**
 configuration file **57**
 backup **304**
 restore **57, 304**
 saving **302**
 config-vlan mode **360**
 console port (accessing the CLI) **354**
 contact information **630**
 copyright **639**
 CPU protection **228, 620**
 current date **87**
 current time **87**
 customer support **630**

D

daylight saving time **87**
 DDMI (Digital Diagnostics Monitoring Interface) **243**
 DDoS attack **620**
 denial-of-service attack **620**
 DHCP **533**
 configuration options **288, 533**
 Dynamic Host Configuration Protocol **288**
 modes **288, 533**
 relay agent **533**
 Relay Agent Information format **291**
 server **533**
 setup **542**

DHCP (Dynamic Host Configuration Protocol) **533**
 DHCP relay option 82 **210**
 DHCP snooping **63, 193, 209**
 configuring **211**
 DHCP relay option 82 **210**
 trusted ports **209**
 untrusted ports **209**
 DHCP snooping database **210**
 DHCPv4
 global relay **292**
 global relay example **293**
 Option 82 **291**
 Relay Agent Information **291**
 DHCPv4 relay **291**
 diagnostics **332, 559**
 dial plan **513**
 disclaimer **639**
 double-tagged frames **165, 475**
 dual firmware **356**
 dual firmware images **303**
 dynamic link aggregation **138, 446**

E

egress rate, and bandwidth control **133**
 enable mode **360, 626**
 error disable **228**
 CPU protection **229**
 detect **231**
 recovery **231**
 error-disable recovery **228, 623**
 Ethernet broadcast address **344, 568**
 Ethernet MAC **85**
 external authentication server **183**

F

fan module
 installation **40**
 removing **40**
 FCC interference statement **639**
 file transfer using FTP
 command example **306, 543**

filename convention, configuration
configuration
file names **305, 543**
filtering **114**
rules **114**
filtering database, MAC table **339, 565**
firmware **85**
select firmware index **356**
upgrade **303**
flow control
back pressure **94**
IEEE802.3x **94**
forwarding
delay **124**
frames
tagged **101**
untagged **101**
front panel **42**
FTP **305, 543**
file transfer procedure **306, 544**
restrictions over WAN **307, 544**

G

GARP **96**
GARP (Generic Attribute Registration Protocol) **96**
GARP timer **89, 96**
GEM port **596**
general setup **86**
getting help **58**
Gigabit ports **43**
GMT (Greenwich Mean Time) **87**
GUI-based FTP **544**
GVRP **96, 100, 101**
and port assignment **101**
GVRP (GARP VLAN Registration Protocol) **96**

H

hardware overview **42**
hello time **124**
help (in the CLI) **355**
high alarm threshold **244, 247, 248**

HTTPS **326**
certificates **326**
implementation **326**
public keys, private keys **326**
HTTPS example **327**

I

IGMP
version **485**
IGMP (Internet Group Management Protocol) **485**
IGMP Call Detail Record **493**
IGMP snooping **171, 485**
ingress rate, and bandwidth control **132**
initial setup **59**
installation
fan module **40**
rack **32**
transceivers **44**
IP
routing domain **375**
setup **375**
IP and MAC anti-spoofing **616**
IP setup **90**
IP source guard **192**
ARP inspection **193, 211**
DHCP snooping **193, 209**
static bindings **193**
IP table **342**
how it works **342**
IPv4 source guard **192**

L

LACP **138, 446**
system priority **144**
timeout **144**
latch **44**
LEDs **48**
Link Aggregate Control Protocol (LACP) **446**
link aggregation **138, 446**
dynamic **138, 446**
ID information **139, 447**

- setup **140**
 - traffic distribution algorithm **140**
 - traffic distribution type **142**
 - trunk group **138**
- Link Aggregation Control Protocol (LACP) **138**
 - lockout **56**
 - login **51, 355**
 - password **55**
 - login account
 - Administrator **313, 551**
 - non-administrator **313, 551**
 - login account privilege levels **357**
 - login accounts **313, 551, 552**
 - configuring via telnet **551**
 - configuring via web configurator **313**
 - multiple **313, 551**
 - number of **313, 551**
 - login password **313**
 - logout **356**
 - loop guard **214, 526**
 - examples **215**
 - how it works **527**
 - port shut down **215**
 - probe packet **527**
 - setup **215**
 - vs. STP **214**
 - loop guard, vs STP **526**
 - low alarm threshold **244, 247, 248**
- M**
 - MAC **85**
 - MAC (Media Access Control) **85**
 - MAC address **85, 344, 568**
 - maximum number per port **148**
 - MAC address learning **89, 103, 105, 148**
 - specify limit **148**
 - MAC Filtering **424**
 - MAC table **339, 565**
 - display criteria **341**
 - how it works **339, 565**
 - sorting criteria **341**
 - transfer type **341**
 - viewing **340**
 - maintanence
 - configuration backup **304**
 - firmware **303**
 - restoring configuration **304**
 - maintenance **301, 543**
 - current configuration **302**
 - fan **40**
 - main screen **302**
 - Management Information Base (MIB) **317, 547**
 - management IP address **90**
 - man-in-the-middle attacks **211**
 - Maximum Transmission Unit **440**
 - MDIX (Media Dependent Interface Crossover) **43**
 - Media Access Control **85**
 - MGMT LEDs **49**
 - MIB
 - and SNMP **317, 547**
 - supported MIBs **317, 547**
 - MIB (Management Information Base) **317, 547**
 - mirroring ports **136, 444**
 - modes **359**
 - modes, changing **626**
 - monitor port **136**
 - MST Instance, See MSTI **129, 429**
 - MST region **129, 429**
 - MSTI **124, 129, 429**
 - MST ID **429**
 - MSTI (Multiple Spanning Tree Instance) **124, 428**
 - MSTP **116, 118, 426, 428, 433**
 - bridge ID **127**
 - configuration digest **128**
 - forwarding delay **124**
 - Hello Time **127**
 - hello time **124**
 - Max Age **124, 127**
 - maximum hops **124**
 - MST region **429**
 - network example **428**
 - revision level **124**
 - status **127**
 - MSTP (Multiple Spanning Tree Protocol) **426**
 - MTU **440**
 - MTU (Multi-Tenant Unit) **88, 400**
 - multicast **485**
 - and IGMP **485**
 - IP addresses **171, 485**
 - overview **485**

multicast MAC address **111**
multimedia **233**
Multiple Spanning Tree Instance, See MSTI **428**
Multiple Spanning Tree Protocol, See MSTP **116, 118**
Multiple Spanning Tree Protocol, See MSTP. **426**
Multiple STP **118**
Multiple STP, see MSTP **428**
Multi-Tenant Unit **88**

N

network management system (NMS) **316, 546**
NTP (RFC-1305) **87**

O

OLT (Optical Line Terminal) **248**
ONT **580**
Option 82 **291**

P

password **55**
 administrator **313**
Password encryption **553**
Path MTU **391**
Path MTU Discovery **391**
PMTU **391**
policy **156**
 and classifier **156**
 and DiffServ **155, 466**
 configuration **156**
 example **160**
 overview **155, 466**
 rules **155, 156, 466**
Policy Rules **466**
PON port status **579**
port authentication **451**
port bridge **615**
Port by Port Queuing **472**
port details **80, 245**

port mirroring **136, 444**
Port protection switching **606**
port redundancy **138, 446**
port security **146, 453**
 limit MAC address learning **148**
 MAC address learning **146, 453**
 overview **146, 453**
 setup **146**
port setup **92**
port status
 port details **80, 245**
port VLAN ID, see PVID **101**
port VLAN trunking **97, 405**
ports
 "standby" **446**
 mirroring **136, 444**
 speed/duplex **94**
 standby **139**
power
 voltage **86**
power status **86**
PPPoE IA **218, 609**
 agent sub-options **219**
 configuration **220**
 drop PPPoE packets **222**
 port state **219**
 sub-option format **219**
 tag format **219**
 trusted ports **219, 609**
 untrusted ports **219, 609**
 VLAN **224**
PPPoE Intermediate Agent **218, 609**
priority level **90**
priority queue assignment **90**
privilege levels **357**
product registration **643**
protocol based VLAN **104, 408**
 and IEEE 802.1Q tagging **104, 408**
 hexadecimal notation for protocols **104, 106**
 isolate traffic **104, 408**
 priority **104, 106**
PVID **96, 401**
PVID (Priority Frame) **401**

Q

QoS
and classifier **148, 456**
queuing **162, 472**
queuing method **162, 164, 472**

R

rack
installation **32**
specifications **628**
RADIUS **183**
advantages **183**
and tunnel protocol attribute **190**
setup **183**
RADIUS and TACACS+ **417**
Rapid Spanning Tree Protocol, See RSTP. **116, 426**
reboot
load configuration **303**
reboot system **303**
receiving power **244, 248**
registration
product **643**
remote management **315**
service **316**
trusted computers **316**
Remote Network Monitor **462**
remote ONT **580**
removing
fan module **40**
removing a transceiver **45**
resetting **57**
restoring configuration **57, 304**
RFC 3164 **334, 563**
RMON **462**
routing domain **375**
routing table **346, 570**
RSTP **116, 426**
configuration **119**
status **121**

S

save configuration **56, 302**
saving configuration **356**
Secure Shell See SSH
service access control **314, 556**
 service port **315**
Session Initiation Protocol **233**
session privilege levels **358**
shortcuts **355**
show interfaces config protocol-based-vlan **409**
show subnet-vlan **407**
Simple Network Management Protocol, see SNMP
SIP account **233**
SIP identities **233**
SIP number **234**
SIP service domain **234**
SIP URI **233**
SNMP **316, 546**
 agent **317, 547**
 and MIB **317, 547**
 authentication **312**
 communities **309**
 management model **316, 546, 606**
 manager **317, 547**
 MIB **317, 547**
 network components **316, 546**
 object variables **317, 547**
 protocol operations **317, 547**
 security **312**
 setup **309**
 traps **310**
 users **311**
 version 3 and security **317, 547**
 versions supported **316, 546**
SNMP traps **318**
 supported **318, 324**
SP **472**
Spanning Tree Protocol, See STP. **116, 426**
SSH
 encryption methods **326, 555**
 how it works **325, 554**
 implementation **326, 555**
SSH (accessing the CLI) **355**
SSH (Secure Shell) **324, 554**
SSL (Secure Socket Layer) **326**

standby ports **139, 446**
static bindings **193**
static MAC address **109, 411**
static MAC forwarding **103, 105, 109**
static multicast address **111, 413**
static multicast forwarding **111, 413**
static route **531**
 enable **286**
 metric **286**
static routes **285**
static VLAN **106**
 control **108**
 tagging **108**
status **52, 79**
 MSTP **127**
 power **86**
 RSTP **121**
 VLAN **98**
STP **116, 426**
 bridge ID **122**
 bridge priority **120**
 designated bridge **117, 427**
 edge port **121**
 forwarding delay **121**
 Hello BPDU **117, 427**
 Hello Time **120, 122**
 how it works **117, 427**
 Max Age **120, 122**
 path cost **117, 121, 426**
 port priority **121**
 port state **118, 427**
 root port **117, 427**
 status **118**
 terminology **117, 426**
 vs loop guard **526**
 vs. loop guard **214**
Strictly Priority **472**
subnet based VLANs **102, 406**
 and DHCP VLAN **104**
 and priority **102, 406**
 configuration **103**
switch lockout **56**
switch reset **57**
switch setup **88, 375**
syntax conventions **352**
syslog **334**
 protocol **334, 563**

settings **334**
setup **334**
severity levels **334, 563**
system information **84**
system reboot **303**
System-Wide Queuing **474**

T

TACACS+ **182, 183, 421**
advantages **183**
setup **185**
tagged VLAN **95, 400**
telnet **551**
Telnet (accessing the CLI) **354**
temperature **244, 247, 248**
temperature indicator **85**
Terminal Access Controller Access-Control System Plus **182**
time
 current **87**
Time (RFC-868) **87**
time server **87**
time service protocol **87**
 format **87**
trademarks **643**
transceiver removal **45**
transceivers
 installation **44**
transmitting power **244, 248**
traps
 destination **310**
TRTCM
 color-aware mode **469**
 color-blind mode **469**
trunk group **138, 446**
trunking **138, 446**
trusted ports
 DHCP snooping **209**
 PPPoE IA **219, 609**
tunnel protocol attribute
 and RADIUS **190**
tutorials **63**
 DHCP snooping **63**
Two Rate Three Color Marker (TRTCM) **156**

Two Rate Three Color Marker, see TRTCM **156**

U

Uniform Resource Identifier **233**

untrusted ports

 DHCP snooping **209**

 PPPoE IA **219, 609**

user mode **359**

user profiles **183**

V

Vendor Specific Attribute, See VSA **189**

VID **92, 98, 99, 167, 400, 477**

 number of possible VIDs **95, 400**

 priority frame **95, 400**

VID (VLAN Identifier) **95, 400**

Virtual Local Area Network **88**

VLAN **88, 400**

 acceptable frame type **101**

 automatic registration **96**

 ID **95, 400**

 ingress filtering **100**

 introduction **88, 95, 400**

 number of VLANs **98**

 port number **99**

 port settings **99**

 PVID **101**

 static VLAN **106**

 status **98, 99**

 tagged **95, 400**

 terminology **96**

 trunking **97, 101, 405**

 type **89, 97**

VLAN (Virtual Local Area Network) **88, 400**

VLAN ID **95**

VLAN mapping

 tagged **476**

 traffic flow **476**

 untagged **476**

VLAN number **92**

VLAN stacking **165, 166, 475**

 configuration **167**

example **165**
frame format **167, 477**
port roles **166, 168, 475**
port-based Q-in-Q **169, 477**
priority **167, 477**
selective Q-in-Q **477**
VLAN tag **476**
VLAN terminology **96**
VLAN translation **476**
example **476**
VLAN trunking **101**
VLAN, protocol based, See protocol based VLAN
VLAN, subnet based, See subnet based VLANs **102, 406**
VoIP **505**
voltage **244, 247, 248**
VSA **189**

W

warranty **643**
note **643**
web configurator
getting help **58**
home **52**
login **51**
logout **57**
navigation panel **52**
Weighted Random Early Detection **608**
WRED **608**

Z

ZyNOS (ZyXEL Network Operating System) **305, 543**