FURUKAWA ELECTRIC

LD3008 / LD3016

GPON OLT system

User Manual

Content

1 Introduction 17

1.1 Audience 17

1.2 Document Structure 17

1.3 Document Convention 18

1.4 Document Notation 18

1.5 Virus Protection 19

2 System Overview 20

2.1 System Features 22

3 Command Line Interface (CLI) 25

3.1 Configuration Mode 25

3.1.1 Privileged EXEC View Mode 25

3.1.2 Privileged EXEC Enable Mode 26

3.1.3 Global Configuration Mode 26

3.1.4 Bridge Configuration Mode 27

3.1.5 DHCP Pool Configuration Mode 28

3.1.6 DHCP Option Configuration Mode 28

3.1.7 DHCP Option 82 Configuration Mode 28

3.1.8 Interface Configuration Mode 29

3.1.9 Rule Configuration Mode 29

3.1.10 RMON Configuration Mode 30

3.1.11 GPON Configuration Mode 30

3.2 Configuration Mode Overview 32

3.3 Useful Tips 33

3.3.1 Listing Available Command 33

3.3.2 Calling Command History 34

3.3.3 Using Abbreviation 36

3.3.4 Using Command of Privileged EXEC Enable Mode 37

3.3.5 Exit Current Command Mode 37

3.3.6 The Command Execution Limit 37

4 System Connection and IP Address 38

4.1 System Connection 38

4.1.1 System Login 38

4.1.2 Password for Privileged EXEC Enable Mode 38

4.1.3 Changing Login Password 39

4.1.4 Login Password Recovery Process 40

4.1.5 Management for System Account 41

4.1.6 Limiting the Number of Users 45

4.1.7 Limiting the Number of login attemps 45

4.1.8 Auto Log-out 45

4.1.9 Telnet Access 46

4.1.10 IP Login Delay 47

4.1.11 System Rebooting 48

4.1.12 Auto Reset Configuration 49

4.2 System Authentication 51

4.2.1 Authentication Method 51

4.2.2 Authentication Interface 51
4.2.3 Primary Authentication Method 52
4.2.4 RADIUS Server 52
4.2.5 TACACS+ Server 53
4.2.6 Accounting Mode 55
4.2.7 Displaying System Authentication 55
4.3 Configuring Interface 56
4.3.1 Enabling Interface 56
4.3.2 Assigning IP Address to Network Interface 56
4.3.3 Static Route and Default Gateway 57
4.3.4 Interface Description 58
4.3.5 Displaying Interface 59
4.3.6 Interface Identifier 59
4.3.7 Enabling Interface Overlapping 59
4.4 Assigning an IPv6 Address 61
4.4.1 Enabling Interface 63
4.4.2 Assigning IPv6 Address to Network Interface 64
4.4.3 Assigning Link Local Address to Network Interface 65
4.4.4 Static Route and Default Gateway 65
4.4.5 Enabling IPv6 Processing 66
4.4.6 IPv6 Interface Mode 67
4.4.7 Displaying Interface 67
4.5 Secure Shell (SSH) 69
4.5.1 SSH Server 69
4.5.2 SSH Client 70
4.6 802.1x Authentication 71
4.6.1 802.1x Authentication 73
4.6.2 802.1x Re-Authentication 76
4.6.3 Initializing Authentication Status 78
4.6.4 Restoring Default Value 78
4.6.5 Displaying 802.1x Configuration 78
4.6.6 802.1x User Authentication Statistics 78
4.6.7 Sample Configuration 79

5 Port Configuration 80

5.1 Ethernet Port Configuration 80
5.1.1 Enabling Ethernet Port 80
5.1.2 Auto-Negotiation 80
5.1.3 Transmit Rate 81
5.1.4 Duplex Mode 81
5.1.5 Flow Control 81
5.1.6 Port Description 82
5.1.7 Network Service Port 82
5.1.8 L2 Port Bridge 82
5.1.9 Port Crossover 83
5.1.10 Traffic Statistics 83
5.1.11 Port Information 85
5.1.12 Port Debounce Timer 86
5.2 Port Mirroring 87

6 System Environment 90
6.1 Environment Configuration 90
6.1.1 Host Name 90
6.1.2 Time and Date 90
6.1.3 Time Zone 91
6.1.4 Network Time Protocol (NTP) 92
6.1.5 Simple Network Time Protocol (SNTP) 93
6.1.6 Terminal Configuration 94
6.1.7 Login Banner 94
6.1.8 DNS Server 95
6.1.9 Fan Operation 96
6.1.10 Enabling FTP/TFTP Connection 96
6.1.11 Disabling Daemon Operation 97
6.1.12 FTP Bind Address 97
6.1.13 System Threshold 98
6.1.14 Enabling DMI Module 101
6.1.15 Software Watchdog Configuration 102
6.1.16 Auto USB-Restore 102
6.2 Configuration Management 104
6.2.1 Displaying System Configuration 104
6.2.2 Writing System Configuration 104
6.2.3 Auto-Saving 105
6.2.4 System Configuration File 105
6.2.5 Restoring Default Configuration 106
6.2.6 Core Dump File 107
6.3 System Management 108
6.3.1 Network Connection 108
6.3.2 IP ICMP Source Routing 110
6.3.3 Tracing Packet Route 111
6.3.4 Displaying User Connecting to System 112
6.3.5 MAC Table 113
6.3.6 System Running Time 113
6.3.7 System Information 113
6.3.8 System Memory Information 114
6.3.9 System EDFA 114
6.3.10 CPU Packet Management 115
6.3.11 Running Process 118
6.3.12 Displaying System Software 118
6.3.13 Displaying Installed OS 119
6.3.14 Default OS 119
6.3.15 Switch Status 119
6.3.16 Forwarding Information Base (FIB) Table 119
6.3.17 Tech Support Information 120
6.3.18 System Boot Information 120
6.3.19 Network Service Module (NSM) Daemon Debugging 121

7 Network Management 122
7.1 Simple Network Management Protocol (SNMP) 122
7.1.1 SNMP Service 122
7.1.2 SNMP Community 122

7.1.3 SNMP Agent Administrator 123
7.1.4 Assigning IP Address of SNMP Agent 124
7.1.5 SNMP Com2sec.....124
7.1.6 SNMP Group.....125
7.1.7 SNMP View Record 125
7.1.8 Permission to Access SNMP View Record 126
7.1.9 SNMP Version 3 User 126
7.1.10 SNMP Engine ID 127
7.1.11 SNMPv3 Notification 127
7.1.12 SNMP Trap.....130
7.1.13 SNMP Alarm.....134
7.1.14 SNMP Message Logging 137
7.1.15 Disabling SNMP 138
7.1.16 Displaying SNMP Configuration.....138
7.2 Link Layer Discovery Protocol (LLDP) 139
7.2.1 LLDP Operation 139
7.2.2 Enabling LLDP 139
7.2.3 LLDP Operation Type.....139
7.2.4 Basic TLV 139
7.2.5 LLDP Message.....140
7.2.6 Reinitiating Delay 140
7.2.7 Displaying LLDP Configuration 141
7.3 Remote Monitoring (RMON) 142
7.3.1 RMON History.....142
7.3.2 RMON Alarm 144
7.3.3 RMON Event 147
7.3.4 Simple RMON Event Configuration 149
7.4 Syslog.....151
7.4.1 Syslog Output Level.....151
7.4.2 Facility Code 153
7.4.3 Syslog Bind Address 154
7.4.4 Debug Message for Remote Terminal 154
7.4.5 Disabling Syslog 154
7.4.6 Syslog Local Message Configuration 154
7.4.7 Displaying Syslog Status.....155
7.5 Rule and QoS.....156
7.5.1 How to Operate QoS.....157
7.5.2 Packet Classification.....158
7.5.3 Packet Conditioning 163
7.5.4 Rule Action 165
7.5.5 Displaying Rule 175
7.5.6 Admin Rule.....175
7.5.7 Admin Rule Action.....179
7.5.8 Displaying Admin Rule 181
7.5.9 Scheduling 183
7.6 EFM OAM.....190
7.6.1 Enabling EFM OAM 190
7.6.2 OAM Link Monitoring 190
7.6.3 EFM OAM Mode 191
7.6.4 OAM Loopback 192

7.6.5 OAM Unidirection 192
7.6.6 Displaying EFM OAM Configuration 193
7.7 NetBIOS Filtering 194
7.8 Martian Filtering 195
7.9 Max Host 196
7.10 Port Security 197
7.10.1 Port Security on Port 197
7.10.2 Port Security Aging 198
7.10.3 Displaying Port Security 199
7.11 Outband Management Port Security 199
7.12 Max Host 199
7.13 MAC Table 200
7.14 MAC Filtering 202
7.14.1 Default MAC Filter Policy 202
7.14.2 Configuring MAC Filter Policy 202
7.14.3 Listing MAC Filter Policy 203
7.14.4 Displaying MAC Filter Policy 203
7.15 Address Resolution Protocol (ARP) 204
7.15.1 ARP Table 204
7.15.2 ARP Request Message Interval 205
7.15.3 ARP Alias 205
7.15.4 ARP Inspection 206
7.15.5 Gratuitous ARP 212
7.15.6 Proxy ARP 212
7.16 IPv6 Neighbor Discovery(ND) 214
7.16.1 Stateful Auto Configuration 214
7.16.2 Configuring IPv6 Prefix 215
7.16.3 Interval of RA Messages 215
7.16.4 RA Destination Configuration 216
7.16.5 Router's Lifetime 216
7.16.6 Reachable Time 216
7.16.7 RA Suppression 217
7.16.8 Hop Limit 217
7.16.9 Retrans-time 217
7.16.10 ND Duplicate Address Detection (DAD) 218
7.16.11 Static IPv6 Neighbor Entry 218
7.16.12 Setting the Stale Timer 219
7.16.13 IPv6 Neighbor Discovery (ND) Inspection 219
7.16.14 Gratuitous ND 224
7.16.15 ND Alias 225
7.16.16 Displaying Neighbor Discovery 225
7.17 ICMP Message Control 227
7.17.1 Blocking Echo Reply Message 227
7.17.2 Interval for Transmit ICMP Message 228
7.17.3 ICMP Destination Unreachable Message 230
7.17.4 ICMP Redirect Message 230
7.18 TCP Flag Control 231
7.18.1 RST Configuration 231

7.18.2 SYN Configuration 231
7.19 The Utilization on L3 table 231
7.20 Packet Dump 232
7.20.1 Packet Dump by Protocol 232
7.20.2 Packet Dump with Option 232
7.20.3 Debug Packet Dump 234
7.20.4 Displaying Dump Packets 234
7.20.5 Dump File 234
7.21 Access List 236
7.21.1 Standard Access List 237
7.21.2 Extended Access List 238
7.21.3 Named Access List 240
7.21.4 Access List Range 241
7.21.5 Named Access List for IPv6 address 242
7.21.6 Displaying Access List Entries 243

8 System Main Functions 244

8.1 Virtual Local Area Network (VLAN) 244
8.1.1 Port-based VLAN 245
8.1.2 Protocol-based VLAN 247
8.1.3 MAC-based VLAN 248
8.1.4 Subnet-based VLAN 248
8.1.5 Tagged VLAN 249
8.1.6 VLAN Cross-connect 250
8.1.7 VLAN Description 251
8.1.8 VLAN Precedence 251
8.1.9 Displaying VLAN Information 251
8.1.10 QinQ VLAN Mapping 251
8.1.11 Layer 2 Isolation 258
8.1.12 Sample Configuration 261
8.2 Link Aggregation (LAG) 264
8.2.1 Port Trunk 264
8.2.2 Link Aggregation Control Protocol (LACP) 266
8.3 Spanning Tree Protocol (STP) 271
8.3.1 STP Operation 272
8.3.2 RSTP Operation 276
8.3.3 MSTP Operation 280
8.3.4 STP Mode 283
8.3.5 STP Basic Configuration 283
8.3.6 Configuring MSTP 287
8.3.7 Configuring PVSTP 292
8.3.8 Root Guard 295
8.3.9 Loop Guard 296
8.3.10 Topology Change Detection 296
8.3.11 Restarting Protocol Migration 297
8.3.12 Loop Back Detection 297
8.3.13 BPDU Configuration 298
8.3.14 Sample Configuration 302
8.4 Loop Detection 304

8.5 Dynamic Host Configuration Protocol (DHCP) 307
8.5.1 DHCP Server 308
8.5.2 DHCP Address Allocation with Option 82 316
8.5.3 DHCP Lease Database 318
8.5.4 DHCP Relay Agent 319
8.5.5 DHCP Option 323
8.5.6 DHCP Option 82 327
8.5.7 DHCP Snooping 330
8.5.8 IP Source Guard 337
8.5.9 DHCP Client 339
8.5.10 DHCP Filtering 341
8.5.11 Debugging DHCP 343
8.6 Dynamic Host Configuration Protocol (DHCP) for IPv6 344
8.6.1 DHCPv6 Server 349
8.6.2 DHCPv6 Snooping 353
8.6.3 DHCPv6 Relay Agent 357
8.6.4 DHCPv6 Option 357
8.6.5 Debugging DHCPv6 359
8.7 Virtual Router Redundancy Protocol (VRRP) 360
8.7.1 Configuring VRRP 361
8.7.2 VRRP Monitoring and Management 367
8.8 Rate Limit 369
8.9 Flood Guard 370
8.9.1 MAC Flood Guard 370
8.9.2 CPU Flood Guard 371
8.9.3 System Flood Guard 372
8.9.4 Invalid Traffic Guard 373
8.10 PPS Control 376
8.11 Storm Control 377
8.12 Jumbo Frame Capacity 377
8.13 Configuring PPPoE Tag Option Format 379
8.13.1 PPPoE Vendor Tag Option 379
8.13.2 PPPoE Vendor Tag Filtering 380
8.13.3 PPPoE Debug 381
8.14 Bandwidth 382
8.15 Maximum Transmission Unit (MTU) 382
8.16 Blocking Packet Forwarding 382

9 IP Multicast 384
9.1 Multicast Group Membership 386
9.1.1 IGMP Basic 386
9.1.2 IGMP Version 2 388
9.1.3 IGMP Version 3 394
9.1.4 Displaying IGMP Information 395
9.2 Multicast Functions 396
9.2.1 Multicast Forwarding Database 396
9.2.2 IGMP Snooping Basic 397
9.2.3 IGMPv2 Snooping 400

9.2.4 IGMPv3 Snooping 409
9.2.5 Displaying IGMP Snooping Information 410
9.2.6 Multicast VLAN Registration (MVR) 412
9.2.7 IGMP Filtering and Throttling 414
9.2.8 IGMP Proxy 417
9.2.9 IGMP State Limit 421
9.2.10 Multicast-Source Trust Port 422

10 IPv6 Multicast 423

10.1 Multicast Listener Discovery (MLD) 424
10.1.1 MLD Version 427
10.1.2 MLD Querier's Robustness Variable 427
10.1.3 Clearing MLD Entry 427
10.1.4 MLD Debug 427
10.1.5 MLD Access Control 428
10.1.6 MLD Querier Configuration 428
10.1.7 Displaying MLD Information 431
10.2 IPv6 Multicast Functions 432
10.2.1 Multicast Forwarding Database 432
10.2.2 MLD Snooping Basic 434
10.2.3 MLD Snooping 435
10.2.4 MLD State Limit 439
10.2.5 MLD Snooping Debug 439
10.2.6 MLD-Proxy IF Flap Discredit 440

11 GPON Configuration 442

11.1 OLT Management 444
11.1.1 Opening OLT Mode 444
11.1.2 Downstream Encryption 445
11.1.3 OLT Bandwidth 446
11.1.4 Auto ONU Fault Detection 447
11.1.5 Maximal Distance between OLT and ONU (ONT) 448
11.1.6 Forward Error Correction (FEC) Mode 448
11.1.7 MAC Aging Time 449
11.1.8 OLT Link Down Detection 449
11.1.9 Maximum Number of ONU 450
11.1.10 OLT Anti-Spoofing 450
11.1.11 Downstream Traffic Control 451
11.1.12 Multicast/Broadcast GEM Port Separation 453
11.1.13 Configuring Port/TCONT Threshold 454
11.1.14 ONU Deactivation Monitoring 455
11.1.15 OLT Bit Error Ratio (BER) 456
11.1.16 OMCC Monitoring 457
11.1.17 PLOAM Message 458
11.1.18 OLT Flow Control 458
11.1.19 Transceiver Type Configuration 459
11.1.20 Statistics GEM Configuration 459
11.1.21 Displaying OLT Information 459
11.2 ONU Management 464
11.2.1 ONU Registration 464

11.2.2 Assigning IP address 471
11.2.3 Activating Administration for UNI 472
11.2.4 Forward Error Correction (FEC) Mode 472
11.2.5 Loopback 473
11.2.6 ONU Laser Down 473
11.2.7 Source MAC address Monitoring 474
11.2.8 ONU MAC address Filtering 475
11.2.9 POTS Interface Configuration 476
11.2.10 VoIP MGC Configuration 477
11.2.11 ONU Port Configuration 478
11.2.12 ONU Loop Detect Configuration 479
11.2.13 ONU Inactive Aging-time 480
11.2.14 ONU Reset 480
11.2.15 ONU Password Type Configuration 481
11.2.16 Diagnostic Monitoring for ONU's Optical Transceiver 481
11.2.17 ONU System Account 481
11.2.18 ONU CoS Remarking 482
11.2.19 ONU Extended VLAN Tagging Operation 482
11.2.20 ONU RateLimit Configuration 483
11.2.21 ONU Authentication from RADIUS Server 486
11.2.22 CFM OAM for ONU Management 489
11.2.23 ONU DBA Profile 492
11.2.24 ONU Firmware Upgrade 493
11.2.25 Displaying ONU Information 502
11.2.26 ONU's Basic Configurations via OLT 506
11.2.27 Generic Status Portal (GSP) 512
11.3 ONU Profile 516
11.3.1 Creating ONU Profile 516
11.3.2 Configuring ONU Profile 517
11.3.3 Overwriting Traffic Profile Configuration 526
11.3.4 Saving Profile 528
11.3.5 Applying ONU Profile 528
11.3.6 Checking ONU Profile Configuration 528
11.3.7 Assigning IP Host of SNMP Agent 529
11.3.8 SNMP Trap Host 529
11.3.9 Displaying ONU profile 529
11.4 Traffic Profile 531
11.4.1 Creating Traffic Profile 531
11.4.2 Creating a Mapper 532
11.4.3 MAC Bridge Service Profile 533
11.4.4 T-CONT Mode 541
11.4.5 IP Host Service Configuration 543
11.4.6 VoIP Service Configuration (POTS UNI) 546
11.4.7 TDM Service Configuration (CES UNI) 550
11.4.8 Management Mode 554
11.4.9 Configuring Rate-limit 554
11.4.10 Video Return Path Mode 555
11.4.11 Creating a GEM Port Network CTP 556
11.4.12 Saving Traffic Profile 556
11.4.13 Adding/Applying Traffic Profile 557

11.4.14 Displaying Traffic Profile Information 557
11.4.15 Sample Configuration 558
11.5 DBA Profile 559
11.5.1 Creating DBA Profile 559
11.5.2 Configuring DBA Profile 559
11.5.3 Saving DBA Profile 560
11.5.4 Displaying DBA Profile 560
11.6 Extended VLAN Tagging Operation Profile 561
11.6.1 Received Frame VLAN Tagging Operation Table Configuration 561
11.6.2 TPID Configuration 567
11.6.3 Downstream Mode Configuration 567
11.6.4 Saving Profile 567
11.6.5 Displaying Extended VLAN Tagging Operation Profile 568
11.7 VoIP Profile 569
11.7.1 OMCI Management Configuration 569
11.7.2 OMCI-based SIP Configuration 574
11.7.3 OMCI-based MGC Configuration 582
11.7.4 Saving VoIP Profile 583
11.7.5 Displaying VoIP Information 584
11.7.6 Sample Configuration 584
11.8 TDM Pseudowire Profile 585
11.8.1 Creating TDM Pseudowire Profile 585
11.8.2 Basic Service Type 586
11.8.3 Signalling 586
11.8.4 Payload Size 586
11.8.5 Payload Encapsulation Delay 587
11.8.6 Timing Mode 587
11.8.7 RTP Pseudowire Parameter 587
11.8.8 Pseudowire Maintenance Configuration 589
11.8.9 Saving TDM Pseudowire Profile 589
11.8.10 Displaying TDM Pseudowire Information 590
11.9 Pseudowire Maintenance Profile 591
11.9.1 Creating Pseudowire Maintenance Profile 591
11.9.2 Jitter Buffer Maximum Depth 591
11.9.3 Jitter Buffer Desired Depth 592
11.9.4 Fill Policy 592
11.9.5 Alarm-related Policy 592
11.9.6 L-bit/R-bit Receive/Transmit Policy 593
11.9.7 SES Threshold 594
11.9.8 Saving Pseudowire Maintenance Profile 594
11.9.9 Displaying Pseudowire Maintenance Information 595
11.10 Performance Monitoring (PM) Profile 596
11.10.1 Creating PM Profile 596
11.10.2 Collecting ONU Traffic Statistics 596
11.10.3 Saving PM Profile 598
11.10.4 Displaying PM Profile Information 598
11.10.5 Displaying ONU Traffic Statistics 599
11.10.6 Sample Configuration 600
11.11 Multicast Profile 601

11.11.1 Creating Multicast Profile 601
11.11.2 IGMP Configurations 601
11.11.3 Saving Multicast Profile 603
11.11.4 Applying Multicast Profile 603
11.11.5 Displaying Multicast Information 604
11.11.6 Multicast Access List 604
11.12 Rate-limit Profile 607
11.12.1 Creating Rate-limit Profile 607
11.12.2 Configuring Rate-limit Profile 607
11.12.3 Saving Rate-limit Profile 608
11.12.4 Applying Rate-limit Profile 608
11.12.5 Displaying Rate-limit Profile 609
11.13 ONU Service Profile 610
11.14 GPON Debug 611
11.15 Sample Configuration 612

12 System Software Upgrade 616
12.1 General Upgrade 616
12.2 Boot Mode Upgrade 617
12.3 FTP Upgrade 620
12.4 ONU Upgrade 622
12.4.1 Manual Upgrade 622
12.4.2 Auto Upgrade 623
12.4.3 Upgrade Time-out Configuration 624
12.4.4 Upgrade Maximum Count Configuration 625

13 Abbreviations 626

Illustrations

Fig. 2.1 Front View of the LD3008 21
Fig. 2.2 Front View of the LD3016 21
Fig. 3.1 Overview of Configuration Mode 32
Fig. 4.1 Structure of IPv6 Header 61
Fig. 4.2 Process of 802.1x Authentication 72
Fig. 4.3 Multiple Authentication Servers 73
Fig. 5.1 Port Mirroring 87
Fig. 6.1 Ping Test for Network Status 110
Fig. 6.2 IP Source Routing 111
Fig. 7.1 Procedure of QoS operation 157
Fig. 7.2 Structure of Rule 158
Fig. 7.3 Token Bucket Meter 167
Fig. 7.4 Behavior of srTCM (1) 168
Fig. 7.5 Behavior of srTCM (2) 169
Fig. 7.6 Bahavior of srTCM (3) 169
Fig. 7.7 Behavior of trTCM (1) 170
Fig. 7.8 Behavior of trTCM (2) 171
Fig. 7.9 Behavior of trTCM (3) 171
Fig. 7.10 Strict Priority Queuing 183
Fig. 7.11 Deficit Round Robin 184
Fig. 7.12 Weighted Round Robin 184
Fig. 7.13 WRED Packet Drop Probability 188
Fig. 7.14 NetBIOS Filtering 194
Fig. 7.15 Proxy ARP 213
Fig. 7.16 ICMP Message Structure 227
Fig. 8.1 Port-based VLAN 245
Fig. 8.2 Subnet-based VLAN 248
Fig. 8.3 Example of QinQ Configuration 252
Fig. 8.4 QinQ Frame 252
Fig. 8.5 Outgoing Packets under Layer 2 Shared VLAN Environment 259
Fig. 8.6 Incoming Packets under Layer 2 Shared VLAN Environment (1) 260
Fig. 8.7 Incoming Packets under Layer 2 Shared VLAN Environment (2) 260
Fig. 8.8 Link Aggregation 264
Fig. 8.9 Example of Loop 271
Fig. 8.10 Principle of Spanning Tree Protocol 271
Fig. 8.11 Root Switch 272
Fig. 8.12 Designated Switch 273
Fig. 8.13 Port Priority 274
Fig. 8.14 Port States 274
Fig. 8.15 Alternate Port and Backup port 276
Fig. 8.16 Example of Receiving Low BPDU 277
Fig. 8.17 Convergence of 802.1d Network 278
Fig. 8.18 Network Convergence of 802.1w (1) 278
Fig. 8.19 Network Convergence of 802.1w (2) 279
Fig. 8.20 Network Convergece of 802.1w (3) 279
Fig. 8.21 Compatibility with 802.1d (1) 280
Fig. 8.22 Compatibility with 802.1d (2) 280
Fig. 8.23 CST and IST of MSTP (1) 281
Fig. 8.24 CST and IST of MSTP (2) 282

Fig. 8.25 Example of PVSTP 292
Fig. 8.26 Root Guard 295
Fig. 8.27 Example of Layer 2 Network Design in RSTP Environment 303
Fig. 8.28 Example of Layer 2 Network Design in MSTP Environment 304
Fig. 8.29 DHCP Service Structure 307
Fig. 8.30 Example of DHCP Relay Agent 320
Fig. 8.31 DHCP Option 82 Operation 328
Fig. 8.32 DHCP Server Packet Filtering 342
Fig. 8.33 Basic DHCPv6 Message Format 346
Fig. 8.34 General Shared Relay Message Format 347
Fig. 8.35 An Example of Prefix Delegation 347
Fig. 8.36 VRRP Operation 360
Fig. 8.37 VRRP Track 365
Fig. 8.38 Rate Limit and Flood Guard 370
Fig. 9.1 The OLT with IGMP Snooping 384
Fig. 9.2 IGMP Snooping 398
Fig. 10.1 MLDv1 Message Format 425
Fig. 10.2 MLDv2 Query Message Format 426
Fig. 11.1 Example of GPON Network 442
Fig. 11.2 CLI Structure of *GPON Configuration* Mode 443
Fig. 11.3 PON Structure Sample Scheme for VoIP and Internet Connection of ONT 507
Fig. 11.4 ONU Profile 516
Fig. 11.5 Traffic Profile 531
Fig. 11.6 Priority of T-CONT types 541
Fig. 11.7 VoIP Service Architecture 547
Fig. 11.8 Received Frame Layout 562

Tables

Tab. 1.1 Overview of Chapters 17
Tab. 1.2 Command Notation of Guide Book 18
Tab. 3.1 Main Command of *Privileged EXEC View* Mode 25
Tab. 3.2 Main Command of *Privileged EXEC Enable* Mode 26
Tab. 3.3 Main Command of *Global Configuration* Mode 27
Tab. 3.4 Main Command of *Bridge Configuration* Mode 27
Tab. 3.5 Main Command of *DHCP Pool Configuration* Mode 28
Tab. 3.6 Main Command of *DHCP Option Configuration* Mode 28
Tab. 3.7 Main Command of *DHCP Option 82 Configuration* Mode 29
Tab. 3.8 Main Command of *Interface Configuration* Mode 29
Tab. 3.9 Main Command of *Rule Configuration* Mode 30
Tab. 3.10 Main Command of *RMON Configuration* Mode 30
Tab. 3.11 Main Command of *GPON-OLT Configuration* Mode 31
Tab. 3.12 Main Command of *ONU Profile Configuration* Mode 31
Tab. 3.13 Command Abbreviation 36
Tab. 4.1 Overview of IPv6 Header Fields 62
Tab. 6.1 World Time Zone 92
Tab. 6.2 Options for Ping for Multiple IP Addresses 109
Tab. 6.3 Options for Tracing Packet Route 112
Tab. 7.1 ICMP Message Type 227
Tab. 7.2 Mask Calculation of Default Value 229
Tab. 7.3 Examples of Wildcard Masking 237
Tab. 8.1 Advantages and Disadvantages of Tagged VLAN 250
Tab. 8.2 STP Path-cost (short) 284
Tab. 8.3 RSTP Path-cost (long) 284
Tab. 8.4 DHCPv6 Message Types 345
Tab. 8.5 DHCPv6 UDP port 348
Tab. 8.6 DHCPv6 Address 348
Tab. 11.1 RADIUS Authentication Message Type 487
Tab. 11.2 Protocol Types for MAC Filtering 536

1 Introduction

1.1 Audience

This manual is intended for LD3008 and LD3016 multi-platform GPON OLT system operators and maintenance personnel for providers of Gigabit passive optical network (GPON) and Ethernet services. This manual assumes that you are familiar with the following:

- Ethernet networking technology and standards
- Internet topologies and protocols
- GPON technology and standards
- Usage and functions of graphical user interfaces.

All the command lines examples on this manual have output based on the LD3016 speficications.

1.2 Document Structure

Tab. 1.1 briefly describes the structure of this document.

Chapter	Description
1 Introduction	Introduces the overall information of the document.
2 System Overview	Introduces the LD3008 and LD3016 system. It also lists the features of the system.
3 Command Line Interface (CLI)	Describes how to use the Command Line Interface (CLI).
4 System Connection and IP Address	Describes how to manage the system account and IP address.
5 Port Configuration	Describes how to configure the Ethernet ports.
6 System Environment	Describes how to configure the system environment and management functions.
7 Network Management	Describes how to configure the network management functions.
8 System Main Functions	Describes how to configure the system main functions.
9 IP Multicast	Describes how to configure the IP multicast functions.
11 GPON Configuration	Describes how to configure the GPON functions.
12 System Software Upgrade	Describes how to upgrade the system software.
13 Abbreviations	Lists all abbreviations and acronyms which appear in this document.

Tab. 1.1 Overview of Chapters

1.3 Document Convention

This guide uses the following conventions to convey instructions and information.

Information

i

This information symbol provides useful information when using commands to configure and means reader take note. Notes contain helpful suggestions or references.

Warning

⚠

This warning symbol means danger. You are in a situation that could cause bodily injury or broke the equipment. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents by making quick guide based on this guide.

1.4 Document Notation

The following table shows commands used in guide book. Please be aware of each command to use them correctly.

Notation	Description
a	Commands you should use as is.
NAME, PROFILE, VALUE, …	Variables for which you supply values.
[ ]	Commands or variables that appear within square brackets [ ] are optional.
< >	Range of number that you can use.
{ }	A choice of required keywords appears in braces { }. You must select one.
|	Optional variables are separated by vertical bars |.

Tab. 1.2 Command Notation of Guide Book

1.5 Virus Protection

To prevent a virus infection you may not use any software other than that which is released for the Operating System (OS based on Basis Access Integrator), Local Craft Terminal (LCT) and transmission system.

Even when exchanging data via network or external data media(e.g. floppy disks) there is a possibility of infecting your system with a virus. The occurrence of a virus in your system may lead to a loss of data and breakdown of functionality.

The operator is responsible for protecting against viruses, and for carrying out repair procedures when the system is infected.

You have to do the following:

- You have to check every data media (used data media as well as new ones) for virus before reading data from it.
- You must ensure that a current valid virus scanning program is always available. This program has to be supplied with regular updates by a certified software.
- It is recommended that you make periodic checks against viruses in your OS.
- At the LCT it is recommended to integrate the virus scanning program into the startup sequence.

2 System Overview

LD3008 and LD3016 can be used as a GPON Optical Line Termination (OLT) supporting 8-Port and 16-Port GPON interfaces respectively as well as L3 switch of supporting 4-Port 1/10GBase-R (SFP+) 10 Gigabit Ethernet and 4-Port 10/100/1000Base-T(RJ45) Gigabit Ethernet service. It terminates the traffic coming from the subscriber lines and consolidates it on one or more Gigabit Ethernet interfaces towards the metropolitan area.

The GPON technology adds new features and functionality targeted at improving performance and interoperability, and adds support for new applications, services, and deployment scenarios. Among these changes are improvements in data rate and reach performance, diagnostics, and stand-by mode, to name a few.

The LD3008 and LD3016 introduce a point-to-multipoint concept with the GPON technology, which enables a cost-effective FTTx service. The reason why GPON is considered as a cost-effective solution is its usage of a passive splitter rather than an active switching system.

Both LD3008 and LD3016 has two Power Supply Unit (PSU) mounting slots on the front panel. Each PSU is comprised of single power input. For power redundancy, user can equip dual PSUs into 2-slot.

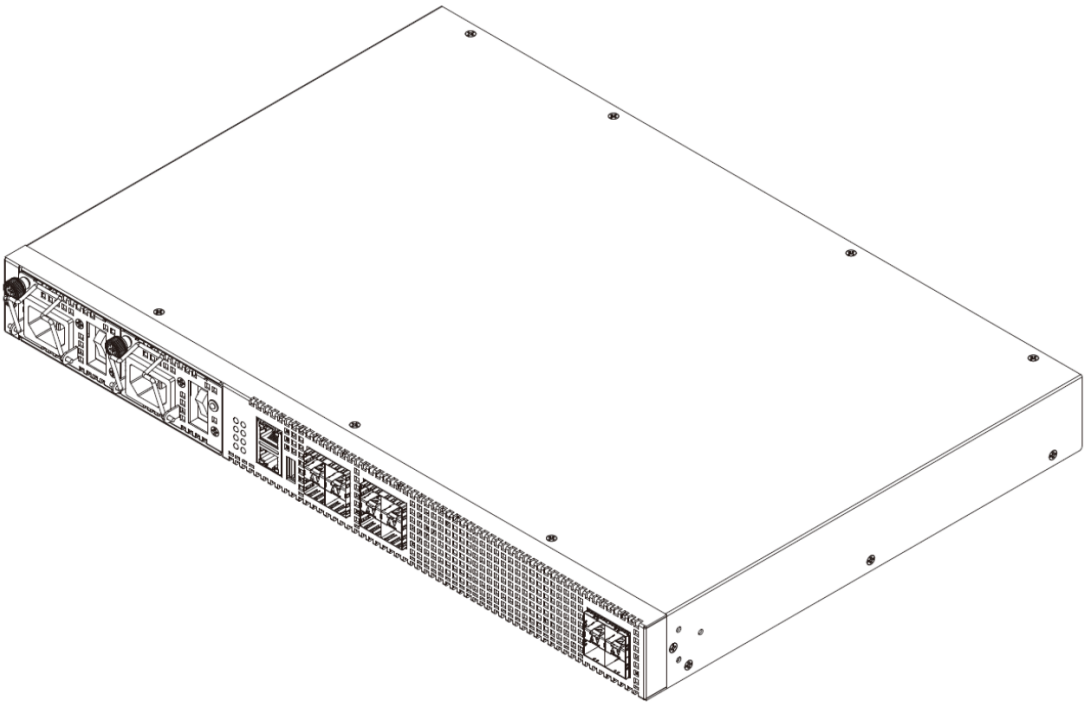


Fig. 2.1 Front View of the LD3008

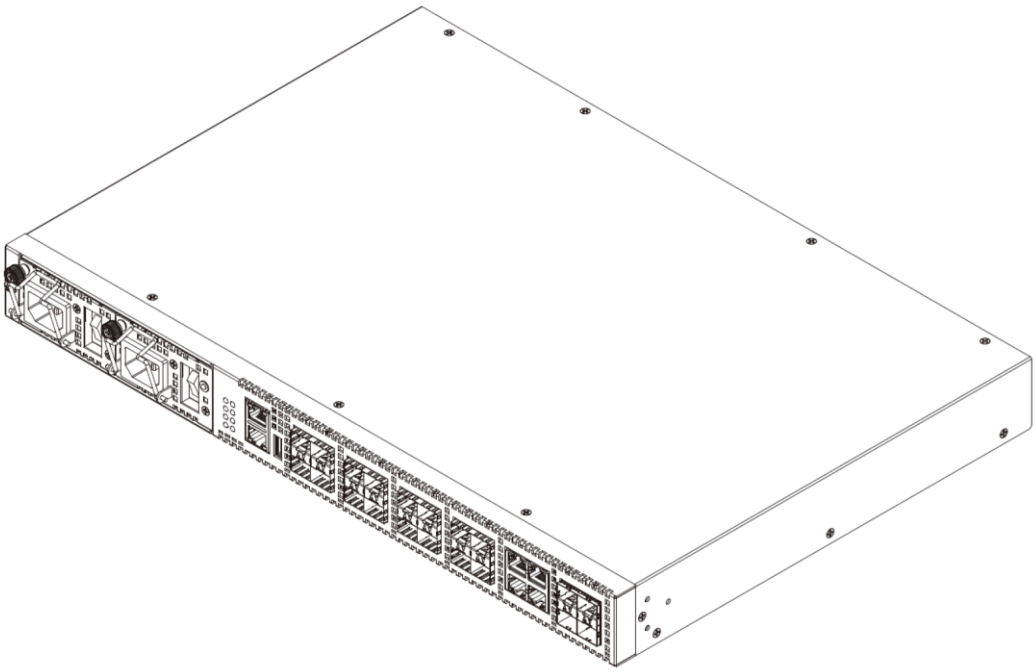


Fig. 2.2 Front View of the LD3016

2.1 System Features

This section introduces the main features of the LD3008 and LD3016 GPON OLT system which provides Layer 3 switching, Ethernet switching and GPON functionalities.

Virtual Local Area Network (VLAN)

Virtual local area network (VLAN) is made by dividing one network into several logical networks. Packets cannot be transmitted between different VLANs. Therefore it can prevent needless packets accumulating and strengthen security. The OLTS recognizes 802.1Q tagged frame and supports maximum 4096 VLANs. Port-based, protocol-based, MAC-based, and subnet-based VLANs are supported in the OLTS.

Quality of Service (QoS)

For the OLTS, QoS-based forwarding sorts traffic into a number of classes and marks the packets accordingly. Thus, different quality of service is provided to each class, which the packets belong to. The rich QoS capabilities enable network managers to protect mission-critical applications and support differentiated level of bandwidth for managing traffic congestion. The OLTS support ingress and egress (shaping) rate limiting, and different scheduling type such as Strict Priority (SP), Weighted Round Robin (WRR) and Deficit Round Robin (DRR).

IP Multicast

Because broadcasting in a LAN is restricted if possible, multicasting could be used instead of broadcasting by forwarding multicast packets only to the member hosts who joined multicast group. The OLTS provides IGMPv2, IGMP snooping.

SNMP

Simple Network Management Protocol (SNMP) is to manage network elements using TCP/IP protocol. The OLTS supports SNMPv1, 2, 3 and Remote Monitoring (RMON). Network operator can use MIB also to monitor and manage the OLTS.

IP Routing

The OLTS is Layer 3 switch, which has routing table and IP address as router. Therefore, it supports static routing.

Dynamic Host Configuration Protocol (DHCP)

The OLTS supports Dynamic Host Configuration Protocol (DHCP) server that automatically assigns IP address to clients accessed to network. That means it has IP address pool, and operator can effectively utilize limited IP source by leasing temporary IP address. In Layer 3 network, DHCP request packet can be sent to DHCP server via DHCP relay and option 82 function.

Spanning Tree Protocol (STP)

To prevent loop and preserve backup route in Layer 2 network, the OLTS supports Spanning Tree Protocol (STP) defined in IEEE 802.1D. Between STP enabled switches, a root bridge is automatically selected and the network remains in tree topology. However, the recovery time in STP is very slow (about 30 seconds), Rapid Spanning Tree Protocol (RSTP) is also provided. IEEE 802.1w defines the recovery time as 2 seconds. If there is only one VLAN in the network, traditional STP works. However, in more than one VLAN network, STP cannot work per VLAN. To avoid this problem, the OLTS supports Multiple Spanning Tree Protocol (MSTP) IEEE 802.1s.

Link Aggregation (Trunking)

The OLTS aggregates several physical interfaces into one logical port (aggregate port). Port trunk aggregates interfaces with the standard of same speed, same duplex mode, and same VLAN ID. According to IEEE 802.3ad, the OLTS can configure maximum 8 aggregate ports and up to 6 trunk groups.

Link Aggregation Control Protocol (LACP)

The OLTS supports Link Aggregation Control Protocol (LACP), complying with IEEE 802.3ad, which aggregates multiple links of equipments to use more enlarged bandwidth.

System Management based on CLI

It is easy for users who administer system by using telnet or console port to configure the functions for system operating through CLI. CLI is easy to configure the needed functions after looking for available commands by help menu different with UNIX.

Broadcast Storm Control

Broadcast storm control is, when too much of broadcast packets are being transmitted to network, a situation of network timeout because the packets occupy most of transmit capacity. The OLTS supports broadcast and multicast storm control, which disuses flooding packet, that exceed the limit during the time configured by user.

Profile-based Management

With profile function, each OLT can be configured and managed. By creating several profiles to have some configurations, if an OLT is assigned to use an appropriate profile of the profiles, the assigned profile will be automatically applied to the OLT. So the use of profile provides easy and efficient manageability for the OLT conforming policies and service environments of users.

Outband Management Interface

The OLTS can connect to equipments at remote place by assigning IP address to MGMT interface. Since MGMT interface is operated regardless of status of service port, it is still possible to configure and manage equipment at remote place even though problem such

as link disconnection is occurred.

RADIUS and TACACS+

The OLTS supports client authentication protocol, that is RADIUS (Remote Authentication Dial-In User Service) and TACACS+ (Terminal Access Controller Access Control System Plus). Not only user IP and password registered in switch but also authentication through RADIUS server and TACACS+ server are required to access. So security of system and network management is strengthened.

Secure Shell (SSH)

Network security is getting more important because the access network has been generalized among numerous users. However, typical FTP and telnet service have big weakness for their security. Secure shell (SSH) is a network protocol that allows establishing a secure channel between a local and a remote computer. It uses public-key cryptography to authenticate the remote computer and to allow the remote computer to authenticate the user.

⚠ Security and Encryption clauses can be negotiated to operate only if there is a special request from the user.

3 Command Line Interface (CLI)

The LD3008 and LD3016 enable system administrators to manage the OLTS by providing the command line interface (CLI). This user-friendly CLI provides you with a more convenient management environment.

To manage the system with the CLI, a management network environment is required. The OLTS can connect to the management network either directly (outband) or through the access network (inband). It can even connect using a combination of the two; for example, a cascaded OLTS connects inband to the cascading switch, and then from the cascading switch to the management network through the outband interface.

The OLTS also provides the RS232 console interface to simply access the system with a provided RJ45-to-DB9 cable.

3.1 Configuration Mode

You can configure and manage the OLTS with the CLI via a management network environment or the console interface.

The CLI provides the following command modes:

- Privileged EXEC View Mode
- Privileged EXEC Enable Mode
- Global Configuration Mode
- Bridge Configuration Mode
- DHCP Pool Configuration Mode
- DHCP Option 82 Configuration Mode
- Interface Configuration Mode
- Rule Configuration Mode
- RMON Configuration Mode
- GPON Configuration Mode

3.1.1 Privileged EXEC View Mode

When you log in to the switch, the CLI will start with *Privileged EXEC View* mode which is a read-only mode. In this mode, you can see a system configuration and information with several commands.

Tab. 3.1 shows main command of *Privileged EXEC View* mode.

Command	Description
enable	Opens *Privileged EXEC Enable* mode.
exit	Logs out the switch.
show	Shows a system configuration and information.

Tab. 3.1 Main Command of *Privileged EXEC View* Mode

3.1.2 Privileged EXEC Enable Mode

To configure the switch, you need to open *Privileged EXEC Enable* mode with the **enable** command, then the system prompt will changes from SWITCH> to SWITCH#.

Command	Mode	Description
enable	View	Opens *Privileged EXEC Enable* mode.

You can set a password to *Privileged EXEC Enable* mode to enhance security. Once setting a password, you should enter a configured password, when you open *Privileged EXEC Enable* mode.

Tab. 3.2 shows main commands of *Privileged EXEC Enable* mode.

Command	Description
clock	Sets a system time and date.
configure terminal	Opens *Global Configuration* mode.
reload	Reboots the system.
telnet	Connects to a remote host through telnet.
terminal length	Configures the number of lines of the current terminal.
traceroute	Traces a packet route.
where	Displays users accessing the system via telnet or console.

Tab. 3.2 Main Command of *Privileged EXEC Enable* Mode

In *Privileged EXEC Enable* mode, you can send a subcommand to an FTP server by using the **quote** *COMMAND commands*.

Command	Mode	Description
quote *COMMAND*	Enable	Sends a command to the Linux. COMMAND: external command

3.1.3 Global Configuration Mode

In *Global Configuration* mode, you can configure general functions of the system. You can also open another configuration mode from this mode.

To open *Global Configuration* mode, enter the **configure terminal** command, and then the system prompt will be changed from SWITCH# to SWITCH(config)#.

Command	Mode	Description
configure terminal	Enable	Opens *Global Configuration* mode.

Tab. 3.3 shows main commands of *Global Configuration* mode.

Command	Description

access-list	Configures an access list.
bridge	Opens *Bridge Configuration* mode.
dns	Sets a DNS server.
dot1x	Configures 802.1X authentication.
exec-timeout	Sets an auto log-out timer.
help	Shows a description of the interactive help system.
hostname	Sets a host name of the system.
interface	Opens *Interface Configuration* mode to configure a specified interface.
mvr	Configures MVR.
ntp	Configures NTP.
passwd	Sets a system password.
qos	Configures QoS.
rmon-alarm	Opens *RMON Configuration* mode to configure RMON alarm.
snmp	Configures SNMP.
ssh	Configures SSH.
syslog	Configures a syslog.
threshold	Sets a system threshold.

Tab. 3.3 Main Command of *Global Configuration* Mode

3.1.4 Bridge Configuration Mode

In *Bridge Configuration* mode, you can configure various Layer 2 functions such as VLAN, STP, LACP, etc.

To open *Bridge Configuration* mode, enter the **bridge** command, then the system prompt will be changed from SWITCH(config)# to SWITCH(bridge)#.

Command	Mode	Description
bridge	Global	Opens *Bridge Configuration* mode.

Tab. 3.4 shows main commands of *Bridge Configuration* mode.

Command	Description
lacp	Configures LACP.
mac	Configures a MAC table.
mirror	Configures a port mirroring.
port	Configures Ethernet port.
trunk	Configures a trunk port.
vlan	Configures VLAN.

Tab. 3.4 Main Command of *Bridge Configuration* Mode

3.1.5 DHCP Pool Configuration Mode

In *DHCP Pool Configuration* mode, you can configure general functions of DHCP per each DHCP pool. The OLTS supports multiple DHCP environments with this pool-based DHCP configuration.

To open *DHCP Pool Configuration* mode, enter the **ip dhcp pool** command, then the system prompt will be changed from SWITCH(config)# to SWITCH(config-dhcp[POOL])#.

Command	Mode	Description
ip dhcp pool *POOL*	Global	Opens *DHCP Pool Configuration mode* to configure DHCP.

To open *DHCP Pool Configuration* mode, use the **service dhcp** command in the *Global Configuration* mode first!

Tab. 3.5 shows main commands of *DHCP Pool Configuration* mode.

Command	Description
default-router	Configures the default gateway of the pool.
dns-server	Configures a DNS server.
range	Configures the range of IP addresses.

Tab. 3.5 Main Command of *DHCP Pool Configuration* Mode

3.1.6 DHCP Option Configuration Mode

In *DHCP Option Configuration* mode, you can configure DHCP option. You can define DHCP options that are carried in the DHCP communication between DHCP server and client or relay agent. A specific DHCP option can be defined by its format type, length and value. To open *DHCP Option Configuration* mode, use the command. Then the system prompt will be changed from SWITCH(config)# to SWITCH(dhcp-opt[NAME])#.

Command	Mode	Description
ip dhcp option format *NAME*	Global	Opens *DHCP Option Configuration* mode to configure DHCP options.

Tab.3.6 is the main commands of *DHCP Option Configuration* mode.

Command	Description
attr	Configures the attribute for option field in the DHCP packet.

Tab. 3.6 Main Command of *DHCP Option Configuration* Mode

3.1.7 DHCP Option 82 Configuration Mode

In *DHCP Option 82 Configuration* mode, you can configure DHCP option 82 for DHCP relay agent. This feature enables network administrators to manage IP resources more

efficiently.

To open *DHCP Option 82 Configuration* mode, enter the **ip dhcp option82** command, then the system prompt will be changed from SWITCH(config)# to SWITCH(config-opt82)#.

Command	Mode	Description
ip dhcp option82	Global	Opens *DHCP Option 82 Configuration* mode to configure DHCP option 82.

To open *DHCP Option 82 Configuration* mode, use the **service dhcp** command in the *Global Configuration* mode first!

Tab. 3.7 is the main commands of *DHCP Option 82 Configuration* mode.

Command	Description
policy	Configures the policy for option 82 field in the DHCP packet.
system-remote-id	Configures a system remote ID.
system-circuit-id	Configures a system circuit ID.

Tab. 3.7 Main Command of *DHCP Option 82 Configuration* Mode

3.1.8 Interface Configuration Mode

In *Interface Configuration* mode, you can configure Ethernet interfaces. GPON interfaces should be configured in *GPON-OLT Configuration* mode.

To open *Interface Configuration* mode, enter the **interface** command, then the system prompt will be changed from SWITCH(config)# to SWITCH(config-if)#.

Command	Mode	Description
interface *INTERFACE*	Global	Opens *Interface Configuration* mode.

Tab. 3.8 shows main commands of *Interface Configuration* mode.

Command	Description
description	Specifies a description.
ip address	Assigns IP address.
shutdown	Deactivates an interface.
mtu	Sets MTU value.

Tab. 3.8 Main Command of *Interface Configuration* Mode

3.1.9 Rule Configuration Mode

Rule configuration is classified by three different modes according to its roles for Rule mechanism. You can configure a rule for incoming or outgoing packets. Using the function, you can handle packets classified by the rule.

To open *Rule Configuration* mode, enter the **flow, policer and policy** commands, then

the system prompt will be changed from SWITCH(config)# to SWITCH(config-flow[NAME])#, SWITCH(config-policer[NAME])# and SWITCH(config-policy[NAME])# .

Command	Mode	Description
flow *NAME* **create**	Global	Opens *Flow Configuration* mode.
policer *NAME* **create**		Opens *Policer Configuration* mode.
policy *NAME* **create**		Opens *Policy Configuration* mode.

Tab. 3.9 shows main commands of *Rule Configuration* mode.

Command	Description
cos	Classifies an IEEE 802.1p priority.
mac	Classifies a MAC address.
action match	Configures a rule action for classified packets.
rate-limit	Comfigures a rate-limit of classified packets
priority	Configures a rule priority of specified policy.

Tab. 3.9 Main Command of *Rule Configuration* Mode

3.1.10 RMON Configuration Mode

In *RMON Configuration* mode, you can configure RMON alarm, RMON event and RMON history. The OLTS provides three different configuration modes to configure each type of RMON.

Command	Mode	Description
rmon-alarm <1-65535>	Global	Opens *RMON Configuration* mode. 1-65535: index number
rmon-event <1-65535>		
rmon-history <1-65535>		

Tab. 3.10 shows main commands of *RMON Configuration* mode.

Command	Description
active	Activates RMON.
owner	Shows the subject which configures each RMON and uses relevant information.

Tab. 3.10 Main Command of *RMON Configuration* Mode

3.1.11 GPON Configuration Mode

In *PON Configuration* mode, you can configure GPON-related functions. To open *GPON Configuration* mode, enter the **gpon** command, then the system prompt will be changed from SWITCH(config)# to SWITCH(gpon)#.

Command	Mode	Description
gpon	Global	Opens *GPON Configuration* mode.

3.1.11.1 GPON-OLT Configuration Mode

In *GPON-OLT Configuration* mode, you can configure general functions a GPON OLT interface such as an alarm, encryption, bandwidth, ONT registration, etc.

To open *GPON-OLT Configuration* mode, enter the **gpon-olt** command, then the system prompt will be changed from SWITCH(gpon)# to SWITCH(config-gpon-olt[N])#.

Command	Mode	Description
gpon-olt *OLT-ID*	GPON GPON-OLT	Opens *GPON-OLT Configuration* mode.

Tab. 3.11 shows main commands of *GPON-OLT Configuration* mode.

Command	Description
discover-serial-number	Configures an ONU (ONT) registration using ONT's serial number.
olt	Configures an OLT-related function.
onu add	Registers an ONU (ONT).
onu upgrade	Upgrades an ONU firmware.

Tab. 3.11 Main Command of *GPON-OLT Configuration* Mode

3.1.11.2 ONU Profile Configuration Mode

In *ONU Profile Configuration* mode, you can configure an ONU profile.

To open *ONU Profile Configuration* mode, enter the **onu-profile** command, then the system prompt will be changed from SWITCH(gpon)# to SWITCH(config-onu-profile[NAME])#.

Command	Mode	Description
onu-profile *NAME* **create**	GPON	Opens *ONU Profile Configuration* mode.

Tab. 3.12 shows main commands of *ONU Profile Configuration* mode.

Command	Description
rate-limit	Comfigures a rate-limit of a traffic flow between OLT and ONU(ONT).
vlan-filter	Configures an VLAN filtering.

Tab. 3.12 Main Command of *ONU Profile Configuration* Mode

3.2 Configuration Mode Overview

Fig. 3.1 shows the overview of the configuration mode for the LD3008 and LD3016.

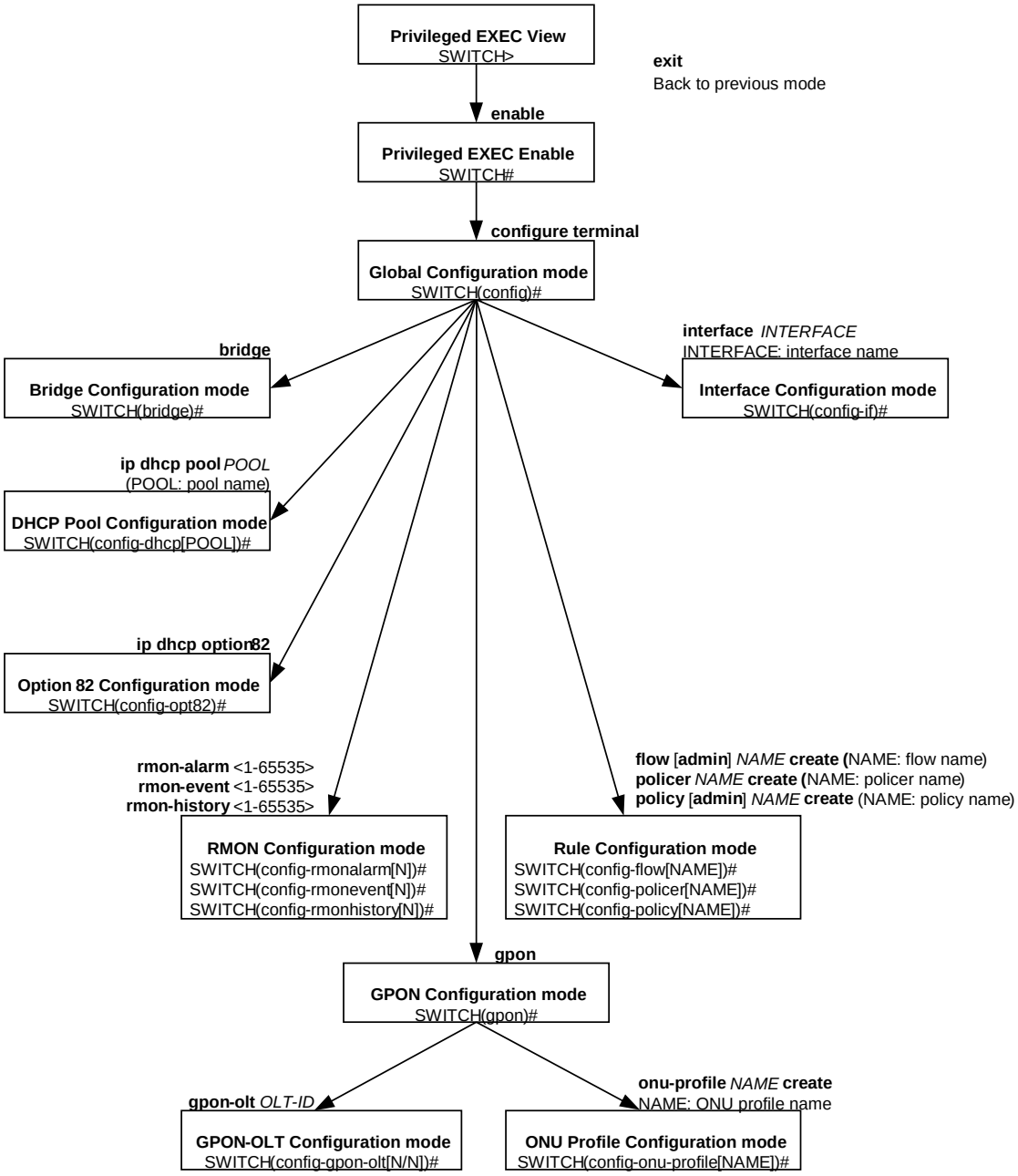


Fig. 3.1 Overview of Configuration Mode

3.3 Useful Tips

This section describes useful tips for operating the OLTS with a CLI. **All examples are refered to the LD3016 outputs.**

3.3.1 Listing Available Command

To list available commands, input question mark <**?**> in the current mode. When you input the question mark <**?**>, you can see available commands used in this mode and variables following after the commands.

The following is the available commands on *Privileged EXEC Enable* mode of the LD3008 ans LD3016.

```
SWITCH# ?
Exec commands:
  clear          Reset functions
  clock          Manually set the system clock
  configure      Enter configuration mode
  copy           Copy from one file to another
  debug          Debugging functions
  default-os     Select default OS
  disconnect     Disconnect user connection
  enable         Turn on privileged mode command
  erase          Erase saved configuration
  exit           End current mode and down to previous mode
  halt           Halt process
  help           Description of the interactive help system
  no             Negate a command or set its defaults
  ping           Send echo messages
  quote          Execute external command
  release        Release the acquired address of the interface

(Omitted)

SWITCH#
```

i

Question mark <**?**> will not be shown in the screen and you do not need to press <**ENTER**> key to display the command list.

If you need to find out the list of available commands of the current mode in detail, use the following commands.

Command	Mode	Description
show list	All	Shows available commands of the current mode.
show cli		Shows available commands of the current mode with tree structure.

In case that the OLTS installed command shell, you can find out commands starting with a specific alphabet. Input the first letter and question mark without space. The following is an example of finding out the commands starting "**s**" in *Privileged EXEC Enable* mode of

the OLTS.

```
SWITCH# s?
show          Show running system information
ssh           Configure secure shell

SWITCH# s
```

In addition, it is possible to view variables you should input following commands. After inputting the command you need, make one space and input a question mark. The following is an example of viewing variables after the **write** command. Please note that you must input one space between the command and question mark.

```
SWITCH# write ?
memory        Write to NV memory
terminal      Write to terminal

SWITCH# write
```

The OLTS also provide the simple instruction of calling the help string with the **help** command. You can see the instruction using the command regardless of the configuration mode.

To display the instruction of calling the help string for using CLI, use the following command.

Command	Mode	Description
help	All	Shows the instruction of calling the help string for using CLI.

The following is the actual output of the **help** command.

```
SWITCH# help
Furukawa CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

SWITCH#
```

3.3.2 Calling Command History

In case of installed command shell, you do not have to enter the command you entered before. When you need to reuse the commands you did, use this arrow key <↑>. When you press the arrow key, the commands will be displayed in the latest order.

The following is an example of calling command history after using several commands. After using these commands in order: **show clock** → **configure terminal** → **interface** *1* → **exit**, press the arrow key <↑> and then you will see the commands from latest one: **exit** → **interface** *1* → **configure terminal** → **show clock**.

```
SWITCH(config)# exit
SWITCH# show clock
Mon, 5 Jan 1970 23:50:12 +0000
SWITCH# configure terminal
SWITCH(config)# interface 1
SWITCH(config-if)# exit
SWITCH(config)# exit
SWITCH# (press the arrow key ↑)
SWITCH# exit (press the arrow key ↑)
SWITCH# interface 1 (press the arrow key ↑)
SWITCH# configure terminal (press the arrow key ↑)
SWITCH# show clock (press the arrow key ↑)
```

To save the command history in non-volatile memory, use the following command.

Command	Mode	Description
history non-volatile [<10-2000>]	Global	Saves the command history. 10-2000: history recording max. count (default:2000)

To delete the non-volatile command history, use the following command.

Command	Mode	Description
clear history non-volatile	Global	Deletes the command history.
no history non-volatile		Disables the function to save a command history.

The system records the command history per the user. To delete the non-volatile command history of the specific user, use the following command.

Command	Mode	Description
remove history user *NAME*	Global	Deletes the command history of the specified user. NAME: user name

To display the command history, use the following command.

Command	Mode	Description
show history	Enable	Shows a command history.
show cli history list		Shows a command history list.
show history non-volatile [<1-2000>]	Enable Global	Shows a command history. non-volatile: reserves the command history. 1-2000: line number to be displayed
show history non-volatile user *NAME* [<1-2000>]		Shows the command history of specified user. NAME: user name

		1-2000: line number to be displayed

To enable/disable the command history logging, use the following command.

Command	Mode	Description
command-history-log enable [**default**]	Enable Global	Enables the command history logging.
command-history-log disable [**default**]		Disables the command history logging.

To display the command history logging in SNMP, use the following command.

Command	Mode	Description
command-history-log snmp {**get** | **set** | **all** | **none**}	Enable Global	Shows command history logs in SNMP. all: all of logs of the SNMP get: logs that SNMP get request . none: no history that SNMP request. set: logs that SNMP set request.

To display the configured status of command history logging, use the following command.

Command	Mode	Description
show command-history-log status	Enable Global	Shows the command history logging status.

To back up a command history log file using FTP or TFTP, use the following command.

Command	Mode	Description
copy {**ftp** | **tftp**} **history-log upload** *LOGFILE*	Enable	Uploads a command history log file to FTP or TFTP server with the log file name. LOGFILE: log file name

3.3.3 Using Abbreviation

Several commands can be used in the abbreviated form. The following table shows some examples of abbreviated commands.

Command	Abbreviation
clock	cl
exit	ex
show	sh
configure terminal	con te

Tab. 3.13 Command Abbreviation

3.3.4 Using Command of Privileged EXEC Enable Mode

You can execute the commands of *Privileged EXEC Enable* mode as **show**, **ping**, **telnet**, **traceroute**, and so on regardless of which mode you are located on.

To execute the commands of *Privileged EXEC Enable* mode on different mode, use the following command.

Command	Mode	Description
do *COMMAND*	All	Executes the commands of *Privileged EXEC Enable* mode.

3.3.5 Exit Current Command Mode

To exit to the previous command mode, use the following command.

Command	Mode	Description
exit	All	Exits to the previous command mode.
end		Exits to *Privileged EXEC Enable* mode.

If you use the **exit** command in *Privileged EXEC Enable* mode or *Privileged EXEC View* mode, you will be logged out!

3.3.6 The Command Execution Limit

If you try to have more than ‘1000’ processes executed by a command, you meet a limit block with “Too many to process” error message by system policy as follows:

```
SWITCH(bridge)# vlan add 3-4090 1-24 tagged
% Too many to process(user-input/maximum:98112/1000)
SWITCH(bridge)#
```

By using command above, it creates 4088 VLANs, and registers each created VLAN to individual ports from 1 to 24 with tagged option repeatedly. It indicates that you try to run 98112 (4088 x 24) actions in the system. The system processes individually the values within a specified range.

4 System Connection and IP Address

4.1 System Connection

After installing the system, the OLT is supposed to examine that each port is correctly connected to network and management PC. You can connect to the system to configure and manage the OLT. This section provides instructions how to change password for system connection and how to connect to the system through telnet.

4.1.1 System Login

After installing the OLT, finally make sure that each port is correctly connected to PC for network and management. Then, turn on the power and boot the system as follows.

Step 1 When you turn on the switch, booting will be automatically started and login prompt will be displayed.

```
SWITCH login:
```

Step 2 When you enter a login ID at the login prompt, the password prompt will be displayed, and then enter the proper password to log in the system. By default setting, the login ID is configured as *admin* with no password.

```
SWITCH login: admin
Password:
SWITCH>
```

Step 3 In *Privileged EXEC View* mode, you can check only the configuration for the switch. To configure and manage the switch, you should begin *Privileged EXEC Enable* mode. The following is an example of beginning *Privileged EXEC Enable* mode.

```
SWITCH> enable
SWITCH#
```

4.1.2 Password for Privileged EXEC Enable Mode

You can configure a password to enhance the security for *Privileged EXEC Enable* mode. To configure a password for *Privileged EXEC Enable* mode, use the following command.

Command	Mode	Description
passwd enable *PASSWORD*	Global	Configures a password to begin *Privileged EXEC Enable* mode.
passwd enable 8 *PASSWORD*		Configures an encrypted password.

⚠ **password enable** does not support encryption at default value. Therefore it shows the string (or password) as it is when you use the **show running-config** command. In this case, the user's password is shown to everyone and has unsecured environment.

To encrypt the password which will be shown at running-config, you should use the **service password-encryption** command. And to represent the string (password) is encrypted, input **8** before the encrypted string.

When you use the **password enable** command with **8** and "the string", you will make into *Privileged EXEC Enable* mode with the encrypted string. Therefore, to log in the system, you should do it with the encrypted string as password that you configured after **8**. In short, according to using the **8** option or not, the next string is encrypted or not.

The following is an example of configuring the password in *Privileged EXEC Enable* mode as *testpassword*.

```
SWITCH# configure terminal
SWITCH(config)# passwd enable testpassword
SWITCH(config)#
```

The following is an example of accessing after configuring a password.

```
SWITCH login: admin
Password:
SWITCH> enable
Password:
SWITCH#
```

To delete the configured password, use the following command.

Command	Mode	Description
no passwd enable	Global	Deletes the password.

The created password can be displayed with the **show running-config** command. To encrypt the password not to be displayed, use the following command.

Command	Mode	Description
service password-encryption	Global	Encrypts the system password.

To disable password encryption, use the following command.

Command	Mode	Description
no service password-encryption	Global	Disables password encryption.

4.1.3 Changing Login Password

To configure a password for created account, use the following command.

Command	Mode	Description
passwd [*NAME*]	Global	Configures a password for created account.

The following is an example of changing the current password.

```
SWITCH(config)# passwd
Changing password for admin
Enter the new password (minimum of 5, maximum of 8 characters)
Please use a combination of upper and lower case letters and numbers.
Enter new password:junior95
Re-enter new password:junior95
Password changed.
SWITCH(config)#
```

The password you are entering will not be shown in the screen, so please be careful not to make a mistake.

4.1.4 Login Password Recovery Process

To recovery login password to default, perform the following step-by-step instruction:

Step 1
After the OLT is manually restarted, the booting messages are shown up. Keep on pressing [**Space Bar**] key right after "`[Loading OS1 image ...]`" is shown up on the screen.

Step 2
Enter "**password**" and press [ENTER] key when the boot process stops for a while next to "`[Image OK : os1]`" messages. The current password returns to the default setting password (*no password*). You have to set new password for admin.

Step 3
Verify the "`password restore to default...`" messages.

```
************************************************************
*                                                          *
*             Boot Loader Version 01.60.0006               *
*                   FURUKAWA ELECTRIC                      *
*                                                          *
************************************************************
Press 's' key to go to Boot Mode:  0

[Loading OS1 image ...]
                                        Step1 (Keep on pressing [Space Bar]

[Image OK : os1]

                                 password   Step 2

Freeing unused kernel memory: 56520k init
INIT: version 2.85 booting
password restore to default...   Step 3
Fri, 10 Mar 2000 22:21:35 +0000
```

```
INIT: Entering runlevel: 3

INIT: Start UP

SWITCH login: admin
Password:
SWITCH>
```

i The password of “admin” is restored to the factory default password (no password) if the operator has not created any user accounts.

4.1.5 Management for System Account

4.1.5.1 Creating System Account

For the OLTs, the administrator can create a system account. In addition, it is possible to set the security level from 0 to 15 to enhance the system security.

To create a system account, use the following command.

Command	Mode	Description
user add *NAME DESCRIPTION*	Global	Creates a system account.
user add *NAME* **level** <0-15> *DESCRIPTION*		Creates a system account with a security level.

i The account of level 0 to level 14 without any configuring authority only can use **exit** and **help** in *Privileged EXEC View* mode and cannot access to *Privileged EXEC Enable* mode. The account with the highest level 15 has a read-write authority.

To delete the created account, use the following command.

Command	Mode	Description
user del *NAME*	Global	Delete the created account.

To display a created account, use the following command.

Command	Mode	Description
show user	Enable/Global/Bridge	Shows a created account.

4.1.5.2 Security Level

For the OLT, it is possible to configure the security level from 0 to 15 for a system account. The level 15, as the highest level, has a read-write authority. The administrator can configure from level 0 to level 14. The administrator decides which level user uses which commands in which level. As the basic right from level 0 to level 14, it is possible to use **exit** and **help** command in *Privileged EXEC View* mode and it is not possible to access to

Privileged EXEC Enable mode.

To define the security level and its authority, use the following command.

Command	Mode	Description
privilege view level <0-15> {*COMMAND* | **all**}	Global	Uses the specific command of *Privileged EXEC View* mode in the level.
privilege enable level <0-15> {*COMMAND* | **all**}		Uses the specific command of *Privileged EXEC Enable* mode in the level.
privilege configure level <0-15> {*COMMAND* | **all**}		Uses the specific command of *Global Configuration* mode in the level.
privilege interface level <0-15> {*COMMAND* | **all**}		Uses the specific command of *Interface Configuration* mode in the level.
privilege vrrp level <0-15> {*COMMAND* | **all**}		Uses the specific command of *VRRP Configuration* mode in the level.
privilege bridge level <0-15> {*COMMAND* | **all**}		Uses the specific command of *Bridge Configuration* mode in the level.
privilege flow level <0-15> {*COMMAND* | **all**}		Uses the specific command of *Flow Configuration* mode in the level.
privilege policer level <0-15> {*COMMAND* | **all**}		Uses the specific command of *Policer Configuration* mode in the level.
privilege policy level <0-15> {*COMMAND* | **all**}		Uses the specific command of *Policy Configuration* mode in the level.
privilege rmon-alarm level <0-15> {*COMMAND* | **all**}		Uses the specific command of *RMON Configuration* mode in the level.
privilege rmon-event level <0-15> {*COMMAND* | **all**}		
privilege rmon-history level <0-15> {*COMMAND* | **all**}		
privilege dhcp-pool level <0-15> {*COMMAND* | **all**}		Uses the specific command of *DHCP Pool Configuration* mode in the level.
privilege dhcp-pool-class level <0-15> {*COMMAND* | **all**}		Uses the specific command of *DHCP Pool Class Configuration* mode in the level.
privilege dhcp-option82 level <0-15> {*COMMAND* | **all**}		Uses the specific command of *DHCP Option 82 Configuration* mode in the level.
privilege dhcp-class level <0-15> {*COMMAND* | **all**}		Uses the specific command of *DHCP Class Configuration* mode in the level.
privilege gpon level <0-15> {*COMMAND* | **all**}		Uses the specific command of *GPON Configuration* mode in the level.
privilege gpon-olt level <0-15> {*COMMAND* | **all**}		Uses the specific command of *GPON-OLT Configuration* mode in the level.

The commands that are used in low level can be also used in the higher level. For example, the command in level 0 can be used in from level 0 to level 14.

The commands starting with the same character are applied by inputting only the starting commands. For example, if you input **show**, all the commands starting with **show** are applied.

To delete a configured security level, use the following command.

Command	Mode	Description
no privilege	Global	Deletes all configured security levels.
no privilege view level <0-15> {*COMMAND* | **all**}		Deletes a configured security level on each mode.
no privilege enable level <0-15> {*COMMAND* | **all**}		
no privilege configure level <0-15> {*COMMAND* | **all**}		
no privilege interface level <0-15> {*COMMAND* | **all**}		
no privilege flow level <0-15> {*COMMAND* | **all**}		
no privilege vrrp level <0-15> {*COMMAND* | **all**}		
no privilege policer level <0-15> {*COMMAND* | **all**}		
no privilege policy level <0-15> {*COMMAND* | **all**}		
no privilege bridge level <0-15> {*COMMAND* | **all**}		
no privilege rmon-alarm level <0-15> {*COMMAND* | **all**}		
no privilege rmon-event level <0-15> {*COMMAND* | **all**}		
no privilege rmon-history level <0-15> {*COMMAND* | **all**}		
no privilege dhcp-pool level <0-15> {*COMMAND* | **all**}		
no privilege dhcp-pool-class level <0-15> {*COMMAND* | **all**}		
no privilege dhcp-option82 level <0-15> {*COMMAND* | **all**}		
no privilege dhcp-class level <0-15> {*COMMAND* | **all**}		
no privilege gpon level <0-15> {*COMMAND* | **all**}		
no privilege gpon-olt level <0-15> {*COMMAND* | **all**}		

To display a configured security level, use the following command.

Command	Mode	Description
show privilege	Enable	Shows a configured security level.

show privilege now	Global Bridge	Shows a security level of current mode.

The following is an example of creating the system account *test0* having a security level 10 and *test1* having a security level 1 with no password.

```
SWITCH(config)# user add test0 level 0 level0user
Changing password for test0
Enter the new password (maximum of 8 characters)
Please use a combination of upper and lower case letters and numbers.
Enter new password:(Enter)
Bad password: too short.

Warning: weak password (continuing).
Re-enter new password: (Enter)
Password changed.
SWITCH(config)# user add test1 level 1 level1user
Changing password for test1
Enter the new password (maximum of 8 characters)
Please use a combination of upper and lower case letters and numbers.
Enter new password: (Enter)
Bad password: too short.

Warning: weak password (continuing).
Re-enter new password: (Enter)
Password changed.
SWITCH(config)# show user
=====================================================
 User name            Description        Level
=====================================================
test0                 level0user          0
test1                 level1user          1
SWITCH(config)#
```

The following is an example of configuring an authority of the security level 0 and 1.

```
SWITCH(config)# privilege view level 0 enable
SWITCH(config)# privilege enable level 0 show
SWITCH(config)# privilege enable level 1 configure terminal
SWITCH(config)# show privilege

 Command Privilege Level Configuration
 ---------------------------------------------
 Node          All   Level   Command
 EXEC(ENABLE)          1     configure terminal
 EXEC(VIEW)            0     enable
 EXEC(ENABLE)          0     show

 3 entry(s) found.

SWITCH(config)#
```

In the above configuration, as level 0, it is possible to use only show command in *Privileged EXEC Enable* mode; however as level 1, it is possible to use not only the commands in level 1 but also time configuration commands in *Privileged EXEC Enable* mode and accessing commands to *Global Configuration* mode.

4.1.6 Limiting the Number of Users

For the OLT, you can limit the number of users accessing the switch through telnet. In case of using the system authentication with RADIUS or TACACS+, a configured number includes the number of users accessing the switch via the authentication server.

To set the number of users accessing the switch, use the following command.

Command	Mode	Description
login connect <1-8>	Global	Sets the number of users accessing the switch. (default: 8)
no login connect		Deletes a configured value.

4.1.7 Limiting the Number of login attemps

For security reasons of the system, Administrator can configure the number of the login attempts. To configure the system login attempts, use the following command.

Command	Mode	Description
login attempts <1-5> **delay** <5-60>	Global	Sets login attempts. 1-5: number of retry login attempts (default: 5) 5-60: access delay time (default: 5 minutes)

To display a configuration of login attempts function, use the following command.

Command	Mode	Description
show login attempts log [*USER*]	Enable Global Bridge	Shows login attempt information

To delete or reset the configured login attempts, use the following command.

Command	Mode	Description
no login attempts delay	Global	Resets the number of login attempts configured and access delay time. (default:5 number , 5minutes)
clear login attempts log [*USER*]	Enable Global Bridge	Deletes the login attempt information.

4.1.8 Auto Log-out

For security reasons of the OLT, if no command is entered within the configured inactivity time, the user is automatically logged out of the system. Administrator can configure the inactive session timeout.

To enable auto log-out function, use the following command.

Command	Mode	Description
exec-timeout <1-35791> [<0-59>]	Global	Enables auto log-out. 1-35791: time unit in minutes (by default 10 minutes) 0-59: time unit in seconds
exec-timeout 0		Disables auto log-out.

To display a configuration of auto-logout function, use the following command.

Command	Mode	Description
show exec-timeout	Enable Global Bridge	Shows a configuration of auto-logout function.

The OLT uses the global auto log-out function to determine how long to manage state information for a session and to determine when to drop sessions that do not become fully established. These global auto log-out timeouts apply globally to all sessions.

To enable auto log-out function for all sessions, use the following command.

Command	Mode	Description
global-timeout <1-35791> [<0-59>]	Global	Enables auto log-out for all sessions. 1-35791: timeout value in minutes 0-59: timeout in seconds
global-timeout 0		Disables auto log-out for all sessions.

4.1.9 Telnet Access

To connect to a remote host via telnet, use the following command.

Command	Mode	Description
telnet *DESTINATION* [*TCP-PORT*]	Enable	Connects to a remote host. DESTINATION: IPv4/IPv6 address or host name INTERFACE: interface name
telnet *DESTINATION* **interface** *INTERFACE* [*TCP-PORT*]		

In case of telnet connection, you need to wait for the **[OK]** message, when you save a system configuration. Otherwise, all changes will be lost when the telnet session is disconnected.

```
SWITCH# write memory
[OK]
SWITCH#
```

The system administrator can disconnect users connected from remote place. To disconnect a user connected through telnet, use the following command.

Command	Mode	Description
disconnect *TTY-NUMBER*	Enable	Disconnects a user connected through telnet.

To enable/disable the telnet service, use the following command.

Command	Mode	Description
service telnet	Global	Enables the use of telnet service (default)
no service telnet		Disables the use of telnet service
show service	Enable/Global/Bridge	Shows the status of network connection services (telnet/ssh/ftp/tftp/snmp).

The following is an example of disconnecting a user connected from a remote place.

```
SWITCH# where
admin at ttys0 from console for 4 days 22 hours 15 minutes 24.88 seconds
admin at ttyp0 from 10.0.1.4:1670 for 4 days 17 hours 53 minutes 28.76 seconds
admin at ttyp1 from 147.54.140.133:49538 for 6 minutes 34.12 seconds
SWITCH# disconnect ttyp0
SWITCH# where
admin at ttys0 from console for 4 days 22 hours 15 minutes 34.88 seconds
admin at ttyp1 from 147.54.140.133:49538 for 6 minutes 44.12 seconds
SWITCH#
```

4.1.10 IP Login Delay

It is possible to set the system that is not to accept users who fail three times of connection via ssh or telnet. And the blocked user can attempt to login after a specified time period.

To set system login delay feature, use the following command.

Command	Mode	Description
ip auth-fail-block	Global	Enables the login delay feature.
no ip auth-fail-block		Disables the login delay feature.
ip auth-fail-block expire-time <1-60>		Sets the expire time for log-in again after the failed log in the system. (default: 5 min)
no ip auth-fail-block expire-time		Restores the default expire time value.
ip auth-fail-block max-entry <1-512>		Sets the number of hosts that can log in the system. (default: 128)
no ip auth-fail-block max-entry		Restores the default value of hosts that can log in the system.
clear ip auth-fail-block entry [*A.B.C.D*]		Release the blocked hosts (IP).

To display the configured auth-fail-block, use the following command.

Command	Mode	Description
show ip auth-fail-block	Enable Global	Shows the configured auth-fail-block information.
show ip auth-fail-block entry		

4.1.11 System Rebooting

4.1.11.1 Manual System Rebooting

When installing or maintaining the system, some tasks require rebooting the system by various reasons. Then you can reboot the system with a selected system OS.

To restart the system manually, use the following command.

Command	Mode	Description
reload [**os1** | **os2**]	Enable	Restarts the system.

System rebooting wipes all the existing configurations. To save the configurations before the rebooting, answer “y” to the question *Do you want to save the system configuration? [y/n]*. If you answer “n” by misoperation, answer “n” to the next question *Do you want to reload the system? [y/n]* to cancel the rebooting and start the operation all over again.

The following is an example of restarting the system with the **reload** command.

```
SWITCH(enable)# reload
Do you want to save the system configuration? [y/n]
Do you want to reload the system? [y/n]
```

4.1.11.2 System Rebooting Scheduler

The **reload** command in *Privileged EXEC Eable Configuration* mode immediately reboots the system. Using **reload at/in** command in *Global Configuration* mode, you can schedule a rebooting time for any reason.

To set the system reloading scheduler, use the following command.

Command	Mode	Description
reload at *HH:MM DAY MONTH YEAR*	Global	Restarts the system at the specified exact time.
reload at *HH:MM* **in daily**		Restarts the system everyday at the same time.
reload in *HH:MM*		Restarts the system when the specified time period is over.

To cancel the reload previously scheduled, use the following command.

Command	Mode	Description
no reload all	Global	Deletes the whole system rebooting schedule settings.
no reload at [*HH:MM DAY*		Cancels the specified reload time, day and month.

MONTH YEAR]		
no reload at *HH:MM* **in daily**		Cancels the specified time (hour, minutes) for reloading everyday.
no reload in		Deletes the specified period for the reload.

To display the reload scheduler, use the following command.

Command	Mode	Description
show reload	Global	Displays the reload scheduler.

4.1.12 Auto Reset Configuration

The OLT reboots the system according to user's configuration. There are two basises for system rebooting. These are CPU and memory. CPU is rebooted in case CPU Load or Interrupt Load continues for the configured time. Memory is automatically rebooted in case memory low occurs as the configured times.

4.1.12.1 CPU Load

To enable auto system rebooting function, use the following command.

Command	Mode	Description
auto-reset cpu <50-100> <1-100> *TIME*	Bridge	Configure to reboot the system automatically in case an average of CPU or interrupt load exceeds the configured value during the user-defined time. 50-100: average of CPU load per 1 minute 1-100: average of interrupt load TIME: minute
no auto-reset cpu		Disables auto system rebooting function by CPU.

To display a current configured auto system rebooting, use the following command.

Command	Mode	Description
show auto-reset cpu	Enable Global Bridge	Shows a current configured auto system rebooting by CPU.

4.1.12.2 Memory

The OLT provides auto system rebooting function using memory low configuration. Memory-low indicates the low threshold value of system memory in use. To enable auto reset function of memory low setting when a memory-low has occurred as many as its specified numbers during the certain minutes, use the following command.

Command	Mode	Description
auto-reset memory <1-120> <1-10>	Bridge	Enable to reboot the system automatically in case memory low has occurred more than its count during the configured time. 1-120: time threshold of memory-low (default: 10 minutes) 1-10: counts of memory-low (default: 5)
no auto-reset memory		Disables auto system rebooting function by memory.

To display a current configured auto system rebooting by system memory, use the following command.

Command	Mode	Description
show auto-reset memory	Enable Global Bridge	Shows a current configured auto system rebooting by system memory.

4.2 System Authentication

For the enhanced system security, the OLT provides two authentication methods to access the switch such as Remote Authentication Dial-In User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+).

4.2.1 Authentication Method

To set the system authentication method, use the following command.

Command	Mode	Description
login {**local** | **remote**} {**radius** | **tacacs** | **host** | **all**} {**enable** | **disable**}	Global	Sets a system authentication method. local: console access remote: telnet/SSH access radius: RADIUS authentication tacacs: TACACS+ authentication host: nominal system authentication (default) all: all types of the authentication
no login {**local** | **remote**} {**radius** | **tacacs** | **host** | **all**}		Deletes a configured system authentication method.
no login		

4.2.2 Authentication Interface

If more than 2 interfaces exist in the OLT, you can set one interface to access RADIUS or TACACS server.

To set an authentication interface, use the following command.

Command	Mode	Description
login {**radius** | **tacacs**} **interface** *INTERFACE* [*A.B.C.D*]	Global	Sets an authentication interface. radius: RADIUS authentication tacacs: TACACS+ authentication INTERFACE: interface name A.B.C.D: source IP address (optional)
no login {**radius** | **tacacs**} **interface**		Deletes a specified authentication interface.

4.2.3 Primary Authentication Method

You can set the order of the authentication method by giving the priority to each authentication method.

To set the primary authentication method, use the following command

Command	Mode	Description
login {**local** | **remote**} {**radius** | **tacacs** | **host**} **primary**	Global	Sets a system authentication method. local: console access remote: telnet/SSH access radius: RADIUS authentication tacacs: TACACS+ authentication host: nominal system authentication (default)

4.2.4 RADIUS Server

4.2.4.1 RADIUS Server for System Authentication

To add/delete a RADIUS server for system authentication, use the following command.

Command	Mode	Description
login radius server *A.B.C.D KEY* [**auth_port** *PORT* **acct_port** *PORT*]	Global	Adds a RADIUS server with its information. A.B.C.D: IP address X:X::X:X: IPv6 address KEY: authentication key value auth_port: authentication port (optional) acct_port: accounting port (optional)
login radius server *X :X ::X :X KEY* [**auth_port** *PORT* **acct_port** *PORT*]		
no login radius server [*A.B.C.D*]		Deletes an added RADIUS server.
no login radius server [*X:X::X:X*]		

i You can add up to 5 RADIUS servers.

4.2.4.2 RADIUS Server Priority

To specify the priority of a registered RADIUS server, use the following command.

Command	Mode	Description
login radius server move *A.B.C.D* <1-5>	Global	Specifies a priority of RADIUS server. A.B.C.D: IP address 1-5: priority of RADIUS server

4.2.4.3 Timeout of Authentication Request

After an authentication request, the OLT waits for a response from a RADIUS server for specified time.

To specify a timeout value, use the following command.

Command	Mode	Description
login radius timeout <1-100>	Global	Specifies a timeout value. 1-100: timeout value for a response (default: 5)
no login radius timeout		Deletes a specified timeout value.

4.2.4.4 Frequency of Retransmit

In case of no response from a RADIUS server, the OLT is supposed to retransmit an authentication request. To set the frequency of retransmitting an authentication request, use the following command.

Command	Mode	Description
login radius retransmit <1-10>	Global	Sets the frequency of retransmit. 1-10: frequency count (default: 3)
no login radius retransmit		Deletes a specified frequency count.

4.2.5 TACACS+ Server

4.2.5.1 TACACS+ Server for System Authentication

To add/delete the TACACS+ server for system authentication, use the following command.

Command	Mode	Description
login tacacs server *A.B.C.D KEY*	Global	Adds a TACACS+ server with its information. A.B.C.D: IP address KEY: authentication key value
no login tacacs server [*A.B.C.D*]		Deletes an added TACACS+ server. A.B.C.D: IP address

i You can add up to 5 TACACS+ servers.

4.2.5.2 TACACS+ Server Priority

To specify the priority of a registered TACACS+ server, use the following command.

Command	Mode	Description
login tacacs server move *A.B.C.D* <1-5>	Global	Specifies the priority of TACACS+ server. A.B.C.D: IP address 1-5: priority of TACACS server

4.2.5.3 Timeout of Authentication Request

After the authentication request, the OLT waits for the response from the TACACS+ server for specified time. To specify a timeout value, use the following command.

Command	Mode	Description
login tacacs timeout <1-100>	Global	Specifies a timeout value. 1-100: timeout value for the response (default: 5)
no login tacacs timeout		Deletes a specified timeout value.

4.2.5.4 Additional TACACS+ Configuration

The OLT provides several additional options to configure the system authentication via TACACS+ server.

TCP Port for the Authentication

To specify TCP port for the system authentication, use the following command.

Command	Mode	Description
login tacacs socket-port <1-65535>	Global	Specifies TCP port for the authentication. 1-65535: TCP port
no login tacacs socket-port		Deletes a specified TCP port for the authentication.

Authentication Type

To select the authentication type for TACACS+, use the following command.

Command	Mode	Description
login tacacs auth-type {**ascii** | **pap** | **chap**}	Global	Selects an authentication type for TACACS+. ascii: plain text pap: password authentication protocol chap: challenge handshake authentication protocol
no login tacacs auth-type		Deletes a specified authentication type.

Priority Level

According to a defined priority level, the user has different authority to access the system. This priority should be defined in the TACACS+ server in the same way. To define the priority level of user, use the following command.

Command	Mode	Description
login tacacs priority-level {**min** | **user** | **max** | **root**}	Global	Defines the priority level of user, see the below information for the order of priority.
no login tacacs priority-level		Deletes a defined priority level.

i The order of priority is **root** = **max** > **user** > **min**.

4.2.6 Accounting Mode

The OLT provides the accounting function of AAA (Authentication, Authorization, and Accounting). Accounting is the process of measuring the resources a user has consumed. Typically, accounting measures the amount of system time a user has used or the amount of data a user has sent and received.

To set an accounting mode, use the following command.

Command	Mode	Description
login accounting-mode {**none** | **start** | **stop** | **both**}	Global	Sets an accounting mode. start: measures start point only. stop: measures stop point only. both: measures start and stop point both.
no login accounting-mode		Deletes a configured accounting mode.

4.2.7 Displaying System Authentication

To display a configured system authentication, use the following command.

Command	Mode	Description
show login	Enable Global Bridge	Shows a configured system authentication.

4.3 Configuring Interface

The Layer 2 switches only see the MAC address in an incoming packet to determine where the packet needs to come from/to and which ports should receive the packet. The Layer 2 switches do not need IP addresses to transmit packets. However, if you want to access to the OLT from a remote place with TCP/IP through SNMP or telnet, it requires an IP address.

You can enable the interface to communicate with another network device on the network.

4.3.1 Enabling Interface

To assign an IP address to an interface, you need to enable the interface first. If the interface is not enabled, you cannot access it from a remote place, even though an IP address has been assigned.

To configure an interface, you need to open *Interface Configuration* mode first. To open *Interface Configuration* mode, use the following command.

Command	Mode	Description
interface *INTERFACE*	Global Interface	Opens *Interface Configuration* mode to configure a specified interface.

To enable/disable an interface, use the following command.

Command	Mode	Description
no shutdown	Interface	Enables an interface.
shutdown		Disables an interface.

The following is an example of enabling the interface 1.

```
SWITCH# configure terminal
SWITCH(config)# interface 1
SWITCH(config-if)# no shutdown
SWITCH(config-if)#
```

i To display if an interface is enabled, use the **show running-config** command.

4.3.2 Assigning IP Address to Network Interface

After enabling an interface, assign an IP address. To assign an IP address to a network interface, use the following command.

Command	Mode	Description
ip address *A.B.C.D/M*	Interface	Assigns a primary IP address to an interface.

ip address *A.B.C.D/M* **secondary**		Assigns a secondary IP address to an interface.
ip address dhcp		Assigns an IP address from a DHCP server.
no ip address [*A.B.C.D/M*]		Clears an IP address assigned to an interface.
no ip address *A.B.C.D/M* **secondary**		Clears a secondary IP address assigned to an interface.
no ip address dhcp		Stops assigning an IP address from a DHCP server.

i

The **ip address dhcp** command is for configuring an interface as a DHCP client. For the detail of configuring a DHCP client, see Section 8.5.9.

To display an assigned IP address, use the following command.

Command	Mode	Description
show ip	Interface	Shows an IP address assigned to an interface.

4.3.3 Static Route and Default Gateway

The static route is a predefined route to a specific network and/or device such as a host. Unlike a dynamic routing protocol, *static routes* are not automatically updated and must be manually reconfigured if the network topology changes. Static route includes destination address, neighbor address, and etc. To configure a static route, use the following command.

Command	Mode	Description
ip route *A.B.C.D SUBNET-MASK* {*GATEWAY* | **null** | *INTERFACE*} [<1-255>]	Global	Configures a static route. A.B.C.D: destination IP prefix A.B.C.D/M: destination IP prefix with mask GATEWAY: gateway address INTERFACE: IP gateway interface name 1-255: distance value for this route src: binding source IP address
ip route *A.B.C.D/M* {*GATEWAY* | **null** | *INTERFACE*} [<1-255> | **src** *A.B.C.D*]		

To delete a configured static route, use the following command.

Command	Mode	Description
no ip route *A.B.C.D SUBNET-MASK* {*GATEWAY* | **null**} [<1-255>]	Global	Deletes a configured static route.
no ip route *A.B.C.D/M* {*GATEWAY* | **null** | *INTERFACE*} [<1-255>]		

To configure a default gateway, use the following command.

Command	Mode	Description

ip route default {*GATEWAY* | **null**} [<1-255>]	Global	Configures a default gateway.

To delete a configure default gateway, use the following command.

Command	Mode	Description
no ip route default {*GATEWAY* | **null**} [<1-255>]	Global	Deletes a default gateway.

To display a configured static route, use the following command.

Command	Mode	Description
show ip route [**database**]	Enable Global Bridge	Shows all IP routing table
show ip route [**connected** | **kernel** | **static** | *A.B.C.D* | *A.B.C.D/M* | **summary**]		Shows configured routing information.
show ip route database [**connected** | **kernel** | **static**]		Shows configured routing information with IP routing table database.

To clear IPv4 stale kernel routes form FIB, use the following command.

Command	Mode	Description
clear ip route [**kernel**]	Enable Global Bridge	Clears IPv4 stale routes.

4.3.4 Interface Description

To specify a description on an interface, use the following command.

Command	Mode	Description
description *LINE*	Interface	Specifies a description on an interface. LINE: 80-character text that describes the interface.
no description		Deletes a specified description.

The following is the example of specifying a description on the interface **1**.

```
SWITCH(config)# interface 1
SWITCH(config-if)# description sample_description
SWITCH(config-if)# show interface 1
Interface default
  Hardware is Ethernet, address is 00d0.cb00.0d83
  Description: sample_description
  index 43 metric 1 mtu 1500  <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  Bandwidth 100m
  inet 10.27.41.91/24 broadcast 10.27.41.255
```

```
    input packets 3208070, bytes 198412141, dropped 203750, multicast packets 0
    input errors 12, length 0, overrun 0, CRC 0, frame 0, fifo 12, missed 0
    output packets 11444, bytes 4192789, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0
SWITCH(config)#
```

4.3.5 Displaying Interface

To display an interface status and configuration, use the following command.

Command	Mode	Description
show interface [*INTERFACE*]	Enable Global Bridge Interface	Shows an interface status and configuration. INTERFACE: interface name
show ip interface {*INTERFACE* | **brief**}	Enable Global Bridge	Shows brief information of interface. INTERFACE: interface name

The following is the sample output of the **show ip interface brief** command.

```
SWITCH(config)# show ip interface brief
Interface            IP-Address      Status              Protocol
lo                   unassigned      up                  up
mgmt                 10.27.41.91     up                  up
default              unassigned      up                  up
SWITCH(config)#
```

4.3.6 Interface Identifier

To specify a identifier on an interface, use the following command.

Command	Mode	Description
identifier hex *LINE*	Interface	Sets interface identifier. *LINE*: Interface identifier of max 8byte value (e.g. ffeac3c434f20a00)

4.3.7 Enabling Interface Overlapping

To enable/disable the IP address overlapping across multiple interfaces, use the following command.

Command	Mode	Description
ip overlap-interface	Global	Enables IP address overlapping. The IP addresses

		should have a different netmask
no overlap-interface		Disables IP address overlapping.

4.4 Assigning an IPv6 Address

IPv6 is designed as an evolutionary step from IPv4. IPv6 runs well on high performance networks like Gigabit Ethernet, ATM, and others, as well as low bandwidth networks.

The main changes from IPv4 to IPv6 are summarized as follows:

- **Expanded addressing capability and auto configuration mechanism**
  IPv6 128bits address size solves the problem of the limited address space of IPv4 and offers a deeper addressing hierarchy and simpler configuration.
- **Simplification of the header format**
  The IPv6 header has a fixed length of 40 bytes. It actually accommodates only an 8-byte header plus two 16-byte IP address (source and destination address). The packets can be handled faster with lower processing costs.
- **Improved support for extensions and options**
  With IPv6, the options are handled as Extension headers. Extension headers are optional and only inserted between the IPv6 header and the payload, if necessary. Forwarding IPv6 packets is much more efficient than IPv4.

IPv6 Header

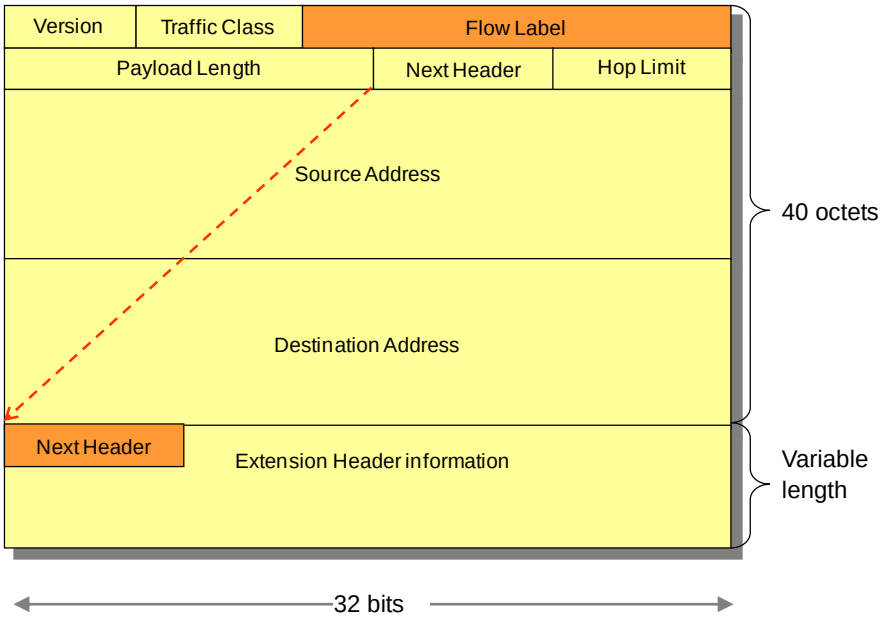


Fig. 4.1 Structure of IPv6 Header

Tab.4.1 provides an overview of the IPv6 header fields.

Field	Description
Version	Version of the protocol (4 Bits)
Priority	This field replaces the Type of Service field in IPv4. This field is used by sending nodes and forwarding routers to identify and distinguish between different classes or priorities of IPv6 packets. (1 Byte)
Flow label	This field distinguishes packets that require the same treatment, in order to facilitate the handling of real-time traffic. (20 Bits)
Payload Length	This field specifies the length of data carried after the IP header. Extension headers are considered part of the payload and are therefore included in the calculation. (2 Bytes)
Next Header	This field contains a protocol number or a value for an extension header. (1 Byte)
Hop limit	The value indicates a number of hops. Every forwarding node decrements the number by one. (1 Byte)
Source Address	This field contains the IP address of the originator of the packet.
Destination Address	This field contains the IP address of the intended recipient of the packet.

Tab. 4.1 Overview of IPv6 Header Fields

IPv6 Addressing

A typical IPv6 address consists of three parts-the global routing prefix, the subnet ID, and the interface ID. An IPv6 address has 128 bits, or 16 bytes. The address is divided into eight, 16-bit hexadecimal blocks, separated by colons.

```
FE80 : 0000 : 0000 : 0000 : 0202 : BA3FF : FE1E : 3210

FE80 : 0 : 0 : 0 : 202 : BA3FF : FE1E : 3210

FE80 :: 202 : BA3FF : FE1E : 3210
```

Some abbreviations are possible to make the IPv6 address easier. As above 3 examples are same IPv6 addresses. For instance, leading zeros in a 16-bit block can be omitted. Sequences of 16 bit blocks containing only zeros are replaced with two colons :: (not more than once per address).

IPv6 Prefix Notation

The prefix length specifies how many left-most bits of the address specify the prefix. The prefix is used to identify the subnet that an interface belongs to and is used by routers for forwarding.

IPv6 Address Types

IPv6 uses multicast addresses instead of the broadcast address. An IPv6 address can be classified into one of three categories, which Unicast, Multicast and Anycast address. The Anicast address, a new type of address introduced with RFC 1546, is now used with IPv6. An anycast address is assigned to multiple interfaces. A packet sent to an anycast address is delivered to only one of these interfaces, usually the nearest one.

IPv6 Special Addresses

There are some special addresses without prefix.

- **Unspecified address** : the unspecified address for IPv6

  `0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 (or ::)`

- **Localhost address** : the special address for the loopback interface.

  `0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0001 (or ::1)`

- **Link local address** : It is assigned automatically to an interface when IPv6 is enabled. The link local address is used only on local links for link communication purposes. These addresses typically begin with `fe80`.

- **Site local address** : These addresses typically begin with `fec0` and are used within a site. They are not for global use.

- **Multicasting addresses** : Multicast capability is formally added into the IPv6 protocol. The multicasting addresses begin with `ff0x`, where `x` is any hexadecimal number. An example of multicast address is `ff02::1`. This stands for all nodes of an address.

You can enable the interface to communicate with another network device on the network by assigning an IPv6 address

4.4.1 Enabling Interface

To assign an IP address to an interface, you need to enable the interface first. If the interface is not enabled, you cannot access it from a remote place, even though an IP address has been assigned.

To configure an interface, you need to open *Interface Configuration* mode first. To open *Interface Configuration* mode, use the following command.

Command	Mode	Description
interface *INTERFACE*	Global Interface	Opens *Interface Configuration* mode to configure a specified interface.

To enable/disable an interface, use the following command.

Command	Mode	Description

no shutdown	Interface	Enables an interface.
shutdown		Disables an interface.

4.4.2 Assigning IPv6 Address to Network Interface

After enabling an interface, assign an IPv6 global address. To assign an IPv6 address to a network interface, use the following command.

Command	Mode	Description
ipv6 address *X:X::X:X/M*	Interface	Assigns an IPv6 global address to an interface. X:X::X:X/M: IPv6 address/prefix-length
ipv6 address *X:X::X:X/M* **anycast**		Assigns an IPv6 anycast address to an interface.

To disable an assigned IPv6 address, use the following command.

Command	Mode	Description
no ipv6 address [*X:X::X:X/M*]	Interface	Clears an IP address assigned to an interface.

The IPv6 address is automatically learned and based upon the received Router Advertisement from its upstream service provider router.

To enable/disable automatic configuration of IPv6 addresses using stateless auto configuration on an interface, use the following command.

Command	Mode	Description
ipv6 address autoconfig	Interface	Enables automatic configuration of IPv6 addresses using stateless autoconfiguration.
no ipv6 address autoconfig		Disables automatic configuration of IPv6 addresses using stateless autoconfiguration.

To enable the interface to acquire an IPv6 address from the DHCPv6 server, use the following command.

Command	Mode	Description
ipv6 address dhcp [**rapid-commit**]	Interface	Acquires an IPv6 address on an interface from the DHCPv6 server. rapid-commit: allows the two-message exchange method for address allocation, the client includes the rapid-commit option in a solicit message if it is enabled
no ipv6 address dhcp		Removes the IPv6 address from the interface.

To configure dynamic IPv6 address allocation to a network interface, use the following command.

Command	Mode	Description
ipv6 address *PREFIX X:X::X:X/M*	Interface	Configures IPv6 address which is dynamically changeable according to the prefix name. PREFIX: prefix name X:X::X:X/M : IPv6 prefix of sub host.
no ipv6 address *PREFIX X:X::X:X/M*		Disables a dynamic IPv6 address allocation using the prefix name and sub-host address.

4.4.3 Assigning Link Local Address to Network Interface

The link-lcal address used between directly connected nodes on a single network link. To assign an IPv6 link-local address to a network interface, use the following command.

Command	Mode	Description
ipv6 address link-local *X:X::X:X*	Interface	Assigns a link-local address on the interface. X:X::X:X: IPv6 address using MAC address according to its EUI-64 format

To disable an assigned IPv6 link-local address, use the following command.

Command	Mode	Description
no ipv6 address link-local	Interface	Clears a link-local address assigned to an interface.

To display an assigned link-local address, use the following command.

Command	Mode	Description
show ipv6 interface [*IN-TERFACE*] **brief**	Enable Global Bridge	Shows a link-local address assigned to an interface.

4.4.4 Static Route and Default Gateway

The static route is a predefined route to a specific network and/or device such as a host.

Packets are transmitted to destination through static route. Static route includes destination address, neighbor router to receive packet, number of routes that packets have to go through. To configure a static route, use the following command.

Command	Mode	Description
ipv6 route *X:X::X:X/M* {*GATEWAY* | *INTERFACE*} [<1-255>]	Global	Configures a static route. X:X::X:X/M: destination IPv6 prefix GATEWAY: IPv6 gateway address INTERFACE: IPv6 gateway interface name or pseudo interface null 1-255: distance value for this prefix
ipv6 route *X:X::X:X/M INTERFACE* [<1-255>]		

To delete a configured static route, use the following command.

Command	Mode	Description
no ipv6 route *X:X::X:X/M* [{*GATEWAY* | *INTERFACE*}]	Global	Deletes a configured static route.
no ipv6 route *X:X::X:X/M GATEWAY INTERFACE*		

The following is an example of configuring a static route to reach three destinations, which are not directly connected.

```
SWITCH(config)# ipv6 route 4000::/16 br101
SWITCH(config)# ipv6 route 3000:3::/64 br103
SWITCH(config)# ipv6 route 3000:2::/64 br102
```

To display a configured static route, use the following command.

Command	Mode	Description
show ipv6 route [**connected** | **kernel** | **static** | *X:X::X:X* | *X:X::X:X/M* | **summary**]	Enable Global Bridge	Shows configured routing information.
show ipv6 route database [**connected** | **kernel** | **static**]		Shows configured routing information with IP routing table database.

To remove all kernel IPv6 route caches, use the following command.

Command	Mode	Description
clear ipv6 route kernel	Enable	Removes all kernel IPv6 route caches

4.4.5 Enabling IPv6 Processing

To enable/disable the IPv6 processing on an interface, use the following command.

Command	Mode	Description
ipv6 enable	Interface	Enables the IPv6 processing on an interface.
no ipv6 enable		Disables the IPv6 processing on an interface.

To enable/disable global IPV6 forwarding between all interfaces, use the following command.

Command	Mode	Description
ipv6 forwarding	Global	Enables global IPv6 packet forwarding function on the system. (Default)
no ipv6 forwarding		Disables global IPv6 packet forwarding function.

To display the status of global IPv6 forwarding, use the following command.

Command	Mode	Description
show ipv6 forwarding	Enable Global	Shows the IPv6 status of forwarding mode.

4.4.6 IPv6 Interface Mode

You can configure the interface for host mode. By default, the switch can receive Router Solicitation(RS) messages or send Router Advertisement (RA) messages to the network within this interface. In case of host mode, it functions as an IPv6 host. The interface can not send RA messages to other devices.

To specify the IPv6 interface mode on an interface, use the following command.

Command	Mode	Description
ipv6 mode host	Interface	Configures the interface for host mode. The interface can not send RA messages to the network.
no ipv6 mode host		Configures the interface for router mode. The interface receives RS messages and send RA messages to the network. (default)

4.4.7 Displaying Interface

To display an assigned IPv6 address, use the following command.

Command	Mode	Description
show ipv6	Interface	Shows the IPv6 addresses assigned to an interface.

To display an interface status and configuration, use the following command.

Command	Mode	Description
show ipv6 interface	Enable	Shows all configured interfaces and their

	Global Bridge	configurations.
show ipv6 interface *INTERFACE*		Shows the specified IPv6 interface information. INTERFACE: IPv6 interface name
show ipv6 interface *INTERFACE* **brief**		Shows a brief summary of IPv6 interface status and configuration.
show ipv6 interface brief		

4.5 Secure Shell (SSH)

Network security is getting more important because the access network has been generalized among numerous users. However, typical FTP and telnet service have big weakness for their security. Secure shell (SSH) is a network protocol that allows establishing a secure channel between a local and a remote computer. It uses public-key cryptography to authenticate the remote computer and to allow the remote computer to authenticate the user.

4.5.1 SSH Server

The OLT can be operated as SSH server. You can configure the switch as SSH server.

4.5.1.1 Enabling SSH Server

To enable/disable SSH server, use the following command.

Command	Mode	Description
service ssh	Global	Enables SSH server.
no service ssh		Disables SSH server.
show service	Enable/Global/Bridge	Shows the status of network connection services (telnet/ssh/ftp/tftp/snmp).

4.5.1.2 Displaying On-line SSH Client

To display SSH clients connected to SSH server, use the following command.

Command	Mode	Description
show ssh	Enable Global Bridge	Shows SSH clients connected to SSH server.

4.5.1.3 Disconnecting SSH Client

To disconnect an SSH client connected to SSH server, use the following command.

Command	Mode	Description
ssh disconnect *PID*	Global	Disconnects SSH clients connected to SSH server. PID: SSH client number

4.5.1.4 Assigning Specific Authentication Key

After enabling SSH server, each client will upload its own generated authentication key. The SSH server can assign the specific key among the uploaded keys from several clients.

To verify an authentication key, use the following command.

Command	Mode	Description
ssh key verify *FILENAME*	Global	Verifies a generated authentication key.

i If the SSH server verify the key for specific client, other clients must download the key file from SSH server to login.

4.5.1.5 Displaying Connection History of SSH Client

To display the connection history of SSH client, use the following command.

Command	Mode	Description
show ssh history	Enable Global Bridge	Shows the connection history of SSH clients who are connected to SSH server up to now.

4.5.2 SSH Client

4.5.2.1 Login to SSH Server

To login to SSH server after configuring the OLT as SSH client, use the following command.

Command	Mode	Description
ssh login *DESTINATION* [*PUBLIC-KEY*] [**vrf** NAME]	Enable	Logins to SSH server. DESTINATION: IP address of SSH server PUBLIC-KEY: public key NAME: VPN Routing/Forwarding instance name

4.5.2.2 Secured File Copy

To copy a system configuration file from/to SSH server, use the following command.

Command	Mode	Description
copy {**scp** | **sftp**} **config** {**download** | **upload**} *FILENAME*	Enable	Downloads and uploads a file to through SSH server. FILE: destination file name

4.5.2.3 Authentication Key

SSH client can access to server through authentication key after configuring authentication key and informing it to server. It is safer to use authentication key than inputting password every time for login, and it is possible to connect to several SSH servers with using one authentication key.

To configure an authentication key in the OLT, use the following command.

Command	Mode	Description

ssh keygen {**rsa1** | **rsa** | **dsa**}	Global	Configures an authentication key. rsa1: SSH ver. 1 authentication rsa: SSH ver. 2 authentication dsa: SSH ver. 2 authentication FILENAME: key file name
copy {**scp** | **sftp**} **key upload** *FILENAME*	Enable	

To configure authentication key and connect to SSH server with the authentication key, perform the following procedure:

Step 1 Configure the authentication key in the switch.

```
SWITCH_A(config)# ssh keygen dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/etc/.ssh/id_dsa):
Enter passphrase (empty for no passphrase):networks
Enter same passphrase again:networks
Your identification has been saved in /etc/.ssh/id_dsa.
Your public key has been saved in /etc/.ssh/id_dsa.pub.
The key fingerprint is:
d9:26:8e:3d:fa:06:31:95:f8:fe:f6:59:24:42:47:7e root@LD3016
SWITCH_A(config)#
```

Step 2 Copy the generated authentication key to SSH server.

Step 3 Connect to SSH server with the authentication key.

```
SWITCH_A(config)# ssh login 172.16.209.10
Enter passphrase for key '/etc/.ssh/id_dsa': networks
SWITCH_B#
```

4.6 802.1x Authentication

To enhance security and portability of network management, there are two ways of authentication based on MAC address and port-based authentication which restrict clients attempting to access to port.

Port-based authentication (802.1x) is used to authenticate the port self to access without users' count to access the network.

802.1x authentication adopts EAP (Extensible Authentication Protocol) structure. In EAP system, there are EAP-MD5 (Message Digest 5), EAP-TLS (Transport Level Security), EAP-SRP (Secure Remote Password), EAP-TTLS (Tunneled TLS) and the OLT supports EAP-MD5 and EAP-TLS. Accessing with user's ID and password, EAP-MD5 is 1-way Authentication based on the password. EAP-TLS accesses through the mutual authentication system of server authentication and personal authentication and it is possible to guarantee high security because of mutual authentication system.

At a request of user Authentication, from user's PC EAPOL-Start type of packets are transmitted to authenticator and authenticator again requests identification. After getting respond about identification, request to approve access to RADIUS server and be authenticated by checking access through user's information.

The following figure explains the process of 802.1x authentication.

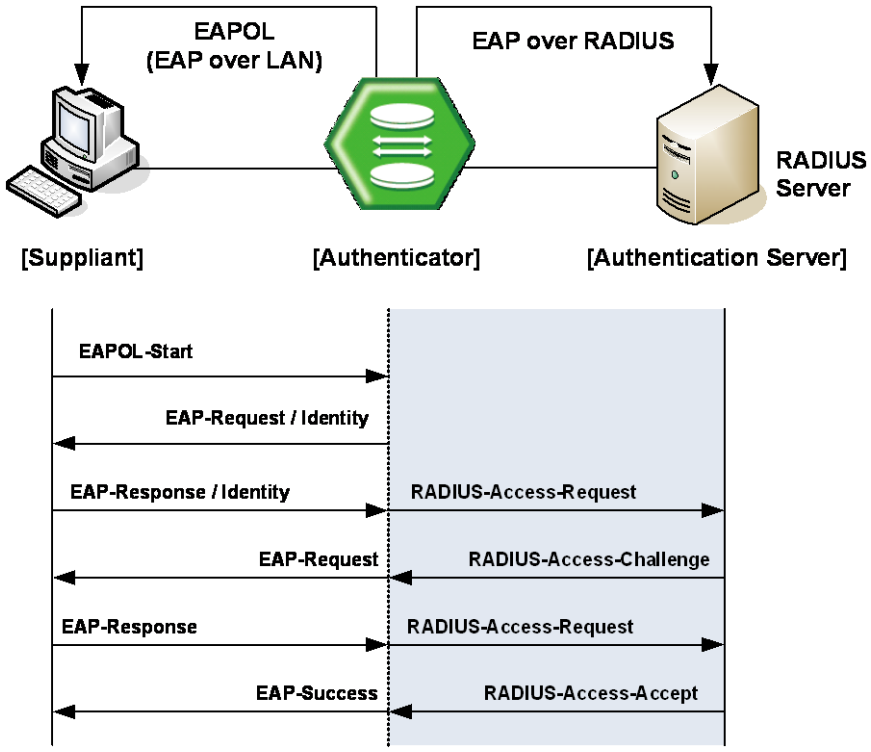


Fig. 4.2 Process of 802.1x Authentication

4.6.1 802.1x Authentication

4.6.1.1 Enabling 802.1x

To configure 802.1x, the user should enable 802.1x daemon first. To enable 802.1x daemon, use the following command.

Command	Mode	Description
dot1x system-auth-control	Global	Enables 802.1x daemon.
no dot1x system-auth-control		Disables 802.1x daemon.

4.6.1.2 RADIUS Server

As RADIUS server is registered in authenticator, authenticator also can be registered in RADIUS server.

Here, authenticator and RADIUS server need extra data authenticating each other besides they register each other's IP address. The data is key and should be the same value for each other. For the key value, every kinds of character can be used except the space or special character.

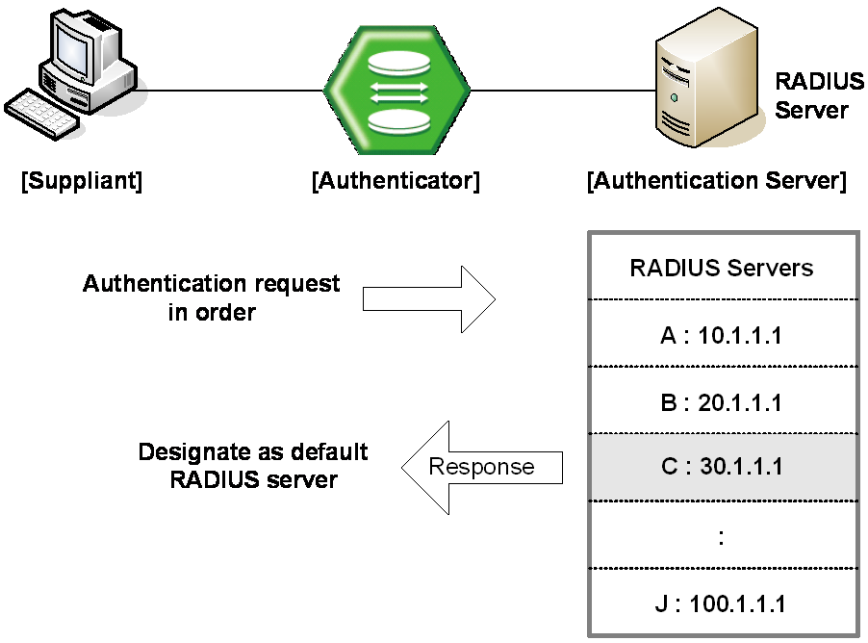


Fig. 4.3 Multiple Authentication Servers

If you register in several servers, the authentication server starts form RADIUS server registered as first one, then requests the second RADIUS server in case there's no response. According to the order of registering the authentication request, the authentication request is tried and the server which responds to it becomes the default server from the point of response time.

After default server is designated, all requests start from the RADIUS server. If there's no response from default server again, the authentication request is tried for RADIUS server designated as next one.

To configure IP address of RADIUS server and key value, use the following command.

Command	Mode	Description
dot1x radius-server host {*A.B.C.D* | *NAME*} **auth-port** <0-65535> **key** *KEY*	Global	Registers RADIUS server with key value and UDP port of radius server. 0-65535: UDP port (default: 1812)
dot1x radius-server host {*A.B.C.D* | *NAME*} **key** *KEY*		Configures IP address of RADIUS server and key value.
no dot1x radius-server host {*A.B.C.D* | *NAME*}		Deletes a registered RADIUS server.

i

You can designate up to five RADIUS servers as authentication server.

The **key** option is authentication information between the authenticator and RADIUS server. The authenticator and RADIUS server must have a same key value, and you can use alphabetic characters and numbers for the key value. The space or special character is not allowed.

To set priority to a registered RADIUS server, use the following command..

Command	Mode	Description
dot1x radius-server move {*A.B.C.D* | *NAME*} **priority** *PRIORITY*	Global	Sets priority to a registered RADIUS server.

4.6.1.3 Authentication Mode

You can set the authentication mode from the port-based to the MAC-based. To set the authentication mode, use the following command.

Command	Mode	Description
dot1x auth-mode mac-base *PORTS*	Global	Sets the authentication mode to the MAC-based.
no dot1x auth-mode mac-base *PORTS*		Restores the authentication mode to the port-based.

⚠

Before setting the authentication mode to the MAC-based, you need to set a MAC filtering policy to **deny** for all the Ethernet ports. To configure a MAC filtering policy, see Section 7.14.1.

4.6.1.4 Authentication Port

After configuring 802.1x authentication mode, you should select the authentication port.

Command	Mode	Description
dot1x nas-port *PORTS*	Global	Designates 802.1x authentication port.
no dot1x nas-port *PORTS*		Disables 802.1x authentication port.

4.6.1.5 Force Authorization

The OLT can permit the users requesting the access regardless of the authentication from RADIUS server. For example, even though a client is authenticated from the server, it is possible to configure not to be authenticated from the server.

To manage the approval for the designated port, use the following command.

Command	Mode	Description
dot1x port-control {**auto** | **force-authorized** | **force-unauthorized**} *PORTS*	Global	Configures a state of the authentication port. auto: authorization up to RADIUS server (default) force-authorized: force authorization force-unauthorized: force unauthorization
no dot1x port-control *PORTS*		Deletes a configured authentication port state.

4.6.1.6 Interval for Retransmitting Request/Identity Packet

In the OLT, it is possible to specify how long the device waits for a client to send back a response/identity packet after the device has sent a request/identity packet. If the client does not send back a response/identity packet during this time, the device retransmits the request/identity packet.

To configure the number of seconds that the switch waits for a response to a request/identity packet, use the following command.

Command	Mode	Description
dot1x timeout tx-period <1-65535> *PORTS*	Global	Sets reattempt interval for requesting request/identity packet. 1-65535: retransmit interval (default: 30)
no dot1x timeout tx-period *PORTS*		Disables the interval for requesting identity.

4.6.1.7 Interval of Authentication

To configure a term of authentication, use the following command.

Command	Mode	Description
dot1x timeout auth-period <1-4294967295>	Global	Sets the period between authentication attempts.
no dot1x timeout auth-period		Deletes the period between authentication attempts.

4.6.1.8 Number of Requests to RADIUS Server

After 802.1x authentication configured as explained above and the user tries to connect with the port, the process of authentication is progressed among user's PC and the equipment as authenticator and RADIUS server. It is possible to configure how many times the device which will be authenticator requests for authentication to RADIUS server.

To configure times of authentication request in the OLT, use the following command.

Command	Mode	Description
dot1x radius-server retries <1-10>	Global	Configure times of authentication request to RADIUS server. 1-10: retry number (default: 3)

4.6.1.9 Interval of Request to RADIUS Server

For the OLT, it is possible to set the time for the retransmission of packets to check RADIUS server. If there is a response from other packets, the switch waits for a response from RADIUS server during the configured time before resending the request.

Command	Mode	Description
dot1x radius-server timeout <1-120>	Global	Configures the interval of request to RADIUS server. 1-120: interval (default: 1)

You should consider the distance from the server for configuring the interval of requesting the authentication to RADIUS server. If you configure the interval too short, the authentication could not be realized. If it happens, you had better to reconfigure the interval longer.

4.6.2 802.1x Re-Authentication

In the OLT, it is possible to update the authentication status on the port periodically. To enable re-authentication on the port, you should perform the below procedure:

Step 1 Enable 802.1x re-authentication.

Step 2 Configure the interval of re-authentication.

Step 3 Configure the interval of requesting re-authentication in case of re-authentication fails.

Step 4 Execute 802.1x re-authenticating regardless of the interval.

4.6.2.1 Enabling 802.1x Re-Authentication

To enable 802.1x re-authentication using the following command.

Command	Mode	Description
dot1x reauth-enable *PORTS*	Global	Enables 802.1x re-authentication.
no dot1x reauth-enable *PORTS*		Disables 802.1x re-authentication.

4.6.2.2 Interval of Re-Authentication

RAIDIUS server contains the database about the user who has access right. The database is real-time upgraded so it is possible for user to lose the access right by updated database even though he is once authenticated. In this case, even though the user is accessible to network, he should be authenticated once again so that the changed database is applied to. Besides, because of various reasons for managing RADIUS server and 802.1x authentication port, the user is supposed to be re-authenticated every regular time. The administrator of the OLT can configure a term of re-authentication.

To configure a term of re-authentication, use the following command.

Command	Mode	Description
dot1x timeout reauth-period <1-4294967295> *PORTS*	Global	Sets the period between re-authentication attempts.
no dot1x timeout reauth-period *PORTS*		Deletes the period between re-authentication attempts.

4.6.2.3 Interval of Requesting Re-Authentication

When the authenticator sends request/identity packet for re-authentication and no response is received from the suppliant for the number of seconds, the authenticator retransmits the request to the suppliant. In the OLT, you can set the number of seconds that the authenticator should wait for a response to request/identity packet from the suppliant before retransmitting the request.

To set reattempt interval for requesting request/identity packet, use the following command.

Command	Mode	Description
dot1x timeout quiet-period <1-65535> *PORTS*	Global	Sets reattempt interval for requesting request/identity packet. 1-65535: reattempt interval (default: 30)
no dot1x timeout quiet-period *PORTS*		Disables the interval for requesting identity.

4.6.2.4 802.1x Re-Authentication

In Section 4.6.2.2, it is described even though the user is accessible to network, he should be authenticated so that the changed database is applied to.

Besides, because of various reasons managing RADIUS server and 802.1x authentication port, the user is supposed to be re-authenticated every regular time.

However, there are some cases of implementing re-authentication immediately. In the OLT, it is possible to implement re-authentication immediately regardless of configured time interval.

Command	Mode	Description
dot1x reauthenticate *PORTS*	Global	Performs re-authentication regardless of the configured

		time interval.

4.6.3 Initializing Authentication Status

The user can initialize the entire configuration on the port. Once the port is initialized, the supplicants accessing to the port should be re-authenticated.

Command	Mode	Description
dot1x initialize *PORTS*	Global	Initializes the authentication status on the port.

4.6.4 Restoring Default Value

To restore the default value of the 802.1x configuration, use the following command.

Command	Mode	Description
dot1x default *PORTS*	Global	Restores the default value of the 802.1x configuration.

4.6.5 Displaying 802.1x Configuration

To display 802.1x configuration, use the following command.

Command	Mode	Description
show dot1x	Enable Global Bridge	Shows 802.1x configuration on the system.
show dot1x *PORTS*		Shows 802.1x configuration on the port.

4.6.6 802.1x User Authentication Statistics

It is possible for user to make reset state by showing and deleting the statistics of 802.1x user authentication.

To display the statistics about the process of 802.1x user authentication, use the following command.

Command	Mode	Description
show dot1x statistics *PORTS*	Enable Global Bridge	Shows the statistics of 802.1x user authentication on the port.

To make reset state by deleting the statistics of 802.1x user authentication, use the following command.

Command	Mode	Description
dot1x clear statistics *PORTS*	Global	Makes reset state by deleting the statistics of 802.1x on the port.

4.6.7 Sample Configuration

The following is the example of configuring the port 6 with the port-based authentication specifying the information of RADIUS server.

```
SWTICH(config)# dot1x system-auth-control
SWTICH(config)# dot1x nas-port 6
SWTICH(config)# dot1x port-control force-authorized 6
SWTICH(config)# dot1x radius-server host 10.1.1.1 auth-port 1812 key test
SWTICH(config)# show dot1x
802.1x authentication is enabled.
RADIUS Server TimeOut: 1(S)
RADIUS Server Retries: 3

RADIUS Server : 10.1.1.1 (Auth key : test)
-------------------------------
           |        1
   802.1x  |123456789012345678
-------------------------------
 PortEnable |.....p............
 PortAuthed |.....u............
  MacEnable |..................
  MacAuthed |..................
-------------------------------
p = port-based, m = mac-based, a = authenticated, u = unauthenticated
SWITCH(config)#
```

The following is the example of setting the interval of requesting reauthentication to 1000 sec and the interval of reauthentication to 1800 sec.

```
SWTICH(config)# dot1x timeout quiet-period 1000 6
SWTICH(config)# dot1x timeout reauth-period 1800 6
SWTICH(config)# dot1x reauth-enable 6
SWTICH(config)# show dot1x 6
Port 6
  SystemAuthControl  : Enabled
  ProtocolVersion    : 0
  PortControl        : Force-Authorized
  PortStatus         : Unauthorized
  ReauthEnabled      : True
  QuietPeriod        : 1000
  ReauthPeriod       : 1800
  TxPeriod           : 30
  PaeState           : INITIALIZE
SWITCH(config)#
```

5 Port Configuration

The OLT features highly flexible hardware configurations with multiple GPON and Gigabit Ethernet components. In this chapter, you can find the instructions for the basic port configuration such as auto-negotiation, flow control, transmit rate, etc. Please read the following instructions carefully before you configure a port in the OLT.

5.1 Ethernet Port Configuration

5.1.1 Enabling Ethernet Port

To enable/disable the Ethernet port, use the following command.

Command	Mode	Description
port {**enable** | **disable**} *PORTS*	Bridge	Enables/disables a port, enter a port number. (default: enable) PORTS: port number

The following is an example of disabling the Ethernet port 9.

```
SWITCH(bridge)# show port 9
-----------------------------------------------------------------------
NO      TYPE      PVID    STATUS        MODE        FLOWCTRL      INSTALLED
                        (ADMIN/OPER)               (ADMIN/OPER)
-----------------------------------------------------------------------
9   Ethernet      10     Up/Down  Auto/Full/0     Off/ Off        Y
SWITCH(bridge)# port disable 9
SWITCH(bridge)# show port 9
-----------------------------------------------------------------------
NO      TYPE      PVID    STATUS        MODE        FLOWCTRL      INSTALLED
                        (ADMIN/OPER)               (ADMIN/OPER)
-----------------------------------------------------------------------
9    Ethernet       1   Down/Down  Auto/Full/0     Off/ Off        Y
SWITCH(bridge)#
```

5.1.2 Auto-Negotiation

Auto-negotiation is a mechanism that takes control of the cable when a connection is established to a network device. Auto-negotiation detects the various modes that exist in the network device on the other end of the wire and advertises it own abilities to automatically configure the highest performance mode of interoperation. As a standard technology, this allows simple, automatic connection of devices that support a variety of modes from a variety of manufacturers.

To enable/disable the auto-negotiation on an Ethernet port, use the following command.

Command	Mode	Description
port nego *PORTS* {**on** | **off**}	Bridge	Enables/disables the auto-negotiation on a specified port, enter a port number. (default: on)

		PORTS: port number

You cannot enable this function on 1000Base-X optical interface.

5.1.3 Transmit Rate

To set the transmit rate of an Ethernet port, use the following command.

Command	Mode	Description
port speed *PORTS* {**10** | **100** | **1000** | **10000**}	Bridge	Sets the transmit rate of a specified port to 10/100/1000Mbps or 10Gbps. PORTS: port number

You cannot set transmit rate on 1000Base-X optical interface.

5.1.4 Duplex Mode

Ethernet operates in either half-duplex or full-duplex mode. In full-duplex mode, frames travel in both directions simultaneously over two channels on the same connection for an aggregate bandwidth of twice that of half-duplex mode. Full duplex networks are very efficient since data can be sent and received simultaneously.

To set the duplex mode on an Ethernet port, use the following command.

Command	Mode	Description
port duplex *PORTS* {**full** | **half**}	Bridge	Sets full-duplex or half-duplex mode on a specified port. PORTS: port number

5.1.5 Flow Control

In Ethernet networking, the flow control is the process of adjusting the flow of data from one network device to another to ensure that the receiving device can handle all of the incoming data. For this process, the receiving device normally sends a PAUSE frame to the sending device when its buffer is full. The sending device then stops sending data for a while. This is particularly important where the sending device is capable of sending data much faster than the receiving device can receive it.

To enable the flow control on an Ethernet port, use the following command.

Command	Mode	Description
port flow-control *PORTS* {**on** | **off**}	Bridge	Enables the flow control on a specified port. (default: off) PORTS: port number

5.1.6 Port Description

To specify a description of an Ethernet port, use the following command.

Command	Mode	Description
port description *PORTS DESCRIPTION*	Bridge	Specifies a description of an Ethernet port. (maximum number of characters is 100) PORTS: port number
no port description *PORTS*		Deletes a specified description of an Ethernet port.

5.1.7 Network Service Port

To change a service port number that is in use by a different network service, use the following command.

Command	Mode	Description
service port {**ftp** | **ftp-data** | **http** | **snmp** | **ssh** | **telnet** } <1-65535>	Global	Chages the default port number for FTP/FTP-data/http/snmp/SSH/Telnet service. 1-65535: port number (Default port number: FTP (21), FTP-data (20), SSH (22), Telnet (23))
no service port {**ftp**| **ftp-data** | **http** | **snmp** | **ssh** | **telnet** }		Deletes the configured service port number and returns to the default port number for network service.

5.1.8 L2 Port Bridge

The L2 port bridge feature allows the port to forward the packets that the outgoing interface in the MAC address entry is the same as the incoming interface where the packet arrived. If one port is enabled with L2 port bridge feature, it forwards the packets to its destination port when the MAC address is found in the L2 table. The switch can have multiple MAC addresses associated with the same port.

To enable/disable the L2 port bridge feature, use the following command.

Command	Mode	Description
port port-bridge enable *PORTS*	Bridge	Enables L2 port bridge feature on a port. PORTS: port number
port port-bridge disable *PORTS*		Disables L2 port bridge feature. (default)

To display the L2 port bridge feature, use the following command.

Command	Mode	Description
show port port-bridge status [*PORTS*]	Enable Global Bridge	Shows the L2 port bridge operation status.

5.1.9 Port Crossover

MDI/MDIX is a type of Ethernet port connection according to the IEEE 802.3 standard using twisted pair cabling. Uplink ports on hubs and switches use the same pin assignments that use pins 1 and 2 for transmit and 3 and 6 for receive. These ports are called Medium Dependent Interface (MDI) ports. Normal ports use the opposite pin assignment, i.e. pins 1 and 2 are used for receive and pins 3 ans 6 are used for transmit. Such ports are called MDIX (MDI-crossed) ports.

In case any downstream equipment directly connected with the TX port cannot support auto MDIX mode, you can specify the MDIX mode by CLI.

To specify MDIX mode on an Ethernet port, use the following command.

Command	Mode	Description
port mdix *PORTS* {**auto** | **normal** | **cross**}	Bridge	Specifies MDIX mode of port. auto: auto MDIX mode cross: crossover MDI mode normal: normal MDI mode

To display the port information, use the following command.

Command	Mode	Description
show port mdix [*PORTS*]	Enable Global Bridge	Shows MDI crossover state of port.

5.1.10 Traffic Statistics

5.1.10.1 Packet Statistics

To display the traffic statistics of an Ethernet port, use the following command.

Command	Mode	Description
show port statistics avg-pkt [*PORTS*]	Enable Global Bridge	Shows the traffic statistics of the average packet for a specified Ethernet port. PORTS: port number
show port statistics avg [*PORTS*]		
show port statistics avg-pps [*PORTS*]		Shows the traffic statistics per packet type for a specified Ethernet port.
show port statistics avg type [*PORTS*]		Shows the pps statistics per packet type for a specified Ethernet port.
show port statistics interface [*PORTS*]		Shows the interface MIB counters of a specified Ethernet port.
show port statistics rfc4293 [*PORTS*]		Shows the RFC4293 statistics for a specified port.
show port statistics rmon [*PORTS*]		Shows the RMON MIB counters of a specified Ethernet port.

To delete all collected statistics for an Ethernet port, use the following command.

Command	Mode	Description
clear port statistics {*PORTS* | **all**}	Enable Global Bridge	Deletes all collected statistics for an Ethernet port. PORTS: port number

5.1.10.2 CPU Statistics

To display the statistics of the traffic handled by CPU, use the following command.

Command	Mode	Description
show cpu statistics avg-pkt [*PORTS*]	Enable Global Bridge	Shows the statistics of the traffic handled by CPU per packet type.
show cpu statistics total [*PORTS*]		Shows the traffic statistics of the average packet handled by CPU.

To delete the collected statistics of the traffic handled by CPU, use the following command.

Command	Mode	Description
clear cpu statistics [*PORTS*]	Global Bridge	Deletes the collected statistics of the traffic handled by CPU.

The OLT can be configured to generate a syslog message when the number of the packets handled by CPU exceeds a specified value. This function allows system administrators to monitor the switch and network status more effectively.

To configure the switch to generate a syslog message according to the number of the packets handled by CPU, use the following command.

Command	Mode	Description
cpu statistics-limit {**unicast** | **multicast** | **broadcast**} *PORTS* <10-100>	Global	Generates a syslog message according to the specified number of the packets handled by CPU. This is configurable for each packet type and physical port. unicast | multicast | broadcast: packet type PORTS: port number 10-100: packet count (actual value: 1000-10000)

To disable the switch to generate a syslog message according to the number of the packets handled by CPU, use the following command.

Command	Mode	Description
no cpu statistics-limit {**unicast** | **multicast** | **broadcast**} {*PORTS* | **all**}	Enable Global	Disables the switch to generate a syslog message according to the number of the packets handled by CPU for each packet type. all: all physical ports

no cpu statistics-limit all {*PORTS* | **all**}		Disables the switch to generate a syslog message according to the number of the packets handled by CPU for all packet types.

To display a configured value to generate a syslog message according to the number of the packets handled by CPU, use the following command.

Command	Mode	Description
show cpu statistics-limit	Enable Global Bridge	Shows a configured value to generate a syslog message according to the number of the packets handled by CPU.

5.1.10.3 Protocol Statistics

To enables/disables the system to collect the statistics of the protocols, use the following command.

Command	Mode	Description
protocol statistics {**enable** | **disable**} [**arp** | **icmp** | **ip** | **tcp** | **udp**]	Global Bridge	Enables/disables the system to collect the statistics of the protocols. (ARP, ICMP, IP, TCP, UDP)

To display the statistics of the protocol, use the following command.

Command	Mode	Description
show protocol statistics avg-pkt [*PORTS*]	Enable Global Bridge	Shows the statistics of the protocol for average packets.
show protocol statistics total [*PORTS*]		Shows the traffic statistics of the protocol for total packets.

To delete the collected statistics of the protocol, use the following command.

Command	Mode	Description
clear protocol statistics [*PORTS*]	Global Bridge	Deletes the collected statistics of the protocol.

5.1.11 Port Information

To display the port information, use the following command.

Command	Mode	Description
show port [*PORTS*]	Enable Global Bridge	Shows a current port status, enter a port number. PORTS: port number
show port status [*PORTS*]		
show port description [*PORTS*]		Shows a specified port description, enter a port number.
show port module-info [*PORTS*]		Shows the information of SFP module (including

		threshold configuration).
show arp port *PORTS*		Shows the information of ARP port.

The **show port module-info** command is only valid for Ethernet optical port. In case of using the command on the PON interface, even if the interface is equipped with the PON module, the system shows the state as Uninstalled.

5.1.12 Port Debounce Timer

The OLT can be configured to enable the debounce timer for Ethernet ports by specifying a debounce time (in milliseconds) or disable the timer by specifying a debounce time of 0.

To enable/disable the debounce timer, use the following command.

Command	Mode	Description
port link-debounce-time *PORTS* <0-5000>	Bridge	Enables the debounce timer for the amount of time (1 to 5000) Disables the debounce timer if you specify 0 (ms) PORTS: port number 0-5000: time (ms)
no port link-debounce-time *PORTS*		Deletes the configured debounce timer.
show port link-debounce [*PORTS*]	Enable Global Bridge	Shows the configured port link-debounce time.

5.2 Port Mirroring

Port mirroring is the function of monitoring a designated port. Here, one port to monitor is called monitor port and a port to be monitored is called mirrored port. Traffic transmitted from mirrored port are copied and sent to monitor port so that user can monitor network traffic.

The following is a network structure to analyze the traffic by port mirroring. It analyzes traffic on the switch and network status by configuring Mirrored port and Monitor port connecting the computer, that the watch program is installed, to the port configured as Monitor port.

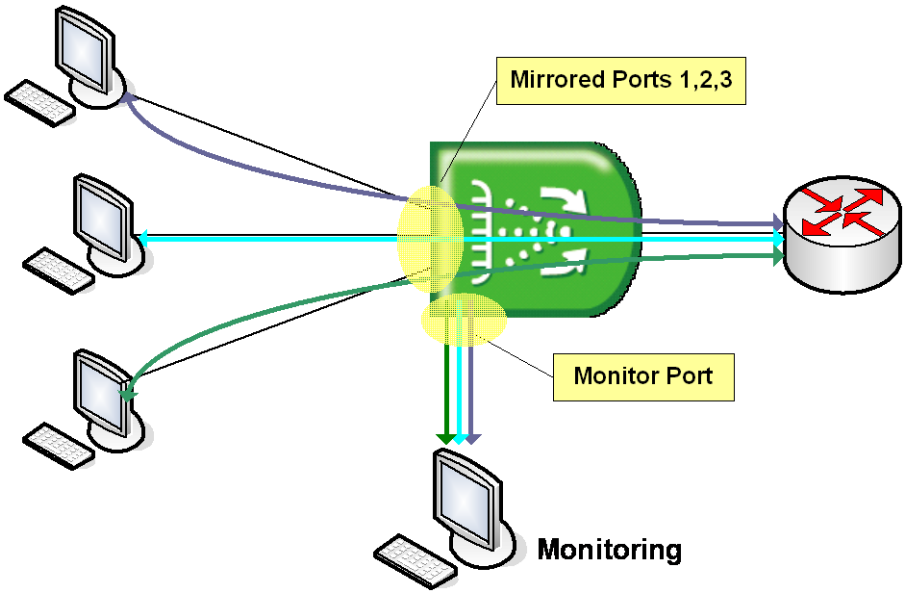


Fig. 5.1 Port Mirroring

To configure port mirroring, designate mirrored ports and monitor port. Then enable port mirroring function. Monitor port should be connected to the watch program installed PC. You can designate only one monitor port but many mirrored ports for one switch.

Step 1 Designate the monitor port, use the following command.

Command	Mode	Description
mirror monitor *PORTS* [**vlan** <2-4094>]	Bridge	Designates the monitor port. PORTS: port number 2-4094: vlan ID
mirror monitor cpu		

Step 2 Designate the mirrored ports, use the following command.

Command	Mode	Description
mirror add *PORTS* [**ingress** | **egress**]	Bridge	Designates the mirrored ports. PORTS: port number ingress: ingress traffic egress: egress traffic

Setting a mirror for VLAN allows you to monitor all traffic to the specified VLAN interface. To designate the mirrored VLAN ID, use the following command.

Command	Mode	Description
mirror add vlan *VLANS*	Bridge	Designates the mirrored VLAN. VLANS: VLAN ID

⚠ The OLT supports the VLAN mirroring function for the ingress traffic only.

Step 3 Activate the port mirroring, using the following command.

Command	Mode	Description
mirror enable	Bridge	Activates port mirroring.

Step 4 To display a configured port mirroring, use the following command.

Command	Mode	Description
show mirror	Enable Global Bridge	Shows a configured port mirroring.

To delete and modify the configuration, use the following command.

Command	Mode	Description
mirror disable	Bridge	Deactivates monitoring.
mirror del *PORTS* [**ingress** | **egress**]		Deletes a port from the mirrored ports.
mirror del vlan *VLANS*		Deletes the VLAN from the mirrored VLANs.

To disable monitoring function, use the following command.

Command	Mode	Description
no mirror monitor	Bridge	Disables port mirroring function.

The following is an example of enabling the port mirroring on the port 11 and 12 with the monitoring port 9.

```
SWITCH(bridge)# mirror enable
SWITCH(bridge)# mirror monitor 9
SWITCH(bridge)# mirror add 11
SWITCH(bridge)# mirror add 12
SWITCH(bridge)# show mirror
Mirroring enabled
 Monitor port = 9
```

```
  - Mirrored Ports
    ----------------------------------------
                          |         1
                          |123456789012345678
    ----------------------------------------
    Ingress Mirrored Ports|..........oo......
    Egress Mirrored Ports |... ......oo......


  - Mirrored VLANs
    ----------------
    NO   |   VID
    ----------------
SWITCH(bridge)#
```

6 System Environment

6.1 Environment Configuration

You can configure a system environment of the OLT.

6.1.1 Host Name

Host name displayed on prompt is necessary to distinguish each device connected to network. To set a new host name, use the following command.

Command	Mode	Description
hostname *NAME*	Global	Creates a host name of the switch, enter the name.
no hostname [*NAME*]		Deletes a configured host name, enter the name.

The following is an example of changing host name to *TEST*.

```
SWITCH(config)# hostname TEST
TEST(config)#
```

6.1.2 Time and Date

To set system time and date, use the following command.

Command	Mode	Description
clock *DATETIME*	Enable	Sets system time and date.
show clock	Enable Global Bridge	Shows system time and date.

The OLT can be configured to observe the daylight saving time in specified area. It means that whenever the system time is updated using a time server located in a different time area, it will be automatically corrected with the local daylight saving time offset.

To set daylight saving time, use the following command.

Command	Mode	Description
clock summer-time *TIMEZONE* **date** [*DATE MONTH YEAR HH:MM DATE MONTH YEAR HH:MM* <1-1440>]	Global	Adjusts the system time to daylight saving time during the specified time. 1-1440: daylight saving time offset (unit: minutes, default: Mar 10 2:00-Nov 10 2:00, offset : 60 minites)
clock summer-time *TIMEZONE* **recurring** [*WEEK DAY MONTH YEAR HH:MM WEEK DAY MONTH YEAR HH:MM* <1-1440>]		Configures daylight saving time during the period date for every year. 1-1440: daylight saving time offset

		(unit: minutes, default: Mar 10 2:00-Nov 10 2:00, offset : 60 minites)
no clock summer-time		Deletes the configured daylight saving time.

To display the configured daylight saving time, use the following command.

Command	Mode	Description
show clock summer-time	Enable Global	Shows the configured summer time.

The following example sets system time from 12:00, August 18, 2013 to 12:00, August 20, 2013.

```
SWITCH(config)# time-zone GMT+9
SWITCH(config)# clock summer-time GMT+9 date 18 8 2013 12:00 20 8 2013 12:00
60
SWITCH(config)# show clock summer-time

=============================================
Summer time is set. But not running.
---------------------------------------------
Summer time type : this year only
---------------------------------------------
Start time : 2013 aug 18 12:00
Stop  time : 2013 aug 20 12:00
=============================================
SWITCH(config)#
```

6.1.3 Time Zone

The OLT provides three kinds of time zone, GMT, UCT and UTC. The time zone of the switch is predefined as GMT (Greenwich Mean Time). You can also set the time zone where the network element belongs.

To set the time zone, use the following command.

Command	Mode	Description
time-zone *TIMEZONE*	Global	Sets the time zone (refer to the below table).
clear time-zone		Clears a configured time zone.

To display the world time zone, use the following command.

Command	Mode	Description
show time-zone	Enable Global Bridge	Shows the world time zone map.

Tab. 6.1 shows the world time zone.

Time Zone	Country/City	Time Zone	Country/City	Time Zone	Country/City
GMT-12	Eniwetok	**GMT-3**	Rio De Janeiro	**GMT+6**	Rangoon
GMT-11	Samoa	**GMT-2**	Maryland	**GMT+7**	Singapore
GMT-10	Hawaii, Honolulu	**GMT-1**	Azores	**GMT+8**	Hong Kong
GMT-9	Alaska	**GMT+0**	London, Lisbon	**GMT+9**	Seoul, Tokyo
GMT-8	LA, Seattle	**GMT+1**	Berlin, Rome	**GMT+10**	Sydney,
GMT-7	Denver	**GMT+2**	Cairo, Athens	**GMT+11**	Okhotsk
GMT-6	Chicago, Dallas	**GMT+3**	Moscow	**GMT+12**	Wellington
GMT-5	New York, Miami	**GMT+4**	Teheran	**-**	-
GMT-4	George Town	**GMT+5**	New Dehli	-	-

Tab. 6.1 World Time Zone

To see a configured time zone, use the **show clock** command.

6.1.4 Network Time Protocol (NTP)

The network time protocol (NTP) provides a mechanism to synchronize time on computers across an internet. The specification for NTP is defined in RFC 1119.

To enable/disable the NTP function, use the following command.

Command	Mode	Description
ntp *SERVER1* [*SERVER2*] [*SERVER3*]	Global	Enables NTP function with a specified NTP server. SERVER: server IP address (maximum 3 servers)
ntp *SERVER* {[**key** <1-4294967295>] **|** [**vrf** *VRFNAME*]}		Enables NTP function with the authentication key. 1-4294967295: key number
no ntp *SERVER1* [*SERVER2*] [*SERVER3*]		Deletes a specified NTP server. SERVER: server IP address
no ntp		Disables the NTP function.

To display a configured NTP, use the following command.

Command	Mode	Description
show ntp	Enable Global Bridge	Shows a configured NTP function.

The following is to register NTP server as 203.255.112.96 and enable it.

```
SWITCH(config)# ntp 203.255.112.96
```

```
SWITCH(config)# show ntp
==========================
 Ntpd is running.
==========================
 Time Servers
--------------------------
 1st : 203.255.112.96
--------------------------

Authentication is disabled.

==========================
SWITCH(config)#
```

To synchronize the system clock, the system periodically sends the NTP message to the NTP server. You can configure the system to bind the IP address to the message which allows the NTP server to recognize your system.

To bind the IP address to the NTP message, use the following command.

Command	Mode	Description
ntp bind-address *A.B.C.D*	Global	Specifies the IP address to be bound to the NTP message.
no ntp bind-address		Deletes a specified IP address.

6.1.5 Simple Network Time Protocol (SNTP)

NTP (Network Time Protocol) and SNTP (Simple Network Time Protocol) are the same TCP/IP protocol in that they use the same UDP time packet from the Ethernet Time Server message to compute accurate time. The basic difference in the two protocols is the algorithms being used by the client in the client/server relationship.

The NTP algorithm is much more complicated than the SNTP algorithm. NTP normally uses multiple time servers to verify the time and then controls the rate of adjustment or slew rate of the PC which provides a very high degree of accuracy. The algorithm determines if the values are accurate by identifying time server that doesn't agree with other time servers. It then speeds up or slows down the PC's drift rate so that the PC's time is always correct and there won't be any subsequent time jumps after the initial correction. Unlike NTP, SNTP usually uses just one Ethernet Time Server to calculate the time and then it "jumps" the system time to the calculated time. However, it can have back-up Ethernet Time Servers in case one is not available.

To configure the switch in SNTP, use the following commands.

Command	Mode	Description
sntp *SERVER1* [*SERVER2*] [*SERVER3*]	Global	Enables SNTP function with a specified SNTP server. SERVER: server IP address (maximum 3 servers)
no sntp *SERVER1* [*SERVER2*]		Deletes a specified SNTP server.

[*SERVER3*]		
no sntp		Disables SNTP function.

i You can configure up to 3 servers so that you use second and third servers as backup use in case the first server is down.

To display SNTP configuration, use the following command.

Command	Mode	Description
show sntp	Enable Global Bridge	Show SNTP configuration.

The following is to register SNTP server as 203.255.112.96 and enable it.

```
SWITCH(config)# sntp 203.255.112.96
SWITCH(config)# show sntp
==========================
 sntpd is running.
==========================
 Time Servers
--------------------------
 1st : 203.255.112.96
==========================
SWITCH(config)#
```

6.1.6 Terminal Configuration

By default, the OLT is configured to display 24 lines composed by 80 characters on console terminal. You can change the number of displaying lines by using the **terminal length** command. The maximum line displaying is 512 lines.

To set the number of the lines displaying on terminal screen, use the following command.

Command	Mode	Description
terminal length <0-512>	Enable	Sets the number of the lines displaying on a terminal screen, enter the value.
no terminal length		Restores a default line displaying.

6.1.7 Login Banner

It is possible to set system login and log-out banner. Administrator can leave a message to other users with this banner.

To set system login and log-out banner, use the following command.

Command	Mode	Description
banner	Global	Sets a banner before login the system.
banner login		Sets a banner when successfully log in the system.
banner login-fail		Sets a banner when failing to login the system.

To restore a default banner, use the following command.

Command	Mode	Description
no banner	Global	Restores a default banner.
no banner login		
no banner login-fail		

To display a current login banner, use the following command.

Command	Mode	Description
show banner	Enable Global Bridge	Shows a current login banner.

6.1.8 DNS Server

To set a DNS server, use the following command.

Command	Mode	Description
dns server *A.B.C.D*	Global	Sets a DNS server. A.B.C.D: DNS server IPv4 address X:X::X:X: DNS server IPv6 address
dns server *X:X::X:X*		
no dns server {*A.B.C.D* | *X:X::X:X*}		Removes a DNS server.

To display a configured DNS server, use the following command.

Command	Mode	Description
show dns	Enable/Global/Bridge	Shows a configured DNS server.

If a specific domain name is registered instead of IP address, user can do telnet, FTP, TFTP and ping to the hosts on the domain with domain name.

To search domain name, use the following command.

Command	Mode	Description
dns search *DOMAIN*	Global	Searches a domain name.
no dns search *DOMAIN*		Removes a domain name.

It is possible to delete DNS server and domain name at the same time with the below command.

Command	Mode	Description
no dns	Global	Deletes DNS server and domain name.

6.1.9 Fan Operation

For the OLT, it is possible to control fan operation. To control fan operation, use the following command.

Command	Mode	Description
fan operation {**on** | **off** | **auto**}	Global	Configures fan operation.

i

It is possible to configure to start and stop fan operation according to the system temperature. To configure this, see Section 6.1.13.3.

To display fan status and the temperature for fan operation, use the following command.

Command	Mode	Description
show status fan	Enable Global Bridge	Shows the fan status and the temperature for the fan operation.

6.1.10 Enabling FTP/TFTP Connection

To enable/disable the connection via FTP, use the following command.

Command	Mode	Description
service ftp	Global	Enables/ disables the connection via FTP.
no service ftp		

To enable/disable the connection via TFTP, use the following command.

Command	Mode	Description
service tftp	Global	Enables/ disables the connection via TFTP.
no service tftp		

To display the status of network connection services, use the following command.

Command	Mode	Description
show service	Enable/Global/Bridge	Shows the status of network connection services (telnet/ssh/ftp/tftp/snmp).

6.1.11 Disabling Daemon Operation

You can disable the daemon operation unnecessarily occupying CPU. To disable certain daemon operation, use the following command.

Command	Mode	Description
halt *PID*	Enable	Disables the daemon operation.

You can display the PID of each running processes with the **show process** command.

```
SWITCH# show process
USER     PID  %CPU  %MEM    VSZ   RSS  TTY   STAT  START  TIME  COMMAND
admin      1   0.2   0.2   1448   592  ?     S     Feb23  0:05  init [3]
admin      2   0.0   0.0      0     0  ?     S     Feb23  0:00  [keventd]
admin      3   0.0   0.0      0     0  ?     SN    Feb23  0:00  [ksoftirqd_CPU0]
admin      4   0.0   0.0      0     0  ?     S     Feb23  0:00  [kswapd]
admin      5   0.0   0.0      0     0  ?     S     Feb23  0:00  [bdflush]
admin      6   0.0   0.0      0     0  ?     S     Feb23  0:00  [kupdated]
admin      7   0.0   0.0      0     0  ?     S     Feb23  0:00  [mtdblockd]
admin      8   0.0   0.0      0     0  ?     S<    Feb23  0:00  [bcmDPC]
admin      9   0.0   0.0      0     0  ?     S<    Feb23  0:29  [bcmCNTR.0]
admin     16   0.0   0.0      0     0  ?     SN    Feb23  0:00  [jffs2_gcd_mtd0]
admin     81   0.0   2.0  10524  5492  ?     S     Feb23  0:53  /usr/sbin/swchd
admin     83   0.0   1.5   6756  3756  ?     S     Feb23  0:53  /usr/sbin/nsm

(Omitted)

SWITCH#
```

6.1.12 FTP Bind Address

When used as an FTP client, the OLT connects to an FTP server via the interface toward that server, which means the FTP client uses the IP address configured in that interface as a source IP address. However, an interface of the OLT may have multiple IP addresses. In such a multiple-IP environment, a primary IP address is normally used. You can configure the OLT to use one of the secondary IP addresses as a source IP of an FTP client.

To use a specific IP address as a source IP of an FTP client, use the following command.

Command	Mode	Description
ftp bind-address *A.B.C.D*	Global	Specifies a source IP address of an FTP client. A.B.C.D: one of the secondary IPv4 addresses configured in an interface X:X::X:X: one of the secondary IPv6 addresses configured in an interface
ftp bind-address *X:X::X:X*		
no ftp bind-address		Deletes a specified source IP address.

i This configuration is also applicable to a TFTP client.

6.1.13 System Threshold

You can configure the system with various kinds of the system threshold such as CPU load, traffic, temperature, etc. Using this threshold, the OLT generates syslog messages, sends SNMP traps, or performs a relevant procedure.

6.1.13.1 CPU Load

To set the threshold of CPU load, use the following command.

Command	Mode	Description
threshold cpu <21-100> {**5** | **60** | **600**} [<20-100> {**5** | **60** | **600**}]	Global	Sets the threshold of CPU load in the unit of percent (%). 21-100: CPU load high (default: 50) 20-100: CPU load low 5 | 60 | 600: time interval (unit: second)
no threshold cpu		Deletes the configured threshold of CPU load.

To display the configured threshold of CPU load, use the following command.

Command	Mode	Description
show cpuload	Enable Global Bridge	Shows the configured threshold and average of CPU load.
show cpu-trueload		Shows the CPU load during the last 10 minutes in the time slots of every 5 seconds.

6.1.13.2 Port Traffic

To set the threshold of port traffic, use the following command.

Command	Mode	Description
threshold port *PORTS THRESHOLD* {**5** | **60** | **600**} {**rx** | **tx**}	Global	Sets the threshold of port traffic. PORTS: port number THRESHOLD: threshold value (unit: kbps) 5 | 60 | 600: time interval (unit: second)
no threshold port *PORTS* {**rx** | **tx**}		Deletes the configured threshold of port traffic.

i The threshold of the port is set to the maximum rate of the port by default.

You can also set the blocking timer. When incoming traffic via a given port exceeds a configured threshold, the port will discard that traffic during a specified time.

To set the blocking timer, use the following command.

Command	Mode	Description
threshold port *PORTS* **block timer** <10-3600>	Global	Sets the blocking timer. PORTS: port number 10-3600: blocking time (unit: second)
no threshold port *PORTS* **block**		Disables the blocking timer

To display the configured threshold of port traffic, use the following command.

Command	Mode	Description
show port threshold	Enable Global Bridge	Shows the configured threshold of port traffic.

6.1.13.3 Fan Operation

The system fan will operate depending on measured system temperature. To set the threshold of fan operation, use the following command.

Command	Mode	Description
threshold fan *START-TEMP STOP-TEMP*	Global	Sets the threshold of fan operation in the unit of Celsius (°C). START-TEMP: starts fan operation. (default: 30) STOP-TEMP: stops fan operation. (default: 0)
no threshold fan		Deletes a configured threshold of fan operation.

When you set the threshold of fan operation, *START-TEMP* must be higher than *STOP-TEMP*.

To display the configured threshold of fan operation, use the following command.

Command	Mode	Description
show status fan	Enable/Global/Bridge	Shows the status and configured threshold of fan operation.

6.1.13.4 System Temperature

To set the threshold of system temperature, use the following command.

Command	Mode	Description
threshold temp *HIGH_VALUE LOW_VALUE*	Global	Sets the threshold of system temperature(°C). HIGH_VALUE: overload system temperature (-40 to 100°C, default: 80°C)

		LOW_VALUE: underload system temperature (-40 to 100°C, default: -20°C)
no threshold temp		Deletes a configured threshold of system temperature.

To display the configured threshold of system temperature, use the following command.

Command	Mode	Description
show status temp	Enable Global Bridge	Shows the status and configured threshold of system temperature.

6.1.13.5 System Memory

To set the threshold of system memory in use, use the following command.

Command	Mode	Description
threshold memory <20-100>	Global	Sets the threshold of system memory in the unit of percent (%). 20-100: system memory in use
no threshold memory		Deletes the configured threshold of system memory.

6.1.13.6 System/SFP Module Operation

The system/SFP module will operate depending on monitoring type of temperaturem, RX/TX power, voltage or Txbias.

To set the threshold of module, use the following command.

Command	Mode	Description
threshold module {**rxpower** | **txpower**} {**alarm** | **warning**} *PORTS* {*START-VALUE STOP-VALUE* | **operational**}	Global	Sets the Diagnostics threshold of SFP module by RX/TX power and monitors the module The range of RX/TX power: -40 to 8.1647 dBm
threshold module temper {**alarm** | **warning**} *PORTS* {*START-VALUE STOP-VALUE* | **operational**}		Sets the Diagnostics threshold of SFP module depending on temperature and monitors the module. The range of temperature: -128 to 127.99℃
threshold module txbias {**alarm** | **warning**} *PORTS* {*START-VALUE STOP-VALUE* | **operational**}		Sets the Diagnostics threshold of SFP module depending on txbias and monitors the module. The range of txbias: 0 ～ 131 mA
threshold module voltage {**alarm** | **warning**} *PORTS* {*START-VALUE STOP-VALUE* | **operational**}		Sets the Diagnostics threshold of SFP module depending on voltage and monitors the module. The range of voltage: 0 to 6.5535 V

To delete the threshold of module operation depending on specified monitoring type, use the following command.

Command	Mode	Description
no threshold module {**rxpower** | **voltage** | **txbias** | **txpower** | **temper**} {**alarm** | **warning**} *PORTS*	Global	Deletes the configured threshold of SFP module and restores the current threshold to a default value.

To display the configuration of SFP module of specific port, use the following command.

Command	Mode	Description
show port module-info [*PORTS*]	Enable Global Bridge	Shows the information of SFP module (including threshold configuration).

6.1.14 Enabling DMI Module

If you insert an SFP module including Diagnostic Monitoring Interface (DMI) into ports, you can see the real-time information about the ports such as transceiver type, length, connector type, and vendor information of the SFP. However, you might not want to see DMI polling information because it may result in CPU overload to collect DMI data via I^2C interface. To enable or disable collecting DMI information from SFP mouldes, use the following command.

Command	Mode	Description
module dmi {**enable** | **disable**}	Global	Specifies whether to collect DMI information from SFP modules.

This module DMI command is enabled by default. Thus, if you don't want to get DMI information, configure this setting as disable.

If disabled, the OLT does not show DMI information of the SFP ports when using the **show port module-info** command.

To display the configuration of DMI module, use the following command.

Command	Mode	Description
show module dmi	Enable Global Bridge	Displays the configuration result of DMI module.

To display the DMI-related information, use the following command.

Command	Mode	Description
show port module-info [*PORTS*]	Enable Global Bridge	Shows the information of SFP module (including threshold configuration).

6.1.15 Software Watchdog Configuration

The watchdog is responsible for bootstrapping OLT and starting the necessary set of server processes. You can configure the software watchdog to take an action for controlling the system of OLT.

To enable/disable the watchdog function, use the following command.

Command	Mode	Description
watchdog {**enable** | **disable**}	Global	Enable/disables the watchdog function.

To configure the software watchdog function, use the following command.

Command	Mode	Description
watchdog trigger-mode {**top-half | timer | thread**}	Global	Configures the watchdog trigger-mode.
watchdog timeout <15-120>		15-120: time (seconds)

To display the watchdog information, use the following command.

Command	Mode	Description
show watchdog	Enable Global Bridge	Shows the configured watchdog function.

i To know at what time the OLT watchdog is restarted, use the **show boot-info** command.

6.1.16 Auto USB-Restore

LD3008 and LD3016 supports auto USB-restore function providing to backup and restore configurations through USB interface. If you want to restore configurations automatically, you can only insert USB stick which should have files located in top directory. As soon as you insert the USB stick, it automatically restore them. However, you might not want to restore automatically because it may result in problems for security.

To configure auto USB-resore, use the following command.

Command	Mode	Description
auto usb-restore {**enable** | **disable**}	Global	Specifies whether to restore configurations from USB.

i This **auto usb-restore** command is disabled by default.

i System restart is required to complete the **auto usb-restore** command.

To display the configuration information of auto usb-restore, use the following command.

Command	Mode	Description
show auto usb-restore	Enable	Displays the information of USB restore feature.

6.2 Configuration Management

You can verify if the system configurations are correct and save them in the system.

6.2.1 Displaying System Configuration

To display the current running configuration of the system, use the following command.

Command	Mode	Description
show running-config	All	Shows a configuration of the system.
show running-config syslog		Shows syslog information.
show running-config {**admin-flow** | **admin-policy** | **arp** | **bridge** | **cpu-pkt-filter** | **dhcp** | **dhcp6** | **dns** | **flow** | **full** | **hostname** | **interface** [*INTERFACE*] | **interface tunel** <0-1023>| **login** | **nd** | **policer** | **policy** | **pppoe** | **qos** | **rmon-alarm** | **rmon-event** | **rmon-history** | **router vrrp** | **router ipv6 vrrp** | **snmp** | **syslog** | **time-out** | **time-zone**}		Shows a configuration of the system with the specific option.
show running-config {**dba-profile** [*NAME*] | **extended-vlan-tagging-operation** [*NAME*] | **gpon** | **gpon-node** | **gpon-olt** [*PORT*] | **multicast-access-list** [*NAME*] | **multicast-profile** [*NAME*] | **onu-profile** [*NAME*] | **pm-profile** [*NAME*] | **pw-maintenance-profile** [*NAME*] | **rate-limit-profile** [*NAME*] | **tdm-pw-profile** [*NAME*] | **traffic-profile** [*NAME*] | **voip-profile** [*NAME*] }		Shows the configurations of the system with the GPON option.

The following is an example to display the configuration of the syslog.

```
SWITCH# show running-config syslog
!
syslog output info local volatile
syslog output info console
syslog output debug local non-volatile
!
SWITCH#
```

6.2.2 Writing System Configuration

If you change the configuration of the system, you need to save the changes in the system flash memory. To write a current running configuration, use the following command.

Command	Mode	Description
write memory	All	Writes a current running configuration in the system flash memory.
write terminal	Enable	Shows a current running configuration on the terminal.

		(alias to the **show running-config** command)

When you use the **write memory** command, make sure there is no key input until **[OK]** message appears.

6.2.3 Auto-Saving

The OLT supports the auto-saving feature, allowing the system to save the system configuration automatically. This feature prevents the loss of unsaved system configuration by unexpected system failure.

To allow the system to save the system configuration automatically, use the following command.

Command	Mode	Description
write interval <10-1440>	Global	Enables auto-saving with a given interval as a multiple of 10. 10-1440: time interval (unit: minute)
no write interval		Disables auto-saving.

6.2.4 System Configuration File

To copy a system configuration file, use the following command.

Command	Mode	Description
copy running-config {*FILENAME* | **startup-config**}	Enable	Copies a running configuration file. FILENAME: configuration file name startup-config: startup configuration file
copy startup-config *FILENAME*		Copies a startup configuration file to a specified file name.
copy *FILENAME* **startup-config**		Copies a specified configuration file to the startup configuration file.
copy *FILENAME1 FILENAME2*		Copies a specified configuration file to another configuration file.

To back up a system configuration file using FTP or TFTP, use the following command.

Command	Mode	Description
copy {**ftp** | **tftp**} **config upload** {*FILE-NAME* | **startup-config**}	Enable	Uploads a file to FTP or TFTP server with the name configured by user.
copy {**ftp** | **tftp**} **config download** {*FILE-NAME* | **startup-config** }		Downloads a file from FTP or TFTP server with a name configured by user.
copy {**ftp** | **tftp**} **os upload** {**os1** | **os2**}		Uploads a file to ftp or FTP server with a name of os1 or os2.
copy {**ftp** | **tftp**} **os download** {**os1** | **os2**}		Downloads a file from FTP or TFTP server with a name of os1 or os2.

copy {**ftp** | **tftp**} **bootloader download**		Downloads a bootloader image file from FTP or TFTP server.
copy {**ftp** | **tftp**} **pld download**		Downloads a PLD image file from FTP or TFTP server.

i To access FTP to back up the configuration or use the backup file, you should know FTP user ID and the password. To back up the configuration or use the file through FTP, you can recognize the file transmission because hash function is automatically turned on.

To delete a system configuration file, use the following command.

Command	Mode	Description
erase config *FILENAME*	Enable Global	Deletes a specified configuration file. FILENAME: configuration file name
erase key *FILENAME*	Enable	Deletes a specified SSH key file. FILENAME: SSH key file name

To display a system configuration file, use the following command.

Command	Mode	Description
show startup-config	Enable Global Bridge	Shows a current startup configuration.
show config-list		Shows a list of configuration files.

The following is an example of displaying a list of configuration files.

```
SWITCH(config)# copy running-config LD3016
SWITCH(config)# show config-list
========================
        CONFIG-LIST
========================
  l3_default
  LD3016
SWITCH(config)#
```

6.2.5 Restoring Default Configuration

To restore a default configuration of the system, use the following command.

Command	Mode	Description
restore factory-defaults	Enable	Restores a factory default configuration.
restore layer2-defaults		Restores an L2 default configuration.
restore layer3-defaults		Restores an L3 default configuration.

i After restoring a default configuration, you need to restart the system to initiate.

6.2.6 Core Dump File

A core dump file contains the memory image of a particular process, or the memory images of parts of the address space of that process, along with other information such as the values of processor registers. The OLT can be configured to generate core dumps and save them in ramdisk for useful debugging aids in several situations such as accesses to non-existent memory, segmentation errors.

To configure a core dump, use the following command.

Command	Mode	Description
generate coredump *PID*	Enable Global Bridge	Generates a core dump file and save it with a name. PID: process ID
clear coredump *PID*		Deletes the specific core dump file.

To back up a core dump file using FTP or TFTP, use the following command.

Command	Mode	Description
copy {**ftp** | **tftp**} **coredump upload**	Enable	Uploads a core dump file to FTP or TFTP server.

To display a core dump file, use the following command.

Command	Mode	Description
show coredump [*NAME*]	Enable Global Bridge	Shows a current status of core dump file NAME: process name

6.3 System Management

When there is any problem in the system, you must find what the problem is and its solution. Therefore, you should not only be aware of a status of the system but also verify if the system is correctly configured.

6.3.1 Network Connection

To verify if your system is correctly connected to the network, use the **ping** command. For IP network, this command transmits a message to Internet Control Message Protocol (ICMP). ICMP is an internet protocol that notifies fault situation and provides information on the location where IP packet is received. When the ICMP echo message is received at the location, its replying message is returned to the place where it came from. To perform a ping test to verify network status, use the following command.

Command	Mode	Description
ping [*A.B.C.D*]	nable	Performs a ping test to verify network status.
ping ipv6 *X:X::X:X* [*INTERFACE*]		Performs a ping test to verify IPv6 network status.

The followings are the available options to perform the **ping** command.

Items	Description
Protocol [ip]	Supports ping test. The default is IP.
Target IP address	Sends ICMP echo message by inputting IP address or host name of destination in order to verify network status.
Repeat count [5]	Sends ICMP echo message as many as count. The default is 5.
Datagram size [100]	Ping packet size. The default is 100 bytes.
Timeout in seconds [2]	It is considered as successful ping test if reply returns within the configured time interval. The default is 2 seconds.
Extended commands [n]	Adds the additional options. The default is no.

Tab. 6.2 Options for Ping (Cont.)

The following is an example of ping test 5 times to verify network status with IP address 10.55.193.110.

```
SWITCH# ping
Protocol [ip]: ip
Target IP address: 10.55.193.110
Repeat count [5]: 5
Datagram size [100]: 100
Timeout in seconds [2]: 2
Extended commands [n]: n
PING 10.55.193.110 (10.55.193.110) 100(128) bytes of data.
108 bytes from 10.55.193.110: icmp_seq=1 ttl=255 time=0.058 ms
108 bytes from 10.55.193.110: icmp_seq=2 ttl=255 time=0.400 ms
108 bytes from 10.55.193.110: icmp_seq=3 ttl=255 time=0.403 ms
--- 10.55.193.110 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 8008ms
```

```
rtt min/avg/max/mdev = 0.058/0.581/1.632/0.542 ms
SWITCH#
```

When multiple IP addresses are assigned to the switch, sometimes you need to verify the connection status between the specific IP address and network status.

In this case, use the same process as ping test and then input the followings after extended commands. It is possible to verify the connection between specific IP address and network using the following command.

The following is the information to use ping test for multiple IP addresses.

Items	Description
Source address or interface	Designates the address where the relative device should respond in source IP address.
Type of service [0]:	The service filed of QoS (Quality Of Service) in Layer 3 application. It is possible to designate the priority for IP packet.
Data pattern [0xABCD]	Configures the data pattern to be used for pinging. Default is 0xABCD.

Tab. 6.2 Options for Ping for Multiple IP Addresses

The following is to verify network status between 10.45.239.203 and 10.55.193.110 when IP address of the switch is configured as 10.45.239.203.

```
SWITCH# ping
Protocol [ip]:ip
Target IP address: 10.55.193.110
Repeat count [5]: 5
Datagram size [100]: 100
Timeout in seconds [2]: 2
Extended commands [n]: y
Source address or interface: 10.45.239.203
Type of service [0]: 0
Data pattern [0xABCD]: 0xABCD
PATTERN: 0xabcd
PING 10.55.193.110 (10.55.193.110) from 10.45.239.203 : 100(128) bytes of data.
108 bytes from 10.55.193.110: icmp_seq=1 ttl=255 time=30.4 ms
108 bytes from 10.55.193.110: icmp_seq=2 ttl=255 time=11.9 ms
108 bytes from 10.55.193.110: icmp_seq=3 ttl=255 time=21.9 ms
108 bytes from 10.55.193.110: icmp_seq=4 ttl=255 time=11.9 ms
108 bytes from 10.55.193.110: icmp_seq=5 ttl=255 time=30.1 ms

--- 10.55.193.110 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 8050ms
rtt min/avg/max/mdev = 11.972/21.301/30.411/8.200 ms
SWITCH#
```

6.3.2 IP ICMP Source Routing

If you implement PING test to verify the status of network connection, ICMP request arrives at the final destination as the closest route according to the routing theory.

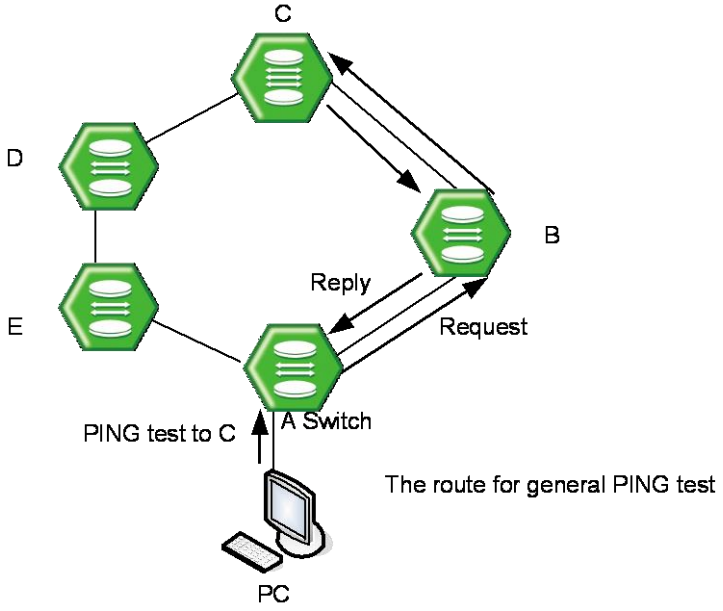


Fig. 6.1 Ping Test for Network Status

In Fig. 6.1, if you perform ping test from PC to C, it goes through the route of **A→B→C**. This is the general case. But, the OLT can enable to perform ping test from PC as the route of **A→E→D→C**.

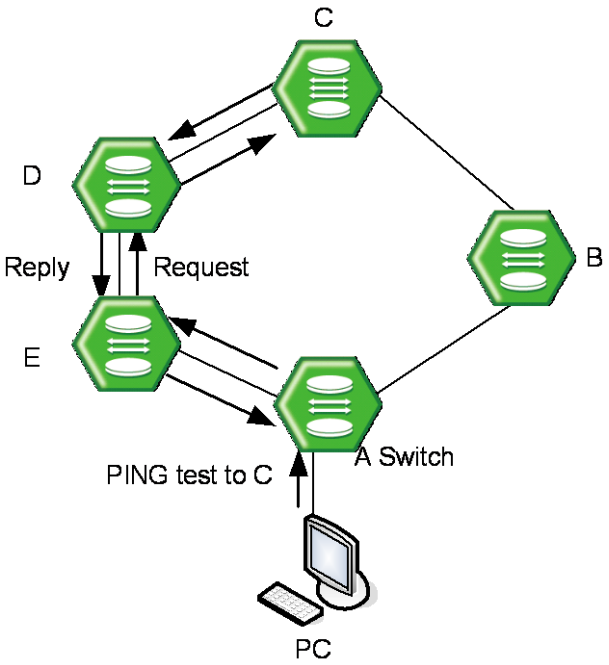


Fig. 6.2 IP Source Routing

To perform ping test as the route which the manager designated, use the following steps.

Step 1 Enable IP source-routing function from the equipment connected to PC which the PING test is going to be performed.

To enable/disable IP source-routing in the OLT, use the following command.

Command	Mode	Description
ip icmp source-route	Global	Enable IP source-routing function.
no ip icmp source-route		Disable IP source-routing function.

Step 2 Perform the ping test from PC as the designate route with the **ping** command.

6.3.3 Tracing Packet Route

You can discover the routes that packets will actually take when traveling to their destinations. To do this, the **traceroute** command sends probe datagrams and displays the round-trip time for each node.

If the timer goes off before a response comes in, an asterisk (*) is printed on the screen.

Command	Mode	Description
traceroute [*WORD*]	Enable	Traces packet routes through the network. WORD: destination IP address or host name A.B.C.D: destination IP address icmp: use ICMP Echo instead of UDP datagrams
traceroute ip *A.B.C.D*		
traceroute icmp *WORD*		

The followings are the configurable options to trace the routes.

Items	Description
Protocol [ip]	Supports ping test. Default is IP.
Target IP address	Sends ICMP echo message by inputting IP address or host name of destination in order to check network status with relative.
Source address	Source IP address which other side should make a response.
Numeric display [n]	Hop is displayed the number instead of indications or statistics.
Timeout in seconds [2]	It is considered as successful ping test if reply returns within the configured time interval. Default is 2 seconds.
Probe count [3]	Set the frequency of probing UDP packets.
Maximum time to live [30]	The TTL field is reduced by one on every hop. Set the time to trace hop transmission (The number of maximum hops). Default is 30 seconds.
Port Number [33434]	Selects general UDP port to be used for performing to trace the routes. The default is 33434.

Tab. 6.3 Options for Tracing Packet Route

The following is an example of tracing packet route sent to 10.55.193.104.

```
SWITCH# traceroute 10.55.193.104
traceroute to 10.55.193.104 (10.55.193.104), 30 hops max, 40 byte packets
 1  10.45.239.254 (10.45.239.254)  2.459 ms  1.956 ms  1.781 ms
 2  10.45.191.254 (10.45.191.254)  1.114 ms  2.112 ms  1.786 ms
 3  10.45.1.254 (10.45.1.254)  2.723 ms  2.604 ms  1.767 ms
 4  10.55.1.1 (10.55.1.1)  2.532 ms  2.522 ms  1.793 ms
 5  10.55.1.1 (10.55.1.1)  1.623 ms  0.879 ms  1.755 ms
 6  10.55.193.104 (10.55.193.104)  9.375 ms  3.817 ms  2.514 ms
SWITCH#
```

6.3.4 Displaying User Connecting to System

To display current users connecting to the system from a remote place or via console interface, use the following command.

Command	Mode	Description
where	Enable	Shows current users connecting to the system from a remote place or via console interface.

The following is an example of displaying current users connecting to the system.

```
SWITCH# where
admin at ttyp0 from 10.20.1.32:2196 for 30 minutes 35.56 seconds
admin at ttyS0 from console for 28 minutes 10.90 seconds
SWITCH#
```

6.3.5 MAC Table

To display MAC table recorded in specific port, use the following command.

Command	Mode	Description
show mac [*BRIDGE*]	Enable Global Bridge	Shows MAC table. BRIDGE: bridge name
show mac *BRIDGE PORTS*		

The following is an example of displaying a current MAC table.

```
SWITCH(config)# show mac
==========================================================================
 vid  port    mac addr            permission    status      in use
==========================================================================
 100   6     LD3016:00:17:05    OK           dynamic      0.42
 101   7     00:00:66:02:01:02    OK           dynamic      19.39
 101   8     00:00:65:01:02:01    OK           dynamic     115.65
SWITCH(config)#
```

6.3.6 System Running Time

To display the system running time, use the following command.

Command	Mode	Description
show uptime	Enable Global Bridge	Shows the system running time.

The following is an example of displaying the system running time.

```
SWITCH# show uptime
10:41am up 15 days, 10:55, 0 users, load average: 0.05, 0.07, 0.01
SWITCH#
```

6.3.7 System Information

To display the system information, use the following command.

Command	Mode	Description
show system	Enable Global Bridge	Shows the system information.

6.3.8 System Memory Information

To display a system memory status, use the following command.

Command	Mode	Description
show memory	Enable Global Bridge	Shows system memory information.
show memory { **dhcp** | **gpon-olt** | **imi** | **lib** | **nsm** | **pppoe** | **swch**}		Shows system memory information with a specific option.

6.3.9 System EDFA

To display the system information of edfa, use the following command.

Command	Mode	Description
show system edfa	Enable Global	Shows the information of erbium doped fiber amplifier system.

6.3.10 CPU Packet Management

6.3.10.1 CPU Packet Limit

If the CPU of the system processes too many packets during the operation, it may cause the performance decrease. To prevent the CPU overload, you can manually limit the number of the packets handled by CPU.

To limit the number of the packets handled by CPU, use the following command.

Command	Mode	Description
cpu packet limit <500-20000>	Global	Limits the number of RX packets of CPU. 500-20000: packets per second (default: 1500)
cpu packet limit <0-7> <500-20000>		Limits the number of RX packets per second based on queue number. 0-7: queue number 500-20000: packets per second (default: 1500)
no cpu packet limit <0-7>		Deletes the configured packet limit.

To display a configured CPU packet limit, use the following command.

Command	Mode	Description
show cpu packet limit	Enable Global	Shows a configured CPU packet limit.

6.3.10.2 CPU Packet Filtering

The OLT provides a packet filtering feature for incoming/outgoing traffic management to/from CPU. You have to create a CPU packet filter first and set the packet classification criteria and the policy. You can use physical port ID, 802.1p priority (CoS), VLAN ID, 802.1q tag, and so on to classify the CPU packets. After applying the CPU packet filter, it classifies the packets, and processes the traffic according to user-defined policies.

To open *CPU Packet Filtering Configuration* mode, use the following command.

Command	Mode	Description
cpu-pkt-filter*NAME*	Global	Creates a CPU packet filter. NAME: CPU packet filter name
no cpu-pkt-filter { *NAME* | **all** }		Deletes the configured CPU packet filter.

After entering CPU packet filtering mode, the prompt changes from SWITCH(config)# to SWITCH(cpu-flt[*NAME*])#.

i

After entering *CPU Packet Filtering Configuration* mode, the filtering parameters can be configured by user. The filter match, filter priority, filter action, stage and policy can be configured for each CPU packet filter.

To configure one or more CPU packet filter match pattern(s), use the following command.

Command	Mode	Description
match vid <1-4094> [**tag-position** <1-8>]	CPU-Filter	Classifies a VLAN ID. VLAN: VLAN ID
match cos <0-7>		Classifies a queue of CPU RX/TX packets. 0-7: queue number
match port *PORT*		Classifies a physical port ID. PORT: port ID
match 802dot1q tpid { - | *TPID* } **pcp** { - | <0-7> } **vid** { - | <1-4094> } [**tag-position** <1-8>]		Classifies an 802.1q tag. tpid: tag protocol ID TPID: tag protocol ID (ex: 8100) pcp: priority code point tag-position: VLAN tag position -: any
match offset <0-127> **data** *HEX* [{ **desc** *DESC* | **mask** *MASK* [**desc** *DESC*]}]		Classifies an offset. 0-127: begin position, max 127 bytes HEX: hex value (ex: ffaa, up to 16 bytes) MASK: hex value (ex: f0f0) DESC: description up to 16 bytes
match offset <0-127> **length** <1-16> **data** *HEX* [**mask** *MASK*]		
match ethertype { **ip** | **arp** | *ETHERTYPE*}		Classifies a protocol based VLAN Ethernet type. ETHERTYPE : selects Ethernet type (hex digit : 0806)
match protocol { **icmp** | **igmp** [**reportv2** | **reportv1** | **leave** | **query**]}		Classifies an IGMP/ICMP packet.
match protocol { **tcp** | **udp**} [{**srcport** *PORT* | **dstport** *PORT*}]		Classifies an TCP/UDP packet.

To delete the configured CPU packet filter match pattern(s), use the following command.

Command	Mode	Description
no match vid <1-4094> [**tag-position** <1-8>]	CPU-Filter	Deletes a specified packet-classifying pattern for each option.
no match cos <0-7>		
no match port *PORT*		
no match 802dot1q tpid { - | *TPID* } **pcp** { - | <0-7> } **vid** { - | <1-4094>} [**tag-position** <1-8>]		
no match offset <0-127> **data** *HEX* [**mask** *MASK*]		
no match ethertype { **ip** | **arp** | *ETHERTYPE*}		
no match protocol { **icmp** | **igmp**}		
no match protocol { **tcp** | **udp**} [{**srcport** *PORT* | **dstport** *PORT*}]		

To specify the action policy of CPU packet filter for the packets matching the configured

match patterns, use the following command.

Command	Mode	Description
action {**permit** | **drop**}	CPU-Filter	Specifies a drop or permit statement of the CPU packet filter with the configured match pattern. permit: permits the traffic of entries drop: discards the traffic of entries
action {**802dot1q** | **802dot1q-attach**} **tpid** { - | *TPID* } **pcp** { - | <0-7> } **vid** { - | <1-4094> } [**tag-position** <1-8>]		Configures the action to be taken according to the 802.1q tag. 802dot1q: translates 802.1q tag 802dot1q-attach: attaches 802.1q tag 802dot1q-detach: detaches 802.1q tag tpid: tag protocol ID TPID: tag protocol ID (ex: 8100) pcp: priority code point VLAN: VLAN ID, 1 to 4094 tag-position: VLAN tag position -: any
action 802dot1q-detach [**tag-position** <1-8>]		
action rate-limit <1-100> **burst-size** <1-100>		Sets the bandwidth for classified packets belonging to specified CPU packet filter 1-100: permits the number of packets per second 1-100: size that can be store token

If two or more created CPU packet filters match the same packet then the filter having a higher priority will be processed first. To specify a priority of the CPU packet filter, use the following command.

Command	Mode	Description
priority <1-65535>	CPU-Filter	Sets the priority for the CPU packet filter. 1-65535: value of priority

To choose a type of packets to be applied by the configured CPU packet filter, use the following command.

Command	Mode	Description
stage {**cpu-tx** | **cpu-rx** | **vid-assigned**}	CPU-Filter	Selects a type of CPU packets to be applied by the user-defined filtering policy. cpu-tx: filtering for outgoing packets from CPU cpu-rx: filtering for incoming packets to CPU vid-assigned: filtering for the incoming packets after matching VLAN ID assigned
apply		Saves and applies the configured CPU packet filter

To display a configured CPU packet filter, use the following command.

Command	Mode	Description
show cpu-pkt-filter [*NAME*]	Enable	Shows a configured CPU packet filter.

	Global CPU-Filter	

To clear the collected statistics counter of CPU packet filter, use the following command.

Command	Mode	Description
clear cpu-pkt-filter stats [*NAME*]	Global CPU-Filter	Resets the collected statistics counters of CPU packet filter.

6.3.11 Running Process

The OLT provides a function that shows information of the running processes. The information with this command can be very useful to manage the switch.

To display information of the running processes, use the following command.

Command	Mode	Description
show process	Enable Global Bridge	Shows information of the running processes.

The following is an example of displaying information of the running processes.

```
SWITCH# show process
USER     PID  %CPU  %MEM    VSZ   RSS  TTY   STAT  START  TIME  COMMAND
admin      1   0.2   0.2   1448   592  ?     S     20:12  0:05  init [3]
admin      2   0.0   0.0      0     0  ?     S     20:12  0:00  [keventd]
admin      3   0.0   0.0      0     0  ?     SN    20:12  0:00  [ksoftirqd_CPU0]
admin      4   0.0   0.0      0     0  ?     S     20:12  0:00  [kswapd]
admin      5   0.0   0.0      0     0  ?     S     20:12  0:00  [bdflush]
admin      6   0.0   0.0      0     0  ?     S     20:12  0:00  [kupdated]
admin      7   0.0   0.0      0     0  ?     S     20:12  0:00  [mtdblockd]
admin      8   0.0   0.0      0     0  ?     SW<   20:12  0:00  [bcmDPC]
admin      9   1.4   0.0      0     0  ?     SW<   20:12  0:29  [bcmCNTR.0]
admin     10   1.4   0.0      0     0  ?     SW<   20:12  0:29  [bcmCNTR.1]
admin     17   0.0   0.0      0     0  ?     SWN   20:12  0:00  [jffs2_gcd_mtd3]
admin    149   0.0   0.3   1784   776  ?     S     Jan01  0:00  /sbin/syslogd -m
admin    151   0.0   0.2   1428   544  ?     S     Jan01  0:00  /sbin/klogd -c 1
admin    103   2.6   2.0  20552  5100  ?     S     20:12  0:53  /usr/sbin/swchd

(Omitted)

SWITCH#
```

6.3.12 Displaying System Software

To display a current system software version, use the following command.

Command	Mode	Description
show version	Enable Global	Shows a version of system software.

	Bridge	

To display a size of the current system software, use the following command.

Command	Mode	Description
show os-size	Enable Global Bridge	Shows a size of system software.

6.3.13 Displaying Installed OS

To display the current usage of the system flash memory, use the followng command.

Command	Mode	Description
show flash	Enable/Global/Bridge	Shows the current usage of the system flash memory.

6.3.14 Default OS

The OLT supports the dual OS feature. You can verify the running OS in the flash memory with the **show flash** command. When two system OSs are installed, you can set one of those as the default OS. To set the default OS of the system, use the following command.

Command	Mode	Description
default-os {**os1** | **os2**}	Enable	Sets the default OS of the system. (default: os1)

6.3.15 Switch Status

To display the temperature of switch, power status, edfa status and fan status, use the following command.

Command	Mode	Description
show status edfa	Enable Global Bridge	Shows the edfa status of the switch.
show status fan		Shows the fan status of the switch.
show status temp		Shows the current temperature of the switch.
show status power	Enable Global	Shows the current power status.
show power status		
show environment		Shows fan stauts and temperature of switch.

6.3.16 Forwarding Information Base (FIB) Table

The FIB is a table that contains a mirror image of the forwarding information in the IP routing table. When routing or topology changes occur in the network the route processor updates the IP routing table and the information updates the FIB. Because there is a one-to-one correlation between FIB entries and routing table entries, the FIB contains all

known routes and eliminates the need for route cache maintenance that is associated with switching paths, such as fast switching and optimum switching. FIB is used for making IP destination prefix-based switching decisions and maintaining next-hop address information based on the information in the IP routing table.

To display the forwarding entries in the FIB table on the switching fabric, use the following command.

Command	Mode	Description
show ip route fib	Enable Global Bridge	Shows the forwarding entries in the FIB table.

To set the multipath numbers installed to FIB, use the following command.

Command	Mode	Description
ip maximum-paths <1-8>	Global	Sets multipath numbers that installed to the Forwarding Information Base(FIB) 1-8: the numbers of multipath supported (defualt:4)

6.3.17 Tech Support Information

For various reason, a system error may occur. Once the system error occurs, system engineers try to examine the internal system information such as a system configuration, log data, memory dump, and so on to solve the problem.

To reduce the effort to acquire the detail informtation of the system for a technical suppport, the OLT provides the function that generates all the system information reflecting the current state. Using this function, you can verify all the details on a console screen or even in the remote place via FTP/TFTP.

To generate the tech-support information, use the following command.

Command	Mode	Description
tech-support {**all** | **crash-info**} **console**	Enable	Generates the tech-support information on a console screen.
tech-support {**all** | **crash-info**} **remote** *A.B.C.D* {**ftp** | **tftp**}		Generates the tech-support information in the remote place via FTP or TFTP. The name of the generated information file is **a.info**. (This is not changeable.)

In case of generating the tech-support information on a console screen, the contents will be displayed without the screen pause regardless of your terminal configuration.

6.3.18 System Boot Information

To display the information of the last system boot, use the following command.

Command	Mode	Description

show boot-info	Enable Global Bridge	Shows the information of the last system boot.

6.3.19 Network Service Module (NSM) Daemon Debugging

To enable NSM daemon debugging, use the following command.

Command	Mode	Description
debug nsm [**all**]	Enable	Enables NSM debugging. all: all NSM debugging
debug nsm {**events** | **kernel**}		Enables NSM events/kernel debugging.
debug nsm packet {**send** | **recv**} [**detail**]		Enables NSM packets debugging. packet: NSM packets send: outgoing packets recv: incoming packets detail: detailed information
debug nsm packet [**detail**]		

To disable NSM debugging, use the following command.

Command	Mode	Description
no debug nsm [**all**]	Enable	Disables NSM debugging.
no debug nsm {**events** | **kernel**}		
no debug nsm packet {**send** | **recv**} [**detail**]		
no debug nsm packet [**detail**]		

To display the debugging information, use the following command.

Command	Mode	Description
show debugging nsm	Enable Global Bridge	Shows the debugging information of NSM.

To disable all debugging, use the following command.

Command	Mode	Description
no debug all [**ipv6** | **nsm**]	Enable	Disables all debugging.

7 Network Management

7.1 Simple Network Management Protocol (SNMP)

The simple network management protocol (SNMP) is an application-layer protocol designed to facilitate the exchange of management information between network devices. SNMP consists of three parts: an SNMP manager, a managed device and an SNMP agent. SNMP provides a message format for sending information between SNMP manager and SNMP agent. The agent and MIB reside on the switch. In configuring SNMP on the switch, you define the relationship between the manager and the agent. According to community, you can give right only to read or right to both read and write. The SNMP agent has MIB variables to reply to requests from SNMP administrator. In addition, SNMP administrator can obtain data from the agent and save data in the agent. The SNMP agent gets data from MIB, which saves information on system and network.

SNMP agent sends a trap to administrator for specific cases. Trap is a warning message to alert network status to SNMP administrator.

The OLT enhances access management of SNMP agent and limits the range of OID opened to agents.

7.1.1 SNMP Service

To enable/disable SNMP service, use the following command.

Command	Mode	Description
service snmp	Global	Enables SNMP service.
no service snmp		Disables SNMP service. (default)

7.1.2 SNMP Community

Only an authorized person can access SNMP agent by configuring SNMP community with a community name and additional information.

To configure SNMP community to allow an authorized person to access, use the following command.

Command	Mode	Description
snmp community {**ro** | **rw**} *COMMUNITY* [*A.B.C.D*] [*OID*]	Global ONU-Profile	Creates SNMP community. COMMUNITY: community name
no snmp community {**ro** | **rw**} *COMMUNITY*		Deletes created community.

i

You can configure up to 3 SNMP communities for each read-only and read-write.

To display configured SNMP community, use the following command.

Command	Mode	Description
show snmp community	Enable Global Bridge	Shows created SNMP community.

The following is an example of creating 2 SNMP communities.

```
SWITCH(config)# snmp community ro public
SWITCH(config)# snmp community rw private
SWITCH(config)# show snmp community

Community List
Type  Community        Source             OID
-----------------------------------------------
ro    public
rw    private

SWITCH(config)#
```

7.1.3 SNMP Agent Administrator

You can specify the basic information of SNMP agent as administrator, location, and address that confirm its own identity.

To set the basic information of the SNMP agent, use the following command.

Command	Mode	Description
snmp contact *NAME*	Global	Sets the name of the administrator.
snmp location *LOCATION*		Sets the location of the SNMP agent.
no snmp contact		Deletes the specified basic information for each item.
no snmp location		

The following is an example of specifying basic information of SNMP agent.

```
SWITCH(config)# snmp contact furukawa<02.3484.6500>
SWITCH(config)# show snmp contact

contact  furukawa<02.3484.6500>

SWITCH(config)# snmp location Seoul,Korea
SWITCH(config)# show snmp location

location  Seoul,Korea

SWITCH(config)#
```

To display the basic information of the SNMP agent, use the following command.

Command	Mode	Description
show snmp contact	Enable Global	Shows the name of the administrator.
show snmp location		Shows the location of the SNMP agent.

	Bridge	

7.1.4 Assigning IP Address of SNMP Agent

If SNMP agent has several IP addresses, SNMP carries the information through the best suited path (IP address) when SNMP administrator requests for information. It means that SNMP administrator can be received the information from a different IP address which was not actually a given IP address before. To assign IP address of SNMP agent, use the following command.

Command	Mode	Description
snmp agent-address *A.B.C.D*	Global	Assigns an IP address of SNMP agent.
no snmp agent-address		Deletes the configured IP address of SNMP agent

To display IP address of SNMP agent, use the following command.

Command	Mode	Description
show snmp agent-address	Enable/Global/Bridge	Shows an IP address of SNMP agent.

7.1.5 SNMP Com2sec

SNMP v2 authorizes the host to access the agent according to the identity of the host and community name. The **com2sec** command specifies the mapping from the identity of the host and community name to security name.

To configure an SNMP security name, use the following command.

Command	Mode	Description
snmp com2sec *SECURITY* {*IP-ADDRESS* | *IP-ADDRESS/M*} *COMMUNITY*	Global	Specifies the mapping from the identity of the host and community name to security name, enter security and community name. SECURITY: security name COMMUNITY: community name
no snmp com2sec *SECURITY*		Deletes a specified security name, enter the security name. SECURITY: security name
show snmp com2sec	Enable Global Bridge	Shows a specified security name.

The following is an example of configuring SNMP com2sec.

```
SWITCH(config)# snmp com2sec TEST 10.1.1.1 PUBLIC
SWITCH(config)# show snmp com2sec

Com2Sec List
SecName          Source            Community
-------------------------------------------------
```

```
TEST            10.1.1.1          PUBLIC

SWITCH(config)#
```

7.1.6 SNMP Group

You can create an SNMP group that can access SNMP agent and its community that belongs to a group.

To create an SNMP group, use the following command.

Command	Mode	Description
snmp group *GROUP* {**v1** | **v2c** | **v3**} *SECURITY*	Global	Creates SNMP group, enter the group name. GROUP: group name SECURITY: security name
no snmp group *GROUP* [{**v1** | **v2c** | **v3**} [*SECURITY*]]		Deletes SNMP group, enter the group name. GROUP: group name
show snmp group	Enable Global	Shows a created SNMP group.

7.1.7 SNMP View Record

You can create an SNMP view record to limit access to MIB objects with object identity (OID) by an SNMP manager.

To configure an SNMP view record, use the following command.

Command	Mode	Description
snmp view *VIEW* {**included** | **excluded**} *OID* [*MASK*]	Global	Creates an SNMP view record. VIEW: view record name included: includes a sub-tree. excluded: excludes a sub-tree. OID: OID number
no snmp view *VIEW* [*OID*]		Deletes a created SNMP view record. VIEW: view record name

To display a created SNMP view record, use the following command.

Command	Mode	Description
show snmp view	Enable Global Bridge	Shows a created SNMP view record.

The following is an example of creating an SNMP view record.

```
SWITCH(config)# snmp view TEST included 410
SWITCH(config)# show snmp view
```

```
View List
ViewName          Type      SubTree / Mask
-----------------------------------------
TEST              included  410

SWITCH(config)#
```

7.1.8 Permission to Access SNMP View Record

To grant an SNMP group to access to a specific SNMP view record, use the following command.

Command	Mode	Description
snmp access *GROUP* {**v1** | **v2c**} *READ-VIEW WRITE-VIEW NOTIFY-VIEW*	Global	Grants an SNMP group to access a specific SNMP view record. GROUP: group name
snmp access *GROUP* **v3** {**noauth** | **auth** | **priv**} *READ-VIEW WRITE-VIEW NOTIFY-VIEW*		Grants an SNMP version 3 group to access a specific SNMP view record. GROUP: group name
no snmp access *GROUP*		Deletes a granted SNMP group to access a specific SNMP view record.

To display a granted SNMP group to access to a specific SNMP view record, use the following command.

Command	Mode	Description
show snmp access	Enable Global Bridge	Shows a granted SNMP group to access to a specific SNMP view record.

7.1.9 SNMP Version 3 User

In SNMP version 3, you can register an SNMP agent as user. If you register an SNMP version 3 user, you should configure it with the authentication key.

To create/delete an SNMP version 3 user, use the following command.

Command	Mode	Description
snmp user *USER* {**md5** | **sha**} *AUTH_KEY* [**des** *PRIVATE_KEY*]	Global	Creates an SNMP version 3 user.
no snmp user *USER*		Deletes a registered SNMP version 3 user.

To display a current SNMP version 3 user, use the following command.

Command	Mode	Description
show snmp user	Enable Global Bridge	Displays an SNMP version 3 user.

7.1.10 SNMP Engine ID

SNMP Engine ID is an administratively unique identifier of a participant in SNMP communication within a single management domain. The SNMP manager and SNMP agent must be configured by an administrator to have unique SNMP Engine IDs.

The agent needs information for the SNMP Engine ID of the target-address of the recipient to send the inform PDU to the authoritative side. To configure a local SNMP engine ID, use the following command.

Command	Mode	Description
snmp engine-id {**hex** *HEXSTRING* | **text** *STRING*}	Global	Configures the SNMP Engine ID name for the local SNMP engine. HEXSTRING: uses a hexadecimal number STRING: uses an number of characters
no snmp engine-id		Returns the SNMP Engine ID to its default value

To display the configured local SNMP engine IDs, use the following command.

Command	Mode	Description
show snmp engine-id	Enable Global	Shows the configured local SNMP engine IDs

7.1.11 SNMPv3 Notification

In SNMPv3, you create traps and informs by configuring the notification name, target address, and target parameters.

7.1.11.1 Configuring SNMP Target

The target address defines a management application's address and parameters to be used in sending notifications. To configure the notification SNMP target address, use the following command.

Command	Mode	Description
snmp targetaddr *TARGETADDR TARGETPARAM* {*A.B.C.D* | *X:X::X:X*} [*PORT TIMEOUT RETRIES TAG*]	Global	Configures the notification SNMP target address. TARGETADDR: the name of target address TARGETPARAM: the name of target parameter A.B.C.D: IPv4 address of the target X:X::X:X: IPv6 address of the target PORT: UDP port number in the range 1 to 65535 TIMEOUT: the time in seconds to wait for an acknowledgement before resending an unacknowledged PDU RETRIES: the number of retries for resending Inform PDUs TAG: a tag name in the tag list

no snmp targetaddr *TARGETADDR*		Deletes the notification target address.

The SNMP target parameters define the message processing and security parameters that are used in sending notifications to a particular management target. To configure the SNMP parameters with a security model, use the following command.

Command	Mode	Description
snmp targetparams *TARGETPARAM* { **v1**| **v2c**} *SECURITY*	Global	Configures the SNMP parameters used to generate a message to a target and specifies the security model. TARGETPARAM: the target parameters name SECURITY: com2sec name
snmp targetparams *TARGETPARAM* **v3** *SECURITY* { **noauth** | **auth** | **priv**}		Configures the SNMP parameters and specifies v3 security model and its security level for the user. SECURITY: user name for v3 auth noauth: a security level, which implies no authentication. auth: the message digest 5 or the secure hash algorithm packet authentication. priv: data encryption standard packet encryption
no snmp targetparams *TARGETPARAM*		Deletes the notification target parameters.

To display the notification target address and parameters, use the following command.

Command	Mode	Description
show snmp targetaddr	Enable Global	Shows the notification target address.
show snmp targetparams		Shows the notification target parameters.

7.1.11.2 SNMP Notification Type

There are two types of notifications: trap and inform. In case of traps, the sender cannot determine whether the trap is received or not because the receiver does not any acknowledgment when it receives a trap. To increase reliability, an inform is stored and sent again if the sender does not receive a response.

To define the notification and specify the notification type (trap/inform), use the following command.

Command	Mode	Description
snmp notify *NOTIFY TAG* [**trap** | **inform**]	Global	Defines the notification and specifies the type. NOTIFY: the notification name TAG: the notification tag defines a set of target addresses to which this notification is sent trap | inform: type of notification
no snmp notify *NOTIFY*		Deletes the defined notification.

To display information for the notify type, use the following command.

Command	Mode	Description
show snmp notify	Enable Global	Shows information for the notify type.

The following is an example of configuring SNMPv3 trap notification.

```
SWITCH(config)# snmp engine-id hex 80:00:05:23:01:0A:46:01:A3
SWITCH(config)# show snmp engine-id
Local SNMP Engine ID
Type     Engine ID
--------------------------------
hex      80:00:05:23:01:0A:46:01:A3
SWITCH(config)# snmp com2sec com2-test 1.1.2.0/24 mmm
SWITCH(config)# snmp com2sec com2-pakih 10.70.1.163 powertest
SWITCH(config)# snmp user pakih md5 test1234 des des12345
SWITCH(config)# snmp targetparams param1 v1 com2-pakih
SWITCH(config)# snmp targetparams param3 v3 pakih auth
SWITCH(config)# snmp targetparams sss v3 pakih noauth
SWITCH(config)# snmp targetaddr taddr1 param1 10.70.1.163 162 1500 3 tag1 tag3
SWITCH(config)# snmp targetaddr no1 sss 10.70.1.163 162 1500 3 tag5
SWITCH(config)# snmp targetaddr a1 sss 1.1.1.1
SWITCH(config)# snmp notify n5 tag5
SWITCH(config)# show snmp com2sec
Com2Sec List
SecName         Source           Community
-----------------------------------------------
com2-test       1.1.2.0/24        mmm
com2-pakih      10.70.1.163       powertest

SWITCH(config)# show snmp user
User List
Name            AuthMode AuthPassphrase   PrivMode PrivPassphrase
-------------------------------------------------------------------
pakih            md5      test1234         des      des12345

SWITCH(config)# show snmp targetparams
Targetparam Table
TargetparamName  SecModel SecName         SecLevel
-------------------------------------------------------
param1             v1      com2-pakih
param3             v3      pakih            auth
sss                v3      pakih            noauth

SWITCH(config)# show snmp targetaddr
Targetaddr Table
TargetaddrName  TargetparamsName Address   Port    Timeout  Retries  Taglist
-------------------------------------------------------------------------------
a1         sss            1.1.1.1
no1        sss            10.70.1.163       162     1500     3        tag5
taddr1     param1         10.70.1.163       162     1500     3        tag1 tag3
```

```
SWITCH(config)# show snmp notify
Notify Table
NotifyName      Tag             Type
-----------------------------------------
n5              tag5

SWITCH(config)#
```

7.1.12 SNMP Trap

SNMP trap is an alert message that SNMP agent notifies SNMP manager about certain problems. If you configure the SNMP trap, the system transmits pertinent information to network management program. In this case, trap message receivers are called a trap host.

7.1.12.1 SNMP Trap Mode

To select the SNMP trap mode, use the following command.

Command	Mode	Description
snmp trap-mode {**alarm-report** | **event**}	Global	Selects the SNMP trap mode. alarm-report: alarm report based trap event: event based trap (default)

7.1.12.2 SNMP Trap Host

To set an SNMP trap host, use the following command.

Command	Mode	Description
snmp trap-host {*A.B.C.D* | *X:X::X:X*} [*COMMUNITY*]	Global	Specifies an SNMP trap v1 host.
snmp trap2-host {*A.B.C.D* | *X:X::X:X*} [*COMMUNITY*]		Specifies an SNMP trap v2 host.
snmp inform-trap-host {*A.B.C.D* | *X:X::X:X*} [*COMMUNITY*]		Specifies an SNMP inform trap host.

To delete a specified SNMP trap host, use the following command.

Command	Mode	Description
no snmp trap-host {*A.B.C.D* | *X:X::X:X* }	Global	Deletes a specified SNMP trap v1 host.
no snmp trap2-host {*A.B.C.D* | *X:X::X:X* }		Deletes a specified SNMP trap v2 host.
no snmp inform-trap-host {*A.B.C.D* | *X:X::X:X* }		Deletes a specified SNMP inform trap host.

i You can set maximum 16 SNMP trap hosts with inputting one by one.

The following is an example of setting an SNMP trap host.

```
SWITCH(config)# snmp trap-host 10.1.1.3
SWITCH(config)# snmp trap-host 20.1.1.5
SWITCH(config)# snmp trap-host 30.1.1.2
SWITCH(config)#
```

7.1.12.3 Enabling SNMP Trap

The system provides various kind of SNMP trap, but it may inefficiently work if all these trap messages are sent very frequently. Therefore, you can select each SNMP trap sent to an SNMP trap host.

- **admin-access-login** is shown to notify the administrator that the system is accessed by SNMP. The system leaves the login information by syslog when it is logged by telnet or console. When the system is accessed by SNMP, it regards the connection as having been maintained for the connection valid time (300 seconds). During the time, the system is accessed by SNMP from the same origin, the connection time will be refreshed to 300 seconds. If there is no SNMP access during the time (300 seconds), the system regards that the connection is invalid. After that, if the system is accessed by SNMP again, the trap will be generated again.
- **authentication-failure** is shown to inform wrong community is input when user trying to access to SNMP inputs wrong community.
- **cold-start** is shown when SNMP agent is turned off and restarts again.
- **cpu-threshold** is shown when CPU utilization exceeds the threshold specified by user. Also, when CPU load falls below the threshold, trap message will be shown to notify it.
- **dhcp-lease** is shown when no more IP address is left in the DHCP pool. Even if this occurs only in one DHCP pool of several pools, this trap message will be shown.
- **dying-gasp** is shown when a power outage of any downstream equipments occur with a critical error.
- **link-up/down** is shown when network of port specified by user is disconnected, or when the network is connected again.
- **login-failed** is shown in case of a security violation (failed login, unauthorized SNMP query).
- **memory-threshold** is shown when memory usage exceeds the threshold specified by user. Also, when memory usage falls below the threshold, trap message will be shown to notify it.
- **port-threshold** is shown when the port traffic exceeds the threshold configured by user. Also, when port traffic falls below the threshold, trap message will be shown.
- **system-restart** is shown to inform the system rebooting.
- **trap-log** is shown when the trap logs are more than 90% full and will wrap around soon.

i The system is configured to send all the SNMP traps as a default.

To enable SNMP trap, use the following command.

Command	Mode	Description
snmp trap admin-access-login	Global	Generates SNMP trap when SNMP authentication is failed.
snmp trap auth-fail		Generates SNMP trap when SNMP authentication is failed.
snmp trap cold-start		Generates SNMP trap when SNMP agent is restarted.
snmp trap dying-gasp		Generates a SNMP trap when a power outage of any downstream equipment occurs with a critical error.
snmp trap link-up *PORTS*		Generates SNMP trap when a port is connected to network.
snmp trap link-down *PORTS*		Generates SNMP trap when a port is disconnected from network.
snmp trap login-failed		Generates a SNMP trap when the login failed.
snmp trap mem-threshold		Generates SNMP trap when memory usage exceeds or falls below the threshold.
snmp trap cpu-threshold		Generates SNMP trap when CPU load exceeds or falls below the threshold.
snmp trap port-threshold		Generates SNMP trap when the port traffic exceeds or falls below the threshold.
snmp trap system-restart		Generates a SNMP trap when a system is restarted.
snmp trap dhcp-lease		Generates SNMP trap when no more IP address is left in the DHCP pool.
snmp trap trap-log		Generates a SNMP trap when the trap logs are more than 90% full.
snmp trap-source-interface *IFNAME*		Generates a SNMP trap when trap-source-interface is configured.

To disable SNMP trap, use the following command.

Command	Mode	Description
no snmp trap	Global	Disables each SNMP trap.
no snmp trap admin-access-login		
no snmp trap auth-fail		
no snmp trap cold-start		
no snmp trap cli-history		
no snmp trap link-up *PORTS*		
no snmp trap link-down *PORTS*		
no snmp trap login-failed		
no snmp trap mem-threshold		
no snmp trap cpu-threshold		
no snmp trap port-threshold		
no snmp trap login-failed		

no snmp trap dhcp-lease		
no snmp trap system-restart		
no snmp trap trap-log		
no snmp trap-log non-volatile		
no snmp trap-log threshold		
no snmp trap-source-interface		

7.1.12.4 Displaying SNMP Trap

To display the configuration of the SNMP trap, use the following command.

Command	Mode	Description
show snmp trap	Enable Global Bridge	Shows the configuration of SNMP trap.
show snmp trap-source-interface		Shows SNMP trap source interface.
show snmp alarm-report		Shows a collected alarm report based trap.

The following is an example of configuring SNMP trap hosts.

```
SWITCH(config)# snmp trap-host 10.1.1.1
SWITCH(config)# snmp trap2-host 20.1.1.1
SWITCH(config)# snmp inform-trap-host 30.1.1.1
SWITCH(config)# show snmp trap

snmp trap mode:        event
----------------------------

Trap-Host List
Type              Host               Community
-------------------------------------------------
inform-trap-host 30.1.1.1
trap2-host        20.1.1.1
trap-host         10.1.1.1

Trap List
Trap-type        Status
--------------------------
auth-fail        enable
cold-start       enable
cpu-threshold    enable
port-threshold   enable
dhcp-lease       enable
power            enable
module           enable
fan              enable
temp-threshold   enable
mem-threshold    enable

SWITCH(config)#
```

7.1.12.5 SNMP Trap Message Logging and Threshold

SNMP trap message logs are useful to the system administrator for troubleshooting problems in the network. To enable/disable SNMP trap message logging to the non-volatile memory, use the following command.

Command	Mode	Description
snmp trap-log non-volatile	Global	Enables saving the SNMP trap message logs to non-volatile memory
snmp trap-log threshold *VALUE*		Sets the threshold of SNMP trap message logs in non-volatile memory. VALUE: threshold [%] (default: 90%)
no snmp trap-log non-volatile		Disables saving the SNMP trap message logs to non-volatile memory
no snmp trap-log threshold		Deletes the configured threshold of SNMP trap messages logs.

To remove all stored SNMP trap message logs from the non-volatile memory, use the following command.

Command	Mode	Description
clear snmp trap-log non-volatile	Global	Clears all the SNMP trap logs in non-volatile memory

To display the SNMP trap message logs in the non-volatile memory, use the following command.

Command	Mode	Description
show snmp trap-log non-volatile [<1-200>]	Enable Global	Shows the recorded SNMP trap message logs in the non-volatile memory. 1-200: SNMP logs line number to be displayed

7.1.13 SNMP Alarm

The OLT provides an alarm notification function. The alarm will be sent to a SNMP trap host whenever a specific event in the system occurs through CLI. You can also set the alarm severity on each alarm and make the alarm be shown only in case of selected severity or higher. This enhanced alarm notification allows system administrators to manage the system efficiently.

7.1.13.1 Alarm Notify Activity

Normally the OLT is supposed to generate an alarm only when a pre-defined event has occurred such as the fan fail, system restart, temperature high, etc. However, you can additionally configure the system to generate an alarm when any configuration parameter has been changed via CLI.

To enable/disable the alarm notify activity, use the following command.

Command	Mode	Description
snmp notify-activity {**enable** | **disable**}	Global	Enables/disables the alarm notify activity. (default: disable)

7.1.13.2 Alarm Severity Criterion

You can set an alarm severity criterion to make an alarm be shown only in case of selected severity or higher. For example, if an alarm severity criterion has been set to **major**, you will see only an alarm whose severity is **major** or **critical**.

To set an alarm severity criterion, use the following command.

Command	Mode	Description
snmp alarm-severity criteria {**critical** | **major** | **minor** | **warning** | **intermediate**}	Global	Sets an alarm severity criterion. (default: warning)

i The order of alarm severity is **critical** > **major** > **minor** > **warning** > **intermediate**.

7.1.13.3 Default Alarm Severity

To set default alarm severity, use the following command.

Command	Mode	Description
snmp alarm-severity default {**critical** | **major** | **minor** | **warning** | **intermediate**}	Global	Sets default alarm severity. (default: minor)

7.1.13.4 Generic Alarm Severity

To set generic alarm severity, use the following command.

Command	Mode	Description
snmp alarm-severity admin-access-login {**critical** | **major** | **minor** | **warning** | **intermediate**}	Global	Sets severity of an alarm for admin-access-login.
snmp alarm-severity auth-fail {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets severity of an alarm for auth-fail.
snmp alarm-severity cli-history {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets severity of cli history log.
snmp alarm-severity cold-start {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets severity of an alarm for system cold restart.
snmp alarm-severity cpu-load-over {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets severity of an alarm for CPU load high.
snmp alarm-severity dhcp-lease {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets severity of an alarm for no more IP address left in the DHCP pool.
snmp alarm-severity dhcp-illegal {**critical** | **major** |		Sets severity of an alarm for illegal

Command	Mode	Description
minor | **warning** | **intermediate**}		DHCP entry.
snmp alarm-severity dying-gasp {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets severity of an alarm for dying-gasp event.
snmp alarm-severity ip-conflict {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets severity of an alarm for IP address conflict.
snmp alarm-severity memory-over {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets severity of an alarm for system memory usage high.
snmp alarm-severity mfgd-block {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets severity of an alarm for MAC flood guard block.
snmp alarm-severity port-link-down {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets severity of an alarm for Ethernet port link down.
snmp alarm-severity port-link-up {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets severity of an alarm for Ethernet port link up.
snmp alarm-severity port-thread-over {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets severity of an alarm for RX/TX port threshold over.
snmp alarm-severity rmon-alarm-rising {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets severity of an alarm for RMON alarm rising.
snmp alarm-severity rmon-alarm-falling {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets severity of an alarm for RMON alarm falling.
snmp alarm-severity system-restart {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets severity of an alarm for system restart.

To delete configured alarm severity, use the following command.

Command	Mode	Description
no snmp alarm-severity admin-access-login	Global	Deletes configured alarm severity.
no snmp alarm-severity auth-ail		
no snmp alarm-severity cli-history		
no snmp alarm-severity cold-start		
no snmp alarm-severity cpu-load-over		
no snmp alarm-severity dhcp-lease		
no snmp alarm-severity dhcp-illegal		
no snmp alarm-severity dying-gasp		
no snmp alarm-severity ip-conflict		
no snmp alarm-severity memory-over		
no snmp alarm-severity mfgd-block		
no snmp alarm-severity port-link-down		
no snmp alarm-severity port-link-up		
no snmp alarm-severity port-thread-over		
no snmp alarm-severity rmon-alarm-rising		
no snmp alarm-severity rmon-alarm-falling		
no snmp alarm-severity system-restart		

7.1.13.5 Displaying SNMP Alarm

To display a collected alarm, use the following command.

Command	Mode	Description
show snmp alarm-severity	Enable Global Bridge	Shows a configured alarm severity.
show snmp alarm-history		Shows a collected alarm history.
show snmp alarm-report		Shows a collected alarm report.

To deletes a collected alarm in the system, use the following command.

Command	Mode	Description
snmp clear alarm-history	Global	Deletes a collected alarm history in the system.
snmp clear alarm-report [*SEQ_NO***]**		Deletes a collected alarm report in the system. ㅊ

7.1.14 SNMP Message Logging

SNMP message logs are useful to the system administrator for troubleshooting problems in the network. To enable/disable SNMP message logging to the non-volatile memory, use the following command.

Command	Mode	Description
snmp log non-volatile	Global	Enables saving the SNMP message logs to non-volatile memory
no snmp log non-volatile		Disables saving the SNMP message logs to non-volatile memory

To remove all stored SNMP message logs from the non-volatile memory, use the following command.

Command	Mode	Description
clear snmp log non-volatile	Global	Clears all the SNMP logs in non-volatile memory

To display the SNMP message logs in the non-volatile memory, use the following command.

Command	Mode	Description
show snmp log	Enable Global	Shows the recorded SNMP message logs.
show snmp log non-volatile [<1-2000>]		Shows the recorded SNMP message logs in the non-volatile memory. 1-100: SNMP logs line number to be displayed

show snmp log non-volatile tail <1-2000>		Shows currently recorded SNMP message logs in the non-volatile memory.

7.1.15 Disabling SNMP

To disable SNMP, use the following command.

Command	Mode	Description
no snmp	Global	Disables SNMP.
no snmp vrf		Disables VPN snmp

When you use the **no snmp** command, all configurations of SNMP will be lost.

7.1.16 Displaying SNMP Configuration

To display all configurations of SNMP, use the following command.

Command	Mode	Description
show snmp	Enable Global Bridge	Shows all configurations of SNMP.

7.2 Link Layer Discovery Protocol (LLDP)

Link Layer Discovery Protocol (LLDP) is the function of transmitting data for network management for the switches connected in LAN according to IEEE 802.1ab standard.

7.2.1 LLDP Operation

The OLT supporting LLDP transmits the management information between near switches. The information carries the management information that can recognize the network elements and the function. This information is saved in internal Management Information Base (MIB).

When LLDP starts to operate, the switches send their information to near switches. If there is some change in local status, it sends their changed information to near switch to inform their status. For example, if the port status is disabled, it informs that the port is disabled to near switches. And the switch that receives the information from near switches processes LLDP frame and saves the information of the other switches. The information received from other switches is aged.

7.2.2 Enabling LLDP

To enable/disable LLDP, use the following command.

Command	Mode	Description
lldp *PORTS*	Bridge	Enables LLDP function on a port.
no lldp *PORTS*		Disables LLDP function.

7.2.3 LLDP Operation Type

If you activated LLDP on a port, configure LLDP operation type.

Each LLDP operation type works as one of the followings:

- **both** sends and receive LLDP frame.
- **tx_only** only sends LLDP frame.
- **rx_only** only receives LLDP frame.
- **disable** does not process any LLDP frame.

To configure how to operate LLDP, use the following command.

Command	Mode	Description
lldp adminstatus *PORTS* [**both** | **tx_only** | **rx_only** | **disable**]	Bridge	Configures LLDP operation type. (default: both)

7.2.4 Basic TLV

LLDP is transmitted through TLV. There are mandatory TLV and optional TLV. In optional TLV, there are basic TLV and organizationally specific TLV. Basic TLV must be in the switch where LLDP is realized, specific TLV can be added according to the feature of the switch.

For the OLT, the administrator can enable and disable basic TLV by selecting it. To enable basic TLV by selecting it, use the following command.

Command	Mode	Description
lldp *PORTS* {**portdescription** | **sysname** | **sysdescription** | **syscap**}	Bridge	Selects basic TLV that to be sent in the port. portdescription: port description sysname: system name sysdescription: system description syscap: system capability
no lldp *PORTS* {**portdescription** | **sysname** | **sysdescription** | **syscap**}		Disables basic TLV configured to be sent in the port.

To specify TLV location ID that is ELIN (Emergency Location Identification Number), use the following command.

Command	Mode	Description
lldp locationID *ELIN*	Bridge	Specifies TLV location ID. ELIN: TLV location ID
no lldp locationID		Deletes the specified TLV location ID.

7.2.5 LLDP Message

For the OLT, it is possible to configure the interval time and times of sending LLDP message. To configure the interval time and times of LLDP message, use the following command.

Command	Mode	Description
lldp msg txinterval <5-32768>	Bridge	Configures the interval of sending LLDP message. The unit is second. (default: 30)
lldp msg txhold <2-10>		Configures the periodic times of LLDP message. (default: 4)

7.2.6 Reinitiating Delay

To configure the interval time of enabling LLDP frame after configuring LLDP operation type, use the following command.

Command	Mode	Description
lldp reinitdelay <1-10>	Bridge	Configures the interval time of enabling LLDP frame from the time of configuring not to process LLDP frame. (default: 2)

To configure delay time of transmitting LLDP frame, use the following command.

Command	Mode	Description
lldp txdelay <1-8192>	Bridge	Configures delay time of transmitting LLDP frame. (default: 2)

7.2.7 Displaying LLDP Configuration

To display LLDP configuration, use the following command.

Command	Mode	Description
show lldp config [*PORTS*]	Enable Global Bridge	Shows LLDP configuration.
show lldp remote [*PORTS*]		Show statistics for remote entries.
show lldp statistics [*PORTS*]		Shows LLDP operation and statistics.

To delete an accumulated statistics on the port, use the following command.

Command	Mode	Description
clear lldp statistics [*PORTS*]	Enable Global Bridge	Deletes an accumulated statistics on the port.

7.3 Remote Monitoring (RMON)

Remote Monitoring (RMON) is a function to monitor communication status of devices connected to Ethernet at remote place. While SNMP can give information only about the device mounting an SNMP agent, RMON gives network status information about overall segments including devices. Thus, user can manage network more effectively. For instance, in case of SNMP it is possible to be informed traffic about certain ports but through RMON you can monitor traffics occurred in overall network, traffics of each host connected to segment, and the current status of traffic between hosts.

Since RMON processes quite lots of data, its processor share is very high. Therefore, administrator should take intensive care to prevent performance degradation and not to overload network transmission caused by RMON. There are nine RMON MIB groups defined in RFC 1757: Statistics, History, Alarm, Host, Host Top N, Matrix, Filter, Packet Capture and Event. The OLT supports two MIB groups of them, most basic ones: Statistics (only for uplink ports) and History.

7.3.1 RMON History

RMON history is periodical sample inquiry of statistical data about each traffic occurred in Ethernet port. Statistical data of all ports are pre-configured to be monitored at 30-minute interval, and 50 statistical data stored in one port. It also allows you to configure the time interval to take the sample and the number of samples you want to save.

To open *RMON Configuration* mode, use the following command.

Command	Mode	Description
rmon-history <1-65535>	Global	Opens *RMON Configuration* mode. 1-65535: index number

The following is an example of opening *RMON Configuration* mode with index number 5.

```
SWITCH(config)# rmon-history 5
SWITCH(config-rmonhistory[5])#
```

Input a question mark <**?**> at the system prompt in *RMON Configuration* mode if you want to list available commands.

The following is an example of listing available commands in *RMON Configuration* mode.

```
SWITCH(config-rmonhistory[5])# ?
RMON history configuration commands:
  active               Activate the history
  data-source          Set data source name for the ethernet port
  do                   To run exec commands in config mode
  exit                 End current mode and down to previous mode
  help                 Description of the interactive help system
  interval             Define the time interval for the history
  owner                Assign the owner who define and is using the history
                       resources
  requested-buckets    Define the bucket count for the interval
  show                 Show running system information
```

```
  write                Write running configuration to memory or terminal

SWITCH(config-rmonhistory[5])#
```

7.3.1.1 Source Port of Statistical Data

To specify a source port of statistical data, use the following command.

Command	Mode	Description
data-source *NAME*	RMON	Specifies a data object ID: NAME: enters a data object ID. (ex. ifindex.n1/port1)

7.3.1.2 Subject of RMON History

To identify a subject using RMON history, use the following command.

Command	Mode	Description
owner *NAME*	RMON	Identifies subject using relevant data, enter the name (max. 32 characters).

7.3.1.3 Number of Sample Data

To configure the number of sample data of RMON history, use the following command.

Command	Mode	Description
requested-buckets <1-65535>	RMON	Defines a bucket count for the interval, enter the number of buckets. 1-65535: bucket number (default: 50)

7.3.1.4 Interval of Sample Inquiry

To configure the interval of sample inquiry in terms of second, use the following command.

Command	Mode	Description
interval <1-3600>	RMON	Defines the time interval for the history (in seconds), enter the value. (default: 1800)

i 1 sec is the minimum time which can be selected. But the minimum sampling interval currently is 30 sec, i.e., all intervals will be round up to a multiple of 30 seconds.

7.3.1.5 Activating RMON History

To activate RMON history, use the following command.

Command	Mode	Description
active	RMON	Activates RMON history.

i Before activating RMON history, check if your configuration is correct. After RMON history is activated, you cannot change its configuration. If you need to change configuration, you need to delete the RMON history and configure it again.

7.3.1.6 Deleting Configuration of RMON History

When you need to change a configuration of RMON history, you should delete an existing RMON history.

To delete an RMON history, use the following command.

Command	Mode	Description
no rmon-history <1-65535>	Global	Deletes the RMON history of specified number, enter the value for deleting.

7.3.1.7 Displaying RMON History

To display an RMON history, use the following command.

Command	Mode	Description
show running-config rmon-history	All	Shows a configured RMON history.

i Always the last values will be displayed but no more than the number of the granted buckets.

The following is an example of displaying RMON history.

```
SWITCH(config-rmonhistory[5])# show running-config rmon-history
!
rmon-history 5
 owner test
 data-source ifindex.hdlc1
 interval 60
 requested-buckets 25
 active
!
SWITCH(config-rmonhistory[5])#
```

7.3.2 RMON Alarm

You need to open *RMON Alarm Configuration* mode first to configure RMON alarm.

Command	Mode	Description
rmon-alarm <1-65535>	Global	Opens *RMON Alarm Configuration* mode. 1-65535: index number

7.3.2.1 Subject of RMON Alarm

You need to configure RMON alarm and identify subject using many kinds of data from alarm. To identify subject of alarm, use the following command.

Command	Mode	Description
owner *NAME*	RMON	Identifies subject using relevant data, enter the name (max. 32 characters).

7.3.2.2 Object of Sample Inquiry

To assign object used for sample inquiry, use the following command.

Command	Mode	Description
sample-variable *MIB-OBJECT*	RMON	Assigns MIB object used for sample inquiry.

7.3.2.3 Absolute and Delta Comparison

There are two ways to compare with the threshold: absolute comparison and delta comparison.

- **Absolute Comparison**
  Comparing sample data with the threshold at configured interval, if the data is more than the threshold or less than it, alarm is occurred
- **Delta Comparison**
  Comparing difference between current data and the latest data with the threshold, if the data is more than the threshold or less than it, alarm is occurred.

To compare object selected as sample with the threshold, use the following command.

Command	Mode	Description
sample-type absolute	RMON	Compares object with the threshold directly.

To configure delta comparison, use the following command.

Command	Mode	Description
sample-type delta	RMON	Compares difference between current data and the latest data with the threshold.

7.3.2.4 Upper Bound of Threshold

If you need to occur alarm when object used for sample inquiry is more than upper bound of threshold, you have to configure the upper bound of threshold. To configure upper bound of threshold, use the following command.

Command	Mode	Description
rising-threshold *VALUE*	RMON	Configures upper bound of threshold. VALUE: 0-2147483647

After configuring upper bound of threshold, configure to generate RMON event when object is more than configured threshold. Use the following command.

Command	Mode	Description
rising-event <1-65535>	RMON	Configures to generate RMON event when object is more than configured threshold. 1-65535: event index

7.3.2.5 Lower Bound of Threshold

If you need an alarm to occur alarm when object used for sample inquiry is less than lower bound of threshold, you should configure lower bound of threshold. To configure lower bound of threshold, use the following command.

Command	Mode	Description
falling-threshold *VALUE*	RMON	Configures lower bound of threshold.

After configuring lower bound of threshold, configure to generate RMON event when object is less than configured threshold. Use the following command.

Command	Mode	Description
falling-event <1-65535>	RMON	Configures to generate RMON alarm when object is less than configured threshold.

7.3.2.6 Standard of the First Alarm

It is possible for users to configure standard when alarm is first occurred. User can select the first point when object is more than threshold, or the first point when object is less than threshold, or the first point when object is more than threshold or less than threshold.

To configure the first RMON alarm to occur when object is less than lower bound of threshold first, use the following command.

Command	Mode	Description
startup-type falling	RMON	Configures the first RMON Alarm to occur when object is less than lower bound of threshold first.

To configure the first alarm to occur when object is firstly more than upper bound of threshold, use the following command.

Command	Mode	Description
startup-type rising	RMON	Configures the first Alarm to occur when object is firstly more than upper bound of threshold.

To configure the first alarm to occur when object is firstly more than threshold or less than threshold, use the following command.

Command	Mode	Description
startup-type rising-and-falling	RMON	Configures the first Alarm to occur when object is firstly more than threshold or less than threshold.

7.3.2.7 Interval of Sample Inquiry

The interval of sample inquiry means time interval to compare selected sample data with upper bound of threshold or lower bound of threshold in terns of seconds.

To configure interval of sample inquiry for RMON alarm, use the following command.

Command	Mode	Description
sample-interval <0-65535>	RMON	Configures interval of sample inquiry. (unit: second)

7.3.2.8 Activating RMON Alarm

After finishing all configurations, you need to activate RMON alarm. To activate RMON alarm, use the following command.

Command	Mode	Description
active	RMON	Activates RMON alarm.

7.3.2.9 Deleting Configuration of RMON Alarm

When you need to change a configuration of RMON alarm, you should delete an existing RMON alarm.

To delete RMON alarm, use the following command.

Command	Mode	Description
no rmon-alarm <1-65535>	Global	Deletes RMON history of specified number, enter the value for deleting.

7.3.3 RMON Event

RMON event identifies all operations such as RMON alarm in the switch. You can configure event or trap message to be sent to SNMP management server when sending RMON alarm.

You need to open *RMON Event Configuration* mode to configure RMON event.

Command	Mode	Description
rmon-event <1-65535>	Global	Opens *RMON Event Configuration* mode. 1-65535: index number

7.3.3.1 Event Community

When RMON event occurs, you need to input community to transmit SNMP trap message to host. Community means a password to give message transmission right.

To configure community for trap message transmission, use the following command.

Command	Mode	Description
community *NAME*	RMON	Configures password for trap message transmission right. NAME: community name

7.3.3.2 Event Description

It is possible to describe event briefly when event occurs. However, the description will not be automatically made. Thus administrator should make the description.

To specify a description about the current RMON event, use the following command.

Command	Mode	Description
description *DESCRIPTION*	RMON	Specifies the description of the current RMON event.

7.3.3.3 Subject of RMON Event

You need to configure event and identify subject using various data from event. To identify subject of RMON event, use the following command.

Command	Mode	Description
owner *NAME*	RMON	Identifies subject of event. You can use maximum 126 characters and this subject should be same with the subject of RMON event.

7.3.3.4 Event Type

When RMON event is happened, you need to configure event type to arrange where to send event.

To configure event type, use the following command.

Command	Mode	Description
type log	RMON	Configures event type as log type. Event of log type is sent to the place where the log file is made.
type trap		Configures event type as trap type. Event of trap type is sent to SNMP administrator and PC.
type log-and-trap		Configures event type as both log type and trap type.
type none		Configures none event type.

7.3.3.5 Activating RMON Event

After finishing all configurations, you should activate RMON event. To activate RMON event, use the following command.

Command	Mode	Description
active	RMON	Activates RMON event.

7.3.3.6 Deleting Configuration of RMON Event

Before changing the configuration of RMON event, you should delete RMON event of the number and configure it again.

To delete RMON event, use the following command.

Command	Mode	Description
no rmon-event <1-65535>	Global	Delete RMON event of specified number.

7.3.4 Simple RMON Event Configuration

You can simply monitor specified event variables, such as total number of received packets on a port during the sample interval. To define what packet types are monitored, the value of parameters' thresholds (falling and rising thresholds) during the sampling interval to generate the syslog message of event, use the following command.

Command	Mode	Description
rmon-simple *PORT* { **crc-align-error** | **jabber** | **oversize-packets** | **undersize-packets** | **fragments** | **drop-events** } <1-65535> *FALLING_THRESHOLD RISING_THRESHOLD*	Global	Configures what packet types are monitored, the value of parameters' thresholds (falling and rising thresholds) to generate the syslog messages of event. PORT : port number 1-65535: sample interval crc-align-error: number of packets received that were from 64 to 1518 octets long, but had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error) jabber: number of occurrences of corrupted data or useless signals the port has encountered oversize-packets: number of received packets that exceeded the maximum size (1518 bytes) undersize-packets: number of frames that were less than the minimum length (64 bytes) fragments: number of undersized frames with alignment errors, and frames with frame check sequence (FCS) errors drop-events: the total number of events in which packets were dropped by the RMON probe due to lack of resources FALLING_THRESHOLD: When the value of the

		monitored variable is smaller than or equal to the falling threshold, a falling event is triggered. (1-2147483647) RISING_THRESHOLD: When the value of the monitored variable is greater than or equal to the rising threshold, a rising event is triggered. (1-2147483647)
no rmon-simple *PORT* { **crc-align-error** | **jabber** | **oversize-packets** | **undersize-packets** | **fragments** | **drop-events** }		Deletes the configured simple RMON event monitoring function.

7.4 Syslog

The syslog is a function that allows the network element to generate the event notification and forward it to the event message collector like a syslog server. This function is enabled as default, so even though you disable this function manually, the syslog will be enabled again.

7.4.1 Syslog Output Level

Syslog Output Level without a Priority

To set a syslog output level, use the following command.

Command	Mode	Description
syslog output {**emerg** | **alert** | **crit** | **err** | **warning** | **notice** | **info** | **debug**} **console**	Global	Generates a syslog message of selected level or higher and forwards it to the console.
syslog output {**emerg** | **alert** | **crit** | **err** | **warning** | **notice** | **info** | **debug**} **local** {**volatile** | **non-volatile**}		Generates a syslog message of selected level or higher in the system memory. volatile: deletes a syslog message after restart. non-volatile: reserves a syslog message.
syslog output {**emerg** | **alert** | **crit** | **err** | **warning** | **notice** | **info** | **debug**} **remote** {*A.B.C.D* | *X:X::X:X*} [**vrf** *VRFNAME*]		Generates a syslog message of selected level or higher and forwards it to a remote host.

To disable a specified syslog output, use the following command.

Command	Mode	Description
no syslog output {**emerg** | **alert** | **crit** | **err** | **warning** | **notice** | **info** | **debug**} **console**	Global	Deletes a specified syslog output.
no syslog output {**emerg** | **alert** | **crit** | **err** | **warning** | **notice** | **info** | **debug**} **local** {**volatile** | **non-volatile**}		
no syslog output {**emerg** | **alert** | **crit** | **err** | **warning** | **notice** | **info** | **debug**} **remote** {*A.B.C.D* | *X:X::X:X*}		

Syslog Output Level with a Priority

To set a user-defined syslog output level with a priority, use the following command.

Command	Mode	Description
syslog output priority {**auth** | **authpriv** | **kern** | **local0** | **local1** | **local2** | **local3** | **local4** | **local5** | **local6** | **local7** | **syslog** | **user**} {**emerg** | **alert** | **crit** | **err** | **warning** |	Global	Generates a user-defined syslog message with a priority and forwards it to the console.

notice | **info**} **console**		
syslog output priority {**auth** | **authpriv** | **kern** | **local0** | **local1** | **local2** | **local3** | **local4** | **local5** | **local6** | **local7** | **syslog** | **user**} {**emerg** | **alert** | **crit** | **err** | **warning** | **notice** | **info**} **local** {**volatile** | **non-volatile**}		Generates a user-defined syslog message with a priority in the system memory. volatile: deletes a syslog message after restart. non-volatile: reserves a syslog message.
syslog output priority {**auth** | **authpriv** | **kern** | **local0** | **local1** | **local2** | **local3** | **local4** | **local5** | **local6** | **local7** | **syslog** | **user**} {**emerg** | **alert** | **crit** | **err** | **warning** | **notice** | **info**} **remote** {*A.B.C.D* | *X:X::X:X*} [**vrf** *VRFNAME*]		Generates a user-defined syslog message with a priority and forwards it to a remote host.

To disable a user-defined syslog output level, use the following command.

Command	Mode	Description
no syslog output priority {**auth** | **authpriv** | **kern** | **local0** | **local1** | **local2** | **local3** | **local4** | **local5** | **local6** | **local7** | **syslog** | **user**} {**emerg** | **alert** | **crit** | **err** | **warning** | **notice** | **info**} **console**	Global	Deletes a specified user-defined syslog output level with a priority.
no syslog output priority {**auth** | **authpriv** | **kern** | **local0** | **local1** | **local2** | **local3** | **local4** | **local5** | **local6** | **local7** | **syslog** | **user**} {**emerg** | **alert** | **crit** | **err** | **warning** | **notice** | **info**} **local** {**volatile** | **non-volatile**}		
no syslog output priority {**auth** | **authpriv** | **kern** | **local0** | **local1** | **local2** | **local3** | **local4** | **local5** | **local6** | **local7** | **syslog** | **user**} {**emerg** | **alert** | **crit** | **err** | **warning** | **notice** | **info**} **remote** {*A.B.C.D* | *X:X::X:X*}		

Syslog Index Level with a Priority

To set a user-defined syslog message index level with a priority, use the following command.

Command	Mode	Description
syslog index {**system** | **physical-entity** | **dhcp** | **filter** | **gpon** | **loop-detect** | **snmp**} *INDEX* **priority** {**emerg** | **alert** | **crit** | **err** | **warning** | **notice** | **info** | **debug**}	Global	Generates a user-defined syslog message index with a priority
no syslog index {**system** |		Deletes a specified user-defined syslog nessage index

physical-entity | **dhcp** | **filter** | **gpon** | **loop-detect** | **snmp**} *INDEX*		level with a priority.

To display the configuration of the syslog index, use the following command.

Command	Mode	Description
show syslog index	Enable Global Bridge	Shows the information of syslog message index
show syslog index {**system** | **physical-entity** | **dhcp** | **filter** | **gpon** | **loop-detect** | **snmp**} [*INDEX*]		Shows the syslog index information of each parameter

i

The order of priority is **emergency** > **alert** > **critical** > **error** > **warning** > **notice** > **info** > **debug**. If you set a specific level of syslog output, you will receive only a syslog message for selected level or higher. If you want receive a syslog message for all the levels, you need to set the level to **debug**.

The following is an example of configuring syslog message to send all logs higher than notice to remote host 10.1.1.1 and configuring local1.info to transmit to console.

```
SWITCH(config)# syslog output notice remote 10.1.1.1
SWITCH(config)# syslog output priority local1 info console
SWITCH(config)# show syslog
System logger on running!

info                local volatile
info                local non-volatile
notice              remote 10.1.1.1
local1.info         console
SWITCH(config)#
```

7.4.2 Facility Code

You can set a facility code of the generated syslog message to send them remote syslog server. This code make a syslog message distinguished from others, so network administrator can handle various syslog messages efficiently. Facility code is only used with syslog messages to send to remote syslog server.

To set a facility code, use the following command.

Command	Mode	Description
syslog local-code <0-7>	Global	Sets a facility code.
no syslog local-code		Deletes a specified facility code.

The following is an example of configuring priority of all syslog messages which is transmitted to remote host 10.1.1.1, as the facility code 0.

```
SWITCH(config)# syslog output err remote 10.1.1.1
SWITCH(config)# syslog local-code 0
SWITCH(config)# show syslog
System logger on running!

info                    local volatile
info                    local non-volatile
err                     remote 10.1.1.1
local_code              0
SWITCH(config)#
```

7.4.3 Syslog Bind Address

You can specify an IP address to attach to the syslog message for its identity. To specify the IP address to bind to a syslog message, use the following command.

Command	Mode	Description
syslog bind-address {*A.B.C.D* | *X:X::X:X*}	Global	Specifies the IP address to bind to a syslog message.
no syslog bind-address		Deletes a specified IP address.

7.4.4 Debug Message for Remote Terminal

To display a syslog debug message to a remote terminal, use the following command.

Command	Mode	Description
terminal monitor	Enable	Enables the terminal monitor function.
no terminal monitor		Disables the terminal monitor function.

i This function is not operational in the local console.

7.4.5 Disabling Syslog

To disable the syslog, use the following command.

Command	Mode	Description
no syslog	Global	Disables the syslog.

i The syslog is enabled by default.

7.4.6 Syslog Local Message Configuration

To configure the volatile size of syslog message, use the following command.

Command	Mode	Description

syslog local volatile size <1-128>	Enable Global Bridge	Configures the volatile size of syslog message. volatile: removes the syslog messages after restart. 1-128: buffer size to save (kbytes)
no syslog local volatile		Removes the local volatile size.

To display the received syslog message in the system memory, use the following command.

Command	Mode	Description
show syslog local {**volatile** | **non-volatile**} [*NUMBER*]	Enable Global Bridge	Shows the received syslog messages. volatile: removes the syslog messages after restart. non-volatile: reserves the syslog messages. NUMBER: shows the last N syslog messages.
show syslog local {**volatile** | **non-volatile**} **reverse**		Shows the received syslog messages in the reverse order.
clear syslog local {**volatile** | **non-volatile**}		Removes the received syslog messages.

7.4.7 Displaying Syslog Status

To display the saved syslog status, use the following command.

Command	Mode	Description
show syslog	Enable Global Bridge	Shows the configuration of the syslog.
show syslog {**volatile** | **non-volatile**} **information**		Shows the usage of the area where the received syslog messages are stored. volatile: the area for volatile syslog messages non-volatile: the area for non-volatile syslog messages
show syslog max-size	Enable Global	

7.5 Rule and QoS

The OLT provides a rule and QoS feature for traffic management. The rule classifies incoming traffic, and then processes the traffic according to user-defined policies. You can use the physical port, 802.1p priority (CoS), VLAN ID, DSCP, and so on to classify incoming packets.

You can configure the policy in order to change some data fields within a packet or to relay packets to a mirror monitor by a rule. QoS (Quality of Service) is one of useful functions to provide more reliable service for traffic flow control. It is very serviceable to prevent overloading and delaying or failing of sending traffic by giving priority to traffic.

QoS can give priority to specific traffic by basically offering higher priority to the traffic or lower priority to the others.

When processing traffic, the traffic is usually supposed to be processed in time-order like first in, first out. This way, not processing specific traffic first, might cause undesired traffic loss in case of traffic overloading. However, in case of overloading traffic, QoS can apply processing order to traffic by reorganizing priorities according to its importance. By favor of QoS, you can predict network performance in advance and manage bandwidth more efficiently.

The QoS provides the following benefits:

Control over network resources

Bandwidth, delay and packet loss can be effectively controlled by QoS feature. The network administrator can limit the bandwidth for non-critical applications (such as FTP file transfers), so that other applications have a greater amount of bandwidth available to them.

Effective use of resources

An effective use of network resorces can support guaranteed bandwidth to a few critical applications to ensure reliable application performance. QoS ensures that the most important and critical traffic is transmitted immediately without starvation.

Customized service

QoS helps the internet service providers provide differentiated services for their customers of the network. It allocates guaranteed bandwidth to more important applications that produce real-time traffic, such as voice, video and audio.

Traffic Prioritization

As you deploly QoS, it guarantees bandwidth and reduces delay time to ensure the applications can transmit the packets properly by handling the traffic with higher priority than regular traffic.

7.5.1 How to Operate QoS

QoS operation is briefly described as below.

Incoming packets are classified by configured conditions, and then processed by packet counter and rate-limiting on specific policer. After marking and remarking action, the switch transmits those classified and processed packets via a given scheduling algorithm.

Fig. 7.1 shows the simple procedure of QoS operation.

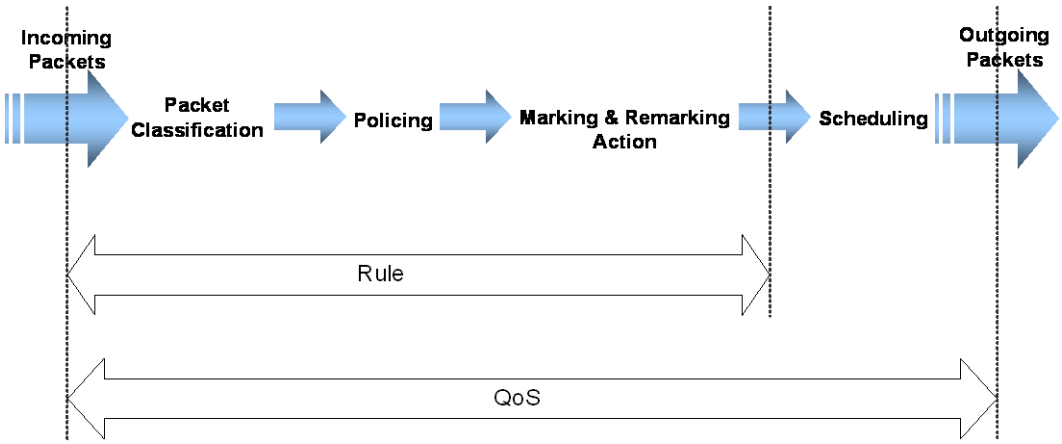


Fig. 7.1 Procedure of QoS operation

The structure of Rule has 4 types of categories with different roles for QoS.

- **Flow**
  Defines traffic classification criterias such as L3 source and destination IP address, L2 source and destination MAC address, Ethernet type, length, Class of Service (CoS), Differentiated Services Code Point (DSCP) and so on. A unique name needs to be assigned to each flow.

- **Class**
  Includes more than 2 flows for the efficient traffic management in the application of rule to this set of flows. Additionally, a unique name needs to be assigned to each class.

- **Policer**
  Defines the packet counter and rate-limit. The policer adjusts how and what is to be classified within transmitted packets.
  − **packet counter** calculates the classified packets for identifying a flow.
  − **rate-limit** defines which packets conform to or exceed the given rate.

- **Policy**
  Configures the policy classifying the action(s) to be performed if the configured rule classification fits transmitted packet(s). It cannot only include a specified Flow, Class or Policer but also set marking/remarking according to the various parameters such as CoS and DSCP which determine the rule action or priority of packets.
  − **mirror** transmits the classified traffic to the monitor port.
  − **redirect** transmits the classified traffic to the specified port.

- **permit** allows traffic matching given characteristics.
- **deny** blocks traffic matching given characteristics.
- **copy-to-cpu** duplicates the profile of classified packets and sends a copy to CPU packets filtering.

• **Scheduling Algorithm**
To handle traffic, you need to configure differently processing orders of traffic by using scheduling algorithms. The OLT provides:
- Strict Priority Queuing (SP)
- Deficit Round Robin (DRR)
- Weighted Round Robin (WRR)

An already applied rule cannot be modified. It needs to be deleted and then created again with changed values.

Weight can be used to additionally adjust the scheduling mode per queue in DWRR mode. Weight controls the scheduling precedence of the internal packet queues.

Fig. 7.2 shows the relationship of Flow, Class, Policer and Policy on basic structure of Rule.

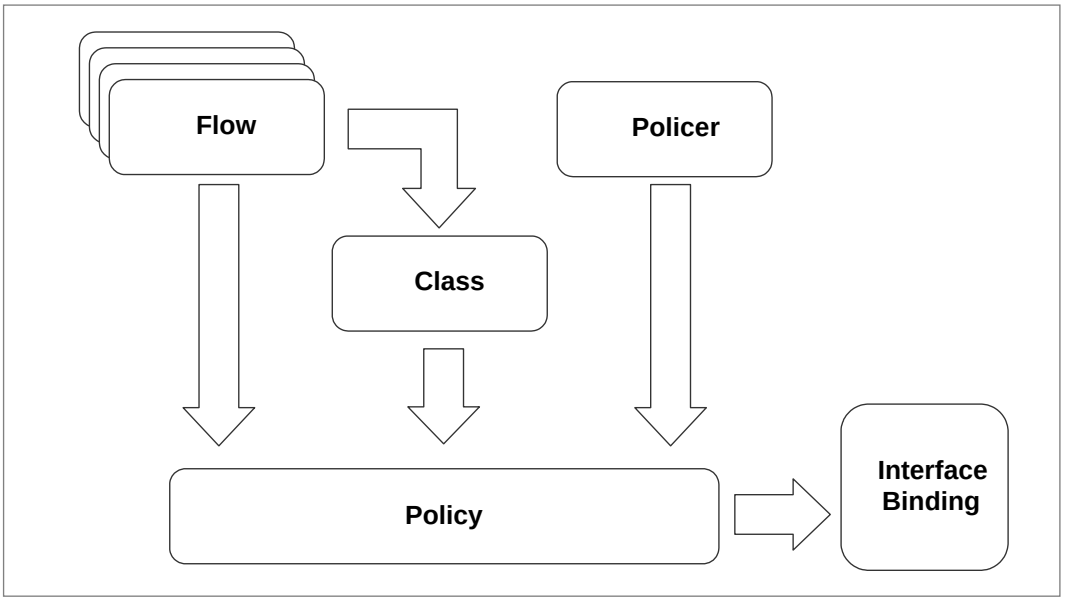


Fig. 7.2 Structure of Rule

You can simply manage more than 2 Flows through one Class. Flow or Class and Policer can be implemented by one policy.

Both Flow and Class cannot belong to one policy together. It means that one policy can include only one either Flow or Class. However, a single flow or class can belong to multiple policies. Otherwise, only one policer can belong to one policy.

7.5.2 Packet Classification

Packet classification features allow traffic to be partitioned into multiple priority levels, or classes of service. In *Flow Configuration* mode, you can set packet classification criterias

via flow, which is with unique name. If you specify the value of parameters, the OLT classifies the packets corresponding to the parameters.

7.5.2.1 Flow Creation

The packet classification involves a traffic descriptor to categorize a packet within a specific flow for QoS handling in the network. You need to open *Flow Configuration* mode first to classify the packets. To open *Flow Configuration* mode, use the following command.

Command	Mode	Description
flow *NAME* **create**	Global	Creates a flow and opens *Flow Configuration* mode. NAME: flow name.

After opening *Flow Configuration* mode, the prompt changes from SWITCH(config)# to SWITCH(config-flow[NAME])#.

To delete the configured Flow or all Flows, use the following command.

Command	Mode	Description
no flow *NAME*	Global	Deletes a specified flow.
no flow all		Deletes all flows.

After opening *Flow Configuration* mode, a flow can be configured by user. The packet classification can be configured for each flow.

- The flow name must be unique. Its size is limited to 32 significant characters.
- The flow name cannot start with the alphabet “a” or “A”.
- The order in which the following configuration commands are entered is arbitrary.
- The configuration of a flow being configured can be changed as often as wanted until the **apply** command is entered.
- Use the **show flow-profile** command to display the configuration entered up to now.

You cannot create the flow name which started with alphabet ‘a’ If you try to make a flow name started with alphabet ‘a’, the error message will display.

7.5.2.2 Configuring Flow

The packet classification condition needs to be defined. You can classify the packets via MAC address, IP address, Ethernet type, CoS, DSCP etc. To specify a packet-classifying pattern with source/destination IP address or MAC address, use the following command.

Command	Mode	Description
ip {*A.B.C.D* | *A.B.C.D/M* | **any**} {*A.B.C.D* | *A.B.C.D/M* | **any**} [<0-255>]	Flow	Classifies an IP address. A.B.C.D: source/destination IP address A.B.C.D/M: source/destination IP address with mask any: any source/destination IP address 0-255: IP protocol number

Command	Mode	Description
ip {*A.B.C.D* | *A.B.C.D/M* | **any**} {*A.B.C.D* | *A.B.C.D/M* | **any**} **icmp**		Classifies an IP protocol (ICMP). A.B.C.D: source/destination IP address A.B.C.D/M: source/destination IP address with mask any: any source/destination IP address
ip {*A.B.C.D* | *A.B.C.D/M* | **any**} {*A.B.C.D* | *A.B.C.D/M* | **any**} {**esp** | **ah** | **gre** | **ipv6**}		Classifies an IP protocol esp: Encapsulating security payload header ah: Authentication header gre: Generic routing encapsulation ipv6: IPv6 encapsulation
ip {*A.B.C.D* | *A.B.C.D/M* | **any**} {*A.B.C.D* | *A.B.C.D/M* | **any**} **icmp** {<0-255> | **any**} {<0-255> | **any**}		Classifies an IP protocol (ICMP). A.B.C.D: source/destination IP address A.B.C.D/M: source/destination IP address with mask any: any source/destination IP address 0-255: ICMP message type number 0-255: ICMP message code number
ip {*A.B.C.D* | *A.B.C.D/M* | **any**} {*A.B.C.D* | *A.B.C.D/M* | **any**} {**tcp** | **udp**}		Classifies an IP protocol (TCP/UDP). A.B.C.D: source/destination IP address A.B.C.D/M: source/destination IP address with mask any: any source/destination IP address
ip {*A.B.C.D* | *A.B.C.D/M* | **any**} {*A.B.C.D* | *A.B.C.D/M* | **any**} {**tcp** | **udp**} {<1-65535> | **any**} {<1-65535> | **any**}		Classifies an IP protocol (TCP/UDP). A.B.C.D: source/destination IP address A.B.C.D/M: source/destination IP address with mask any: any source/destination IP address 0-65535: TCP/UDP source/destination port range any: any TCP/UDP source/destination port
ip {*A.B.C.D* | *A.B.C.D/M* | **any**} {*A.B.C.D* | *A.B.C.D/M* | **any**} **tcp** {<1-65535> | **any**} {<1-65535> | **any**} {*TCP-FLAG* | **any**}		Classifies an IP protocol (TCP). A.B.C.D: source/destination IP address A.B.C.D/M: source/destination IP address with mask any: any source/destination IP address 0-65535: TCP source/destination port range any: any TCP source/destination port TCP-FLAG: TCP flag (e.g. S(SYN), F(FIN)) any: any TCP flag
mac {*SRC-MAC-ADDR* | *SRC-MAC-ADDR/M* | **any**} {*DST-MAC-ADDR* | *DST-MACADDR*/M | **any**}		Classifies MAC address. SRC-MAC-ADDR: source MAC address DST-MAC-ADDR: destination MAC address SRC/DST-MACADDR/M: source/destination MAC address with mask bit any: any source/destination MAC address (ignore)
mac da-found		Classifies destination MAC addresses learned on MAC table.
mac da-not-found		Classifies destination MAC addresses not learned on MAC table.

When specifying a source and destination IP address as a packet-classifying pattern, the destination IP address must be after the source IP address.

To specify a packet-classifying pattern with IPv6 address, use the following command.

Command	Mode	Description
ipv6 { *X:X::X:X* | *X:X::X:X/M* | **any**} {*X:X::X:X* |*X:X::X:X/M* | **any**} [<0-255>]	Flow	Classifies an IPv6 address. X:X::X:X : source/destination IPv6 address X:X::X:X/M: source/destination IPv6 address with mask any: any source/destination IPv6 address 0-255: IP protocol number
ipv6 { *X:X::X:X* | *X:X::X:X/M* | **any**} { *X:X::X:X* | *X:X::X:X/M* | **any**} {**esp** | **ah** | **gre** | **ipv6**}		Classifies an Ipv6 protocol X:X::X:X : source/destination IPv6 address X:X::X:X/M: source/destination IPv6 address with mask esp: Encapsulating security payload header ah: Authentication header gre: Generic routing encapsulation ipv6: IPv6 encapsulation
ipv6 { *X:X::X:X* | *X:X::X:X/M* | **any**} {*X:X::X:X* |*X:X::X:X/M* | **any**} **icmp**		Classifies an IP protocol (ICMP). X:X::X:X : source/destination IPv6 address X:X::X:X/M: source/destination IPv6 address with mask any: any source/destination IPv6 address
ipv6 { *X:X::X:X* | *X:X::X:X/M* | **any**} {*X:X::X:X* |*X:X::X:X/M* | **any**} **icmp** {<0-255> | **any**} {<0-255> | **any**}		
ipv6 { *X:X::X:X* | *X:X::X:X/M* | **any**} {*X:X::X:X* |*X:X::X:X/M* | **any**} {**tcp** | **udp**}		Classifies an IP protocol (TCP/UDP). X:X::X:X : source/destination IPv6 address X:X::X:X/M: source/destination IPv6 address with mask any: any source/destination IPv6 address
ipv6 { *X:X::X:X* | *X:X::X:X/M* | **any**} {*X:X::X:X* |*X:X::X:X/M* | **any**} **tcp** {<1-65535> | **any**} {<1-65535> | **any**} [*TCP_FLAG* | **any**]		Classifies an IP protocol (TCP/UDP). X:X::X:X : source/destination IPv6 address X:X::X:X/M: source/destination IPv6 address with mask any: any source/destination IPv6 address 0-65535: TCP/UDP port range any: any TCP/UDP port TCP_FLAG: TCP flag vlaue
ipv6 { *X:X::X:X* | *X:X::X:X/M* | **any**} {*X:X::X:X* |*X:X::X:X/M* | **any**} **udp** {<1-65535> | **any**} {<1-65535> | **any**}		

To specify a packet-classifying pattern with various parameters (DSCP, CoS, ToS, IP precedence, packet length, Ethernet type, IP header), use the following command.

Command	Mode	Description
dscp {<0-63> | **any**}	Flow	Classifies a DSCP value. 0-63: DSCP value any: any DSCP (ignore)
cos {<0-7> | **any**}		Classifies an 802.1p priority. 0-7: 802.1p priority value any: any 802.1p priority value (ignore)
tos {<0-255> | **any**}		Classifies all ToS field. 0-255: ToS value

		any: any ToS value (ignore)
ip-precedence {<0-7> | **any**}		Classifies IP precedence. 0-7: IP precedence value any: any IP precedence value (ignore)
length {<21-65535> | **any**}		Classifies a packet length. 21-65535: IP packet length any: any IP packet length (ignore)
ethtype {*TYPE-NUM* | **arp** | **any**}		Classifies the Ethernet type. TYPE-NUM: Ethernet type field (hex, e.g. 0800 for IPv4) arp: address resolution protocol any: any Ethertype (ignore)
ip header-error		Classifies the IP header-error.
ip header-length <1-15>		Classifies the IP header-length. 1-15: IP header-length value
traffic-class {<0-255> | **any**}		Classifies the packet's traffic-class filed value.
flow-label {<0-65535> | **any**}		Classifies the packet's flow-label filed value.

ip header-error command can be used only when specifying a source and destination IP address as a packet-classifying pattern.

To delete a specified packet-classifying pattern, use the following command.

Command	Mode	Description
no cos	Flow	Deletes a specified packet-classifying pattern for each option.
no dscp		
no tos		
no length		
no ip-precedence		
no ethtype		
no mac		
no mac da-found		
no mac da-not-found		
no ip		
no ipv6		
no ip header-length		
no ip header-error		
no traffic-class		
no flow-label		

7.5.2.3 Applying and modifying Flow

After configuring a flow using the above commands, apply it to the system with the following command. If you do not apply the flow to the system, all specified configurations on *Flow Configuration* mode will be lost.

To save and apply a flow, use the following command.

Command	Mode	Description
apply	Flow	Applies a flow to the system.

To modify a flow, use the following command.

Command	Mode	Description
flow *NAME* **modify**	Global	Modifies a flow, enter a flow name.

i You should save and apply the flow to system whenever you modify or configure the flow.

7.5.2.4 Class Creation

A class is a set of flows. More than 2 flows can belong to one class. You can simply handle and configure the packets on several flows at once.

To create a class including more than 2 flows, use the following command.

Command	Mode	Description
class *NAME* **flow** *FLOW1* [*FLOW2*] [*FLOW3*]···	Global	Creates a class including more than 2 flows. NAME: class name FLOW: flow name

To delete configured class or all classes, use the following command.

Command	Mode	Description
no class all	Global	Deletes all classes.
no class *NAME*		Deletes specified class, enter the class name.
no class *NAME* **flow** *FLOW1* [*FLOW2*] [*FLOW3*]···		Removes specified flows from class.

7.5.3 Packet Conditioning

After defining traffic classification criteria in *Flow Configuration* mode, then configure how to process the packets. The classified traffic from flow or class is being treated according to the policer configuration. On *Policer Configuration* mode, a policer enforces a rate-limiting and the packet counter for traffic. The traffic is identified via policers, which are used to define traffic conditions including rate-limit and counter. And the policy actions for the identified traffic are created with policy. One policer can belong to one policy.

7.5.3.1 Policer Creation

To configure how to handle the classified packets according to the policer settings, you need to create a policer and open *Policer Configuration* mode.

To open *Policer Configuration* mode, use the following command.

Command	Mode	Description
policer *NAME* **create**	Global	Creates a policer and opens *Policer Configuration* mode. NAME: policer name.

After opening *Policer Configuration* mode, the prompt changes from SWITCH(config)# to SWITCH(config-policer[NAME])#.

After opening *Policer Configuration* mode, a policer can be configured by user. The rate-limit, meter and packet count can be configured for each policer.

i

- The policer name must be unique. Its size is limited to 32 significant characters.
- The policer name cannot start with the alphabet “a” or “A”.
- The order in which the following configuration commands are entered is arbitrary.
- The configuration of a polcer being configured can be changed as often as wanted until the **apply** command is entered.
- Use the **show policer-profile** command to display the configuration entered up to now.

To delete configured policer or all policers, use the following command.

Command	Mode	Description
no policer *NAME*	Global	Deletes a policer, enter a policer name.
no policer all		Deletes all policers.

7.5.3.2 Packet Counter

The packet counter function provides information on the total number of packets that the rule received and analyzed. This feature allows you to know the type of packets transmitted in the system according to rule configuration.

To count the number of packets matching to corresponding policer, use the following command.

Command	Mode	Description
counter	Policer	Enables a packet counter function.
no counter		Disables a packet counter function.

To reset a collected policy counter, use the following command.

Command	Mode	Description
clear policy counter { *NAME* | **all**}	Enable	Resets a collected policy counter.

	Global Bridge	

To display the number of packets on each rule, use the following command.

Command	Mode	Description
show flow statistics	Enable Global	Shows a collected flow counter.
show class statistics		Shows a collected class counter.
show policer statistics		Shows a collected policer counter.
show policy statistics		Shows a collected policy counter.

7.5.3.3 Rate-limit

You can configure the rate limit in kbps unit for the classified packets and control the bandwidth. To set the bandwidth of classified packets in specified policer, use the following command.

Command	Mode	Description
rate-limit *BANDWIDTH*	Policer	Sets the bandwidth for classified packets belonging to specified policer (unit: kbps)
no rate-limit		Deletes the configured bandwidth for classified packets of specified policer.

7.5.3.4 Applying and modifying Policer

After configuring a policer using the above commands, apply it to the system with the following command. If you do not apply the policer to the system, all specified configurations on *Policer Configuration* mode will be lost.

To save and apply a policer, use the following command.

Command	Mode	Description
apply	Policer	Applies a policer to the system.

To modify a policer, use the following command.

Command	Mode	Description
policer *NAME* **modify**	Global	Modifies a policer, enter a policer name.

7.5.4 Rule Action

7.5.4.1 Policy Creation

To configure a policy, you need to open *Policy Configuration* mode first. To open *Policy Configuration* mode, use the following command.

Command	Mode	Description
policy *NAME* **create**	Global	Creates a policy and opens *Policy Configuration* mode. NAME: policy name.

After opening *Policy Configuration* mode, the prompt changes from SWITCH(config)# to SWITCH(config-policy[NAME])#.

To delete configured policy or all policies, use the following command.

Command	Mode	Description
no policy *NAME*	Global	Deletes a policy, enter a policy name.
no policy all		Deletes all policies.

After opening *Policy Configuration* mode, a policy can be configured by user. The rule priority and rule action(s) can be configured for each policy.

- The policy name must be unique. Its size is limited to 32 significant characters.
- The policy name cannot start with the alphabet “a” or “A”.
- The order in which the following configuration commands are entered is arbitrary.
- The configuration of a policy being configured can be changed as often as wanted until the **apply** command is entered.
- Use the **show policy-profile** command to display the configuration entered up to now.

If you already create the policy, you need to include specified flow or class and policer to specify the rule action for the packets matching configured classifying patterns on flow or class and policer.

To include specific flow or class and policer in policy, use the following command.

Command	Mode	Description
include-flow *NAME*	Policy	Includes specified flow in policy. NAME:flow name
include-class *NAME*		Includes specified class in policy. NAME:class name
include-policer *NAME*		Includes specified policer in policy. NAME:policer name

One policy is not able to include both flow and class at the same time. Either flow or class can belong to one policy.

Only one policer can belong to one policy.

To remove flow or class, policer from the policy, use the following command.

Command	Mode	Description
no include-flow	Policy	Removes the flow from policy.
no include-class		Removes the class from policy.

no include-policer		Removes the policer from policy.

7.5.4.2 Metering

Meters measure the temporal state of a flow or a set of flows against a traffic profile. In this event, a meter might be used to trigger real-time traffic conditioning actions (e.g. marking, policing, or shaping).

Typical parameters of a traffic profile are:

- Committed Information Rate (CIR)
- Peak Information Rate (PIR)
- Committed Burst Size (CBS)
- Excess Burst Size (EBS)
- Peak Burst Size (PBS)

A typical meter measures the rate at which traffic stream passes it. Its rate estimation depends upon the flow state kept by the meter. There is a time constraint during which if the flow state is transferred from the old switch to the new switch, then it is effective in estimating the rate at the new switch as if though no transfer of flow has happened.

The OLT provides Token Bucket (srTCM and trTCM) meters.

Token Bucket

The token bucket is a control mechanism that transmits traffic by tokens in the bucket. The tokens are consumed by transmitting traffic and regenerated at the given rate. If all tokens in the bucket are consumed out, traffic cannot be transmitted any more; a flow can transmit traffic up to its peak burst rate. The transmitting cost and regenerating rate of tokens are configurable.

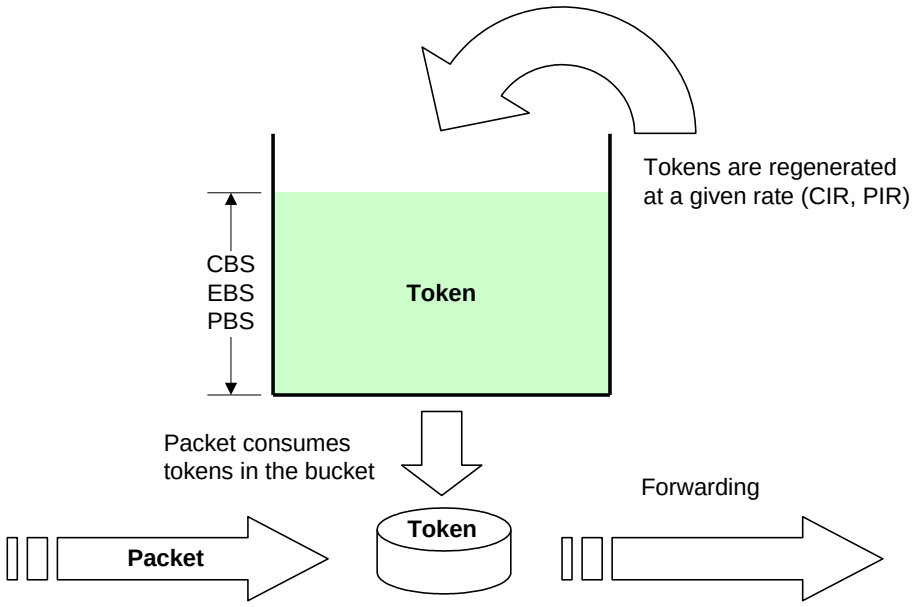


Fig. 7.3 Token Bucket Meter

Single Rate Three Color Marker (srTCM)

The srTCM meters an IP packet stream and marks its packet the one among green, yellow, and red using Committed Information Rate (CIR) and two associated burst sizes, Committed Burst Size (CBS) and Excess Burst Size (EBS). A packet is marked green if it does not exceed the CBS, yellow if it exceeds the CBS, but not the EBS, and red otherwise. The srTCM is useful for ingress policing of a service, where only the length, not the peak rate, of the burst determines service eligibility.

CIR is the regenerating rate of tokens measured in bytes of IP packets per second. CBS and EBS are the maximum size for each token bucket, C and E, measured in bytes. Both token buckets share the common rate CIR. At least one of them (CBS and EBS) must be configured, and it is recommended that the value is larger than or equal to the size of the largest possible IP packet in the stream.

The token buckets C and E are initially full. When a packet arrives, the tokens in the bucket C are decremented by the size of that packet with the green color-marking. If no more tokens to transmit a packet remain in the bucket C, then the tokens in the bucket E are decremented by the size of that packet with the yellow color-marking. If both buckets are empty, a packet is marked red.

The following figures show the behavior of the srTCM.

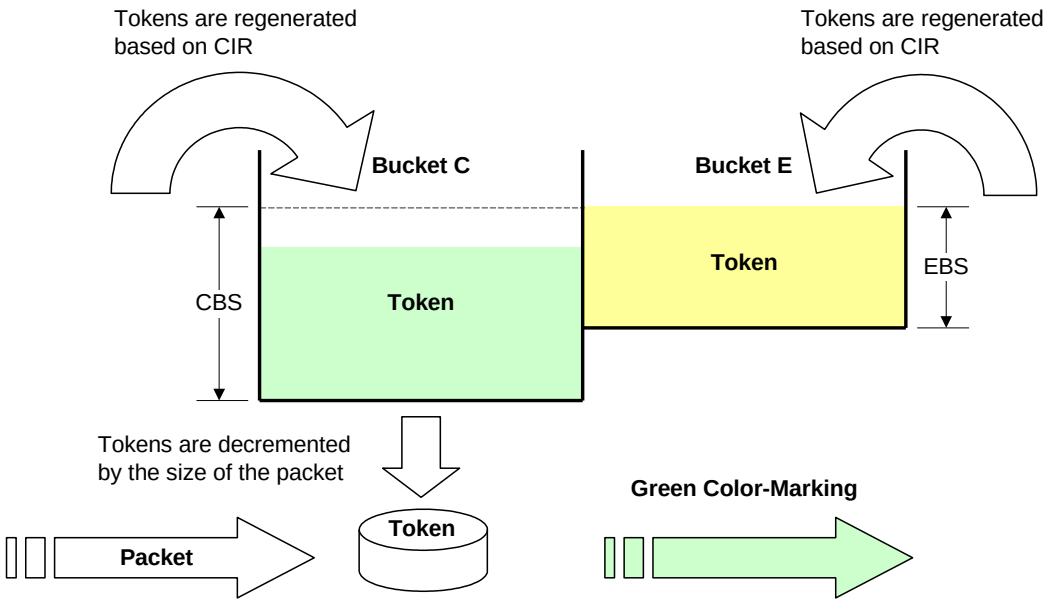


Fig. 7.4 Behavior of srTCM (1)

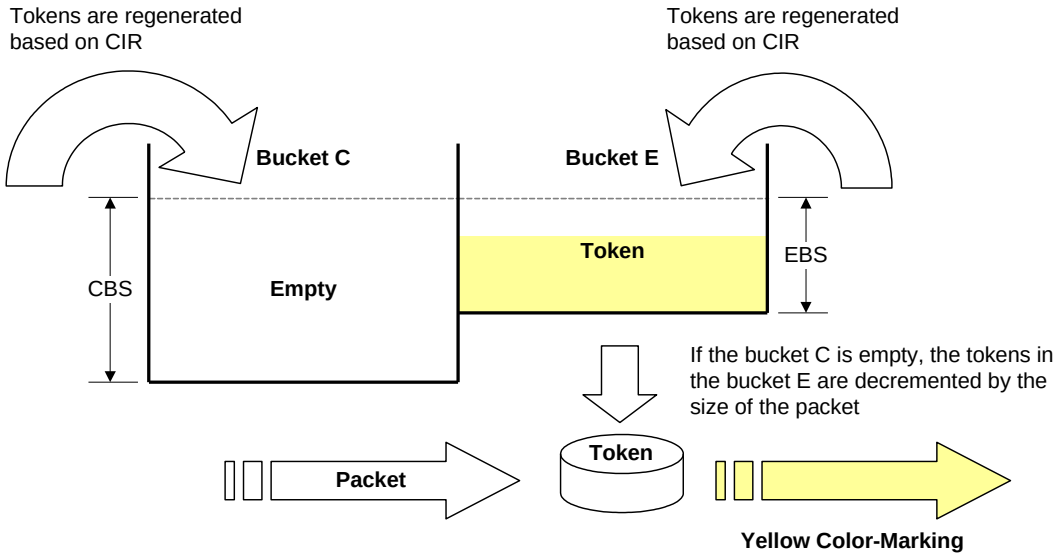


Fig. 7.5 Behavior of srTCM (2)

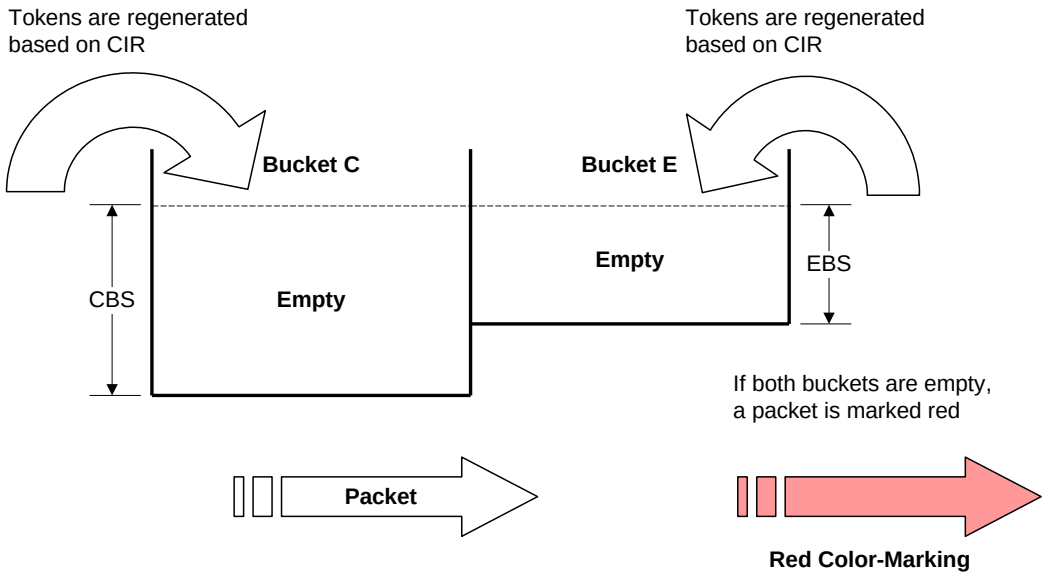


Fig. 7.6 Bahavior of srTCM (3)

Two Rate Three Color Marker (trTCM)

The trTCM meters an IP packet stream and marks its packet the one among green, yellow, and red using Peak Information Rate (PIR) and its associated Peak Burst Size (PBS) and Committed Information Rate (CIR) and its associated Committed Burst Size (CBS). A packet is marked red if it exceeds the PIR. Otherwise, it is marked either yellow or green depending on whether it exceeds or does not exceed CIR. The trTCM is useful for ingress policing of a service, where a peak rate needs to be enforced separately from a committed rate.

PIR and CIR are the regenerating rate of tokens for PBS and CBS respectively, which is measured in bytes of IP packets per second. PIR must be equal to or greater than CIR. PBS and CBS are the maximum size for each token bucket, P and C, measured in bytes. Both of them must be configured with the values equal to or greater than the size of the largest possible IP packet in the stream.

The token buckets P and C are initially full. When a packet arrives, if the tokens in the bucket P are smaller than the size of that packet, the packet is marked red. Else, if the tokens in the bucket C are smaller than the size of that packet, those are decremented by the size of that packet with the yellow color-marking. Else, if the tokens in the bucket C are larger than the size of that packet, those of both bucket P and C are decremented by the size of that packet with the green color-marking.

Note that in the trTCM algorithm, when a packet arrives, the availability of tokens in the token bucket P is checked first contrary to the srTCM; the order of color-marking is red-yellow-green.

The following figures show the behavior of the trTCM.

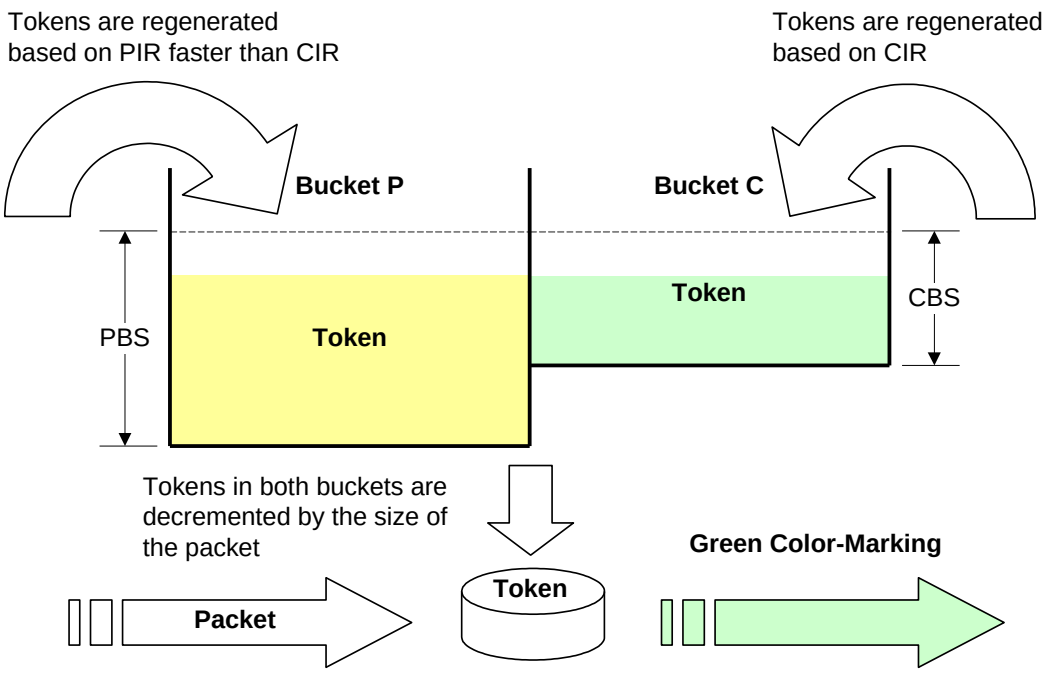


Fig. 7.7 Behavior of trTCM (1)

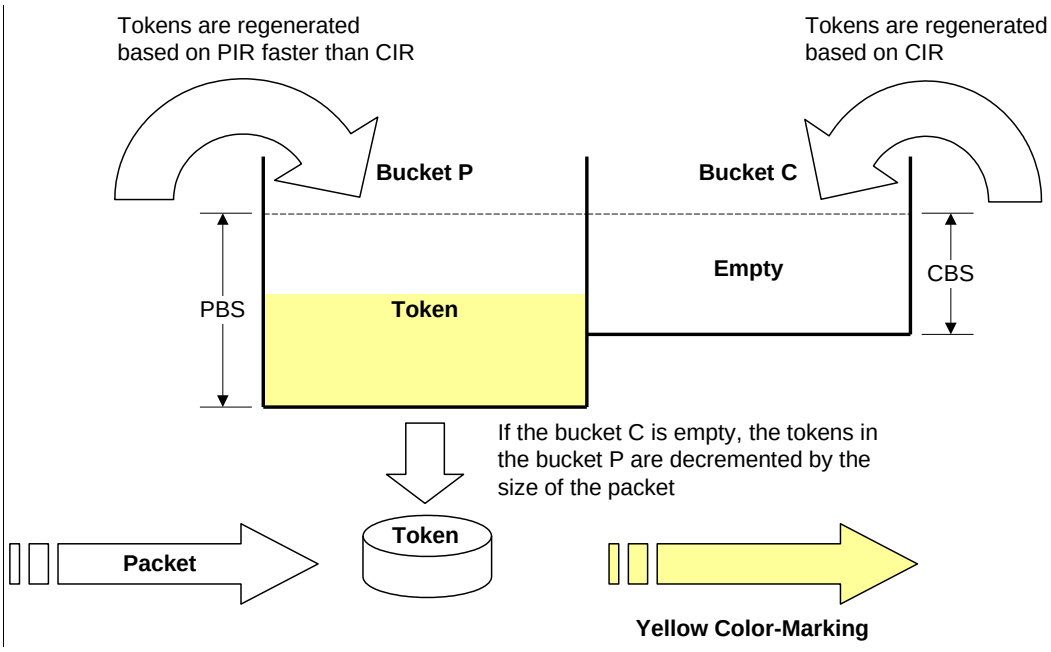


Fig. 7.8 Behavior of trTCM (2)

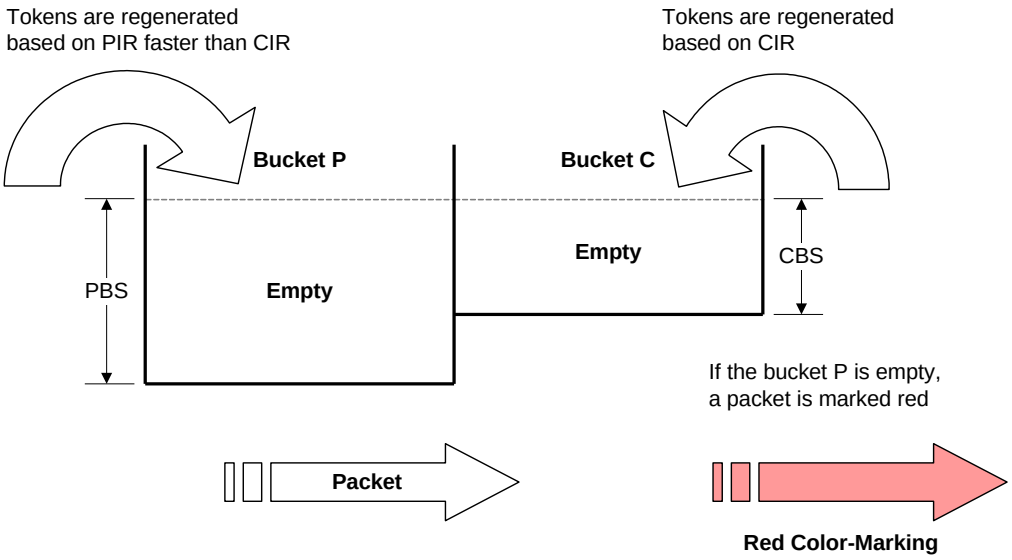


Fig. 7.9 Behavior of trTCM (3)

To set the metering mode, use the following command.

Command	Mode	Description
color mode {srtcm | trtcm} blind	Policer	Sets the metering mode. blind: color-blind mode
no color mode		Sets to the default setting.

In the color-blind mode, the meter assumes that the packet stream is uncolored. In the

i

color-aware mode the meter assumes that some preceding entity has pre-colored the incoming packet stream so that each packet is the one among green, yellow, and red.

To specify the value for metering parameters, use the following command.

Command	Mode	Description
color cir *BANDWIDTH* **cbs** *BURST*	Policer	Specifies CIR and CBS. BANDWIDTH: regenerating rate of token (unit: Kbps) BURST: maximum size of token bucket (unit: byte)
color pir *BANDWIDTH* **pbs** *BURST*		Specifies PIR and PBS. (trTCM only)
color ebs *BURST*		Specifies EBS. (srTCM only)

To configure DSCP values for the colored-packets, use the following command.

Command	Mode	Description
color dscp <0-63> {**green** | **yellow** | **red** }	Policer	Sets DSCP values for each colored packets.

In the color-blind mode, you can configure all green-colored, red-colored or yellow-colored packets to discard. To configure the meter to discard all green-colored, red-colored or yellow-colored packets, use the following command.

Command	Mode	Description
color {**green** | **red** | **yellow**} **action drop**	Policer	Configures the meter to discard green, red-colored or yellow-colored packets.
no color {**green** | **red** | **yellow**} **action**		Deletes the meter configured to permit green, red-colored or yellow-colored packets.

In the color-aware mode, you can configure the DSCP remarking for red-colored packets or yellow-colored packets only. To configure DSCP remarking, use the following command.

Command	Mode	Description
color {**green** | **red** | **yellow**} **action marking**	Policer	Configures DSCP remarking for green, red-colored or yellow-colored packets.
color {**green** | **red** | **yellow**} **action marking drop-precedence** {**red** | **yellow** | **green**}		Configures DSCP remarking and drop precedence for green, red-colored or yellow-colored packets.
color {**green** | **red** | **yellow**} **action marking-cos** <0-7>		Configures IEEE 802.1p priority.

7.5.4.3 Policy Priority

If rules that are more than two match the same packet then the rule having a higher priority will be processed first. To set a priority for a policy, use the following command.

Command	Mode	Description
priority {**low** | **medium** | **high** | **high-middle** | **highest**}	Policy	Sets a priority for a policy. (default: low)

7.5.4.4 Policy Action

To specify the rule action for the packets matching configured classifying patterns, use the following command.

Command	Mode	Description
action match deny	Policy	Denies the classified packets.
action match permit		Permits the classified packets.
action match redirect *PORT*		Redirects the classified packets to specified port. PORT: port number
action match mirror		Sends a copy of classified packets to mirror monitoring port.
action match vlan *VLANS*		Specifies a VLAN ID of classified packets. VLANS: VLAN ID (1-4094)
action match copy-to-cpu		Sends classified packets to CPU.
action match donot-copy-to-cpu		Do not send classified packets to CPU.
action match dmac *DST-MAC-ADDR*		Overwrites a specified destination MAC address.
action match egress filter *PORT*		Deletes a specified egress port.
action match egress port *PORT*		Overwrites a specified egress port

To delete a specified rule action, use the following command.

Command	Mode	Description
no action match deny	Policy	Deletes a specified rule action.
no action match permit		
no action match redirect		
no action match mirror		
no action match vlan		
no action match copy-to-cpu		
no action match donot		
no action match dmac		
no action match egress		

7.5.4.5 Setting CoS and ToS values

To specify a CoS or ToS value for a matching condition, use the following command.

Command	Mode	Description
action match cos <0-7>	Policy	Configures the 802.1p class of service value. 0-7: CoS value

overwrite		overwrite: changes 802.1p class of service value with the one you set
action match cos same-as-tos overwrite		Changes the 802.1p CoS field in the packet with an IP ToS precedence value
action match cpu-cos <0-7>		Configures the CPU rx class of service value. 0-7: CoS value
action match ip-precedence <0-7>		Configures the IP ToS precedence value in the packet. 0-7: ToS precedence value
action match ip-precedence same-as-cos		Changes the IP ToS precedence value in the packet with an 802.1p CoS value.

To delete the CoS or ToS matching condition, use the following command.

Command	Mode	Description
no action match cos [**overwrite**]	Policy	Deletes the CoS or ToS matching condition.
no action match cpu-cos		
no action match cos same-as-tos overwrite		
no action match ip-precedence		
no action match ip-precedence same-as-cos		

7.5.4.6 Attaching a Policy to an interface

After you configure a rule including the packet classification, policing and rule action, you should attach a policy to an interface and to specify port or VLAN in which the policy should be applied. If you do not specify an interface for rule, rule does not work properly.

To attach a policy to an interface, use the following command.

Command	Mode	Description
interface-binding port ingress {*PORTS* | **cpu** | **any** }	Policy	Attaches the policy to a specified ingress port or any port. PORTS: port number
interface-binding port egress {*PORTS* | **cpu** | **any** }		Attaches the policy to a specified egress port or any port. PORTS: port number
interface-binding vlan { *VLANS* | **any** }		Attaches the policy to a specified vlan or any vlan. VLANS: VLAN ID (1-4094)

To detach a policy from an interface, use the following command.

Command	Mode	Description
no interface-binding port ingress [*PORTS*]	Policy	Removes an attached policy from ingress port.
no interface-binding port egress [*PORTS*]		Removes an attached policy from egress port.
no interface-binding vlan		Removes an attached policy from vlan.

7.5.4.7 Applying and Modifying Policy

After configuring a policy using the above commands, apply it to the system with the following command. If you do not apply the policy to the system, all specified configurations from *Policy Configuration* mode will be lost.

To save and apply a policy, use the following command.

Command	Mode	Description
apply	policy	Applies a policy to the system.

To modify a policy, use the following command.

Command	Mode	Description
policy *NAME* **modify**	Global	Modifies a policy, enter a policy name.

7.5.5 Displaying Rule

To show a rule profile configured by user, use the follwing command.

Command	Mode	Description
show flow-profile	Flow	Shows a profile of flow.
show policer-profile	Policer	Shows a profile of policer.
show policy-profile	Policy	Shows a profile of policy.

To dispaly a certain rule by its name or a specific rule of a certain type, use the following command.

Command	Mode	Description
show { **flow** | **class** | **policer** | **policy** } [*NAME*]	View Enable Global Bridge	Shows the information relating to each rule, enter a rule name.
show { **flow** | **class** | **policer** | **policy** } **detail** [*NAME*]		
show running-config { **flow** | **policer** | **policy** }	All	Shows all configurations of each rule

7.5.6 Admin Rule

For the OLT, it is possible to block a specific service connection like telnet, FTP, ICMP, etc with an admin rule function.

7.5.6.1 Creating Admin Flow for packet classification

To classify packets by a specific admin flow for the OLT, you need to open *Admin-Flow Configuration* mode first. To open *Admin-Flow Configuration* mode, use the following command.

Command	Mode	Description
flow admin *NAME* **create**	Global	Creates an admin flow and opens *Admin-Flow Configuration* mode. NAME: admin-flow name.

After opening *Admin-Flow Configuration* mode, the prompt changes from SWITCH(config)# to SWITCH(config-admin-flow[NAME])#.

To delete configured admin flow or all admin flows, use the following command.

Command	Mode	Description
no flow admin *NAME*	Global	Deletes specified admin flow.
no flow admin all		Deletes all admin flows.

After opening *Admin-Flow Configuration* mode, an admin flow can be configured by user. The packet classification can be configured for each admin-flow.

i

- The admin-flow name must be unique. Its size is limited to 32 significant characters.
- The admin-flow name cannot start with the alphabet “a” or “A”.
- The order in which the following configuration commands are entered is arbitrary.
- The configuration of a flow being configured can be changed as often as wanted until the **apply** command is entered.
- Use the **show flow-profile admin** command to display the configuration entered up to now.

7.5.6.2 Configuring Admin Flow

You can classify the packets according to IP address, ICMP, TCP, UDP and IP header length. To specify a packet-classifying pattern, use the following command.

Command	Mode	Description
ip {*A.B.C.D* | *A.B.C.D/M* | **any**} {*A.B.C.D* | *A.B.C.D/M* | **any**} [0-255]	Admin-Flow	Classifies an IP address: A.B.C.D: source/destination IP address A.B.C.D/M: source/destination IP address with mask any: any source/destination IP address 0-255: IP protocol number
ip {*A.B.C.D* | *A.B.C.D/M* | **any**} {*A.B.C.D* | *A.B.C.D/M* | **any**} **icmp**		Classifies an IP protocol (ICMP): A.B.C.D: source/destination IP address A.B.C.D/M: source/destination IP address with mask any: any source/destination IP address
ip {*A.B.C.D* | *A.B.C.D/M* | **any**} {*A.B.C.D* | *A.B.C.D/M* | **any**} **icmp** {<0-255> | **any**} {<0-255> | **any**}		Classifies an IP protocol (ICMP): A.B.C.D: source/destination IP address A.B.C.D/M: source/destination IP address with mask

Command	Mode	Description
		any: any source/destination IP address 0-255: ICMP message type number 0-255: ICMP message code number
ip {*A.B.C.D* | *A.B.C.D/M* | **any**} {*A.B.C.D* | *A.B.C.D/M* | **any**} {**tcp** | **udp**}		Classifies an IP protocol (TCP/UDP): A.B.C.D: source/destination IP address A.B.C.D/M: source/destination IP address with mask any: any source/destination IP address
ip {*A.B.C.D* | *A.B.C.D/M* | **any**} {*A.B.C.D* | *A.B.C.D/M* | **any**} {**tcp** | **udp**} {<0-65535> | **any**} {<0-65535> | **any**}		Classifies an IP protocol (TCP/UDP): A.B.C.D: source/destination IP address A.B.C.D/M: source/destination IP address with mask any: any source/destination IP address 0-65535: TCP/UDP source/destination port number any: any TCP/UDP source/destination port
ip {*A.B.C.D* | *A.B.C.D/M* | **any**} {*A.B.C.D* | *A.B.C.D/M* | **any**} **tcp** {<0-65535> | **any**} {<0-65535> | **any**} {*TCP-FLAG* | **any**}		Classifies an IP protocol (TCP): A.B.C.D: source/destination IP address A.B.C.D/M: source/destination IP address with mask any: any source/destination IP address 0-65535: TCP source/destination port number any: any TCP source/destination port TCP-FLAG: TCP flag (e.g. S(SYN), F(FIN)) any: any TCP flag
ip header-length <1-15>		Classifies an IP header length: 1-15: IP header length value

When specifying a source and destination IP address as a packet-classifying pattern, the destination IP address must be after the source IP address.

To specify a packet-classifying pattern with IPv6 address, use the following command.

Command	Mode	Description
ipv6 { *X:X::X:X* | *X:X::X:X/M* | **any**} {*X:X::X:X* |*X:X::X:X/M* | **any**} [<0-255>]	Admin-Flow	Classifies an IPv6 address. X:X::X:X : source/destination IPv6 address X:X::X:X/M: source/destination IPv6 address with mask any: any source/destination IPv6 address 0-255: IP protocol number
ipv6 { *X:X::X:X* | *X:X::X:X/M* | **any**} {*X:X::X:X* |*X:X::X:X/M* | **any**} **icmp**		Classifies an IP protocol (ICMP). X:X::X:X : source/destination IPv6 address X:X::X:X/M: source/destination IPv6 address with mask any: any source/destination IPv6 address
ipv6 { *X:X::X:X* | *X:X::X:X/M* | **any**} {*X:X::X:X* |*X:X::X:X/M* | **any**} **icmp** {<0-255> | **any**} {<0-255> | **any**}		
ipv6 { *X:X::X:X* | *X:X::X:X/M* | **any**} {*X:X::X:X* |*X:X::X:X/M* | **any**} {**tcp** | **udp**}		Classifies an IP protocol (TCP/UDP). X:X::X:X : source/destination IPv6 address X:X::X:X/M: source/destination IPv6 address with mask any: any source/destination IPv6 address

Command	Mode	Description
ipv6 { *X:X::X:X* | *X:X::X:X/M* | **any**} {*X:X::X:X* |*X:X::X:X/M* | **any**} **tcp** {<1-65535> | **any**} {<1-65535> | **any**} [*TCP_FLAG* | **any**]		Classifies an IP protocol (TCP/UDP). X:X::X:X : source/destination IPv6 address X:X::X:X/M: source/destination IPv6 address with mask any: any source/destination IPv6 address 0-65535: TCP/UDP port range any: any TCP/UDP port TCP_FLAG: TCP flag vlaue
ipv6 { *X:X::X:X* | *X:X::X:X/M* | **any**} {*X:X::X:X* |*X:X::X:X/M* | **any**} **udp** {<1-65535> | **any**} {<1-65535> | **any**}		

To delete a specified packet-classifying pattern, use the following command.

Command	Mode	Description
no ip	Admin-Flow	Deletes a specified packet-classifying pattern for each option.
no ipv6		
no ip header-length		

7.5.6.3 Applying and modifying Admin Flow

After configuring an admin flow using the above commands, apply it to the system with the following command. If you do not apply it to the system, all specified configurations from *Admin-Flow Configuration* mode will be lost.

To save and apply an admin flow, use the following command.

Command	Mode	Description
apply	Admin-Flow	Applies an admin flow to the system.

To modify an admin flow, use the following command.

Command	Mode	Description
flow admin *NAME* **modify**	Global	Modifies a flow, enter an admin flow name.

i You should save and apply the admin flow to system using **apply** command whenever you modify any configuration of the admin flow.

7.5.6.4 Class Creation

One class can include several flows. You can simply handle and configure the packets on several flows at once.

To create a class including more than 2 flows, use the following command.

Command	Mode	Description
class admin *NAME* **flow** *FLOW1* [*FLOW2*] [*FLOW3*]	Global	Creates an admin class including at least 2 admin flows. NAME: admin class name FLOW: admin flow name

To delete configured admin class or all admin classes, use the following command.

Command	Mode	Description
no class admin all	Global	Deletes all admin classes.
no class admin *NAME*		Deletes specified admin class. NAME: admin class name
no class admin *NAME* **flow** *FLOW1* [*FLOW2*] [*FLOW3*]		Removes specified admin flows from class. NAME: admin class name FLOW: admin flow name

7.5.7 Admin Rule Action

7.5.7.1 Admin Policy Creation

For the OLT, you need to open *Admin-Policy Configuration* mode first. To open *Policy Configuration* mode, use the following command.

Command	Mode	Description
policy admin *NAME* **create**	Global	Creates an admin policy and opens *Admin-Policy Configuration* mode. NAME: admin-policy name.

After opening *Admin Policy Configuration* mode, the prompt changes from SWITCH(config)# to SWITCH(config-admin-policy[NAME])#.

To delete configured admin policy or all admin policies, use the following command.

Command	Mode	Description
no policy admin *NAME*	Global	Deletes specified admin policy.
no policy admin all		Deletes all admin policies.

After opening *Admin-Policy Configuration* mode, an admin policy can be configured by user. You can specify the rule action for the classified packets in each admin-policy.

i

- The admin-policy name must be unique. Its size is limited to 32 significant characters.
- The admin- policy name cannot start with the alphabet “a” or “A”.
- The order in which the following configuration commands are entered is arbitrary.
- The configuration of an admin policy being configured can be changed as often as wanted until the **apply** command is entered.
- Use the **show policy-profile admin** command to display the configuration entered up to now.

If you create the admin policy already, you need to include specified flow or class to specify the rule action for the packets matching configured classifying patterns on flow or class.

To include specific flow or class in an admin policy, use the following command.

Command	Mode	Description
include-flow *NAME*	Admin-Policy	Includes an admin flow in a specified policy. NAME:admin-flow name
include-class *NAME*		Includes an admin class in a specified policy. NAME:admin-class name

One admin policy cannot include both flow and class at the same time. Either admin flow or admin class can belong to one policy.

To remove flow or class from the policy, use the following command.

Command	Mode	Description
no include-flow	Admin-Policy	Removes the admin flow from this policy.
no include-class		Removes the admin class from this policy.

7.5.7.2 Admin Policy Priority

If rules that are more than two match the same packet then the rule having a higher priority will be processed first.

To set a priority for an admin access rule, use the following command.

Command	Mode	Description
priority {**highest** | **high** | **medium**| **low**}	Admin-Policy	Sets a priority for an admin policy. (default: low)

7.5.7.3 Admin Policy Action

To specify the rule action (**action match**) for the packets matching configured classifying patterns, use the following command.

Command	Mode	Description
action match deny	Admin-Policy	Denies a packet.
action match permit		Permits a packet.

To delete a specified rule action(**action match**), use the following command.

Command	Mode	Description
no action match deny	Admin-Policy	Deletes a specified rule action.
no action match permit		

To specify a rule action (**no-action match**) for the packets **not** matching configured classifying patterns, use the following command.

Command	Mode	Description

no-action match deny	Admin-Policy	Denies a packet.
no-action match permit		Permits a packet.

To delete a specified rule action(**no-action match**), use the following command.

Command	Mode	Description
no no-action match deny	Admin-Policy	Deletes a specified rule action.
no no-action match permit		

7.5.7.4 Applying and Modifying Admin Policy

After configuring an admin policy using the above commands, apply it to the system with the following command. If you do not apply this policy to the system, all specified configurations from *Admin-Policy Configuration* mode will be lost.

To save and apply an admin policy, use the following command.

Command	Mode	Description
apply	Admin-Policy	Applies an admin policy to the system.

To modify an admin policy, use the following command.

Command	Mode	Description
policy admin *NAME* **modify**	Global	Modifies an admin policy. NAME: admin-policy name.

7.5.8 Displaying Admin Rule

To show an admin rule profile configured by user, use the follwing command.

Command	Mode	Description
show flow-profile admin	Admin-Flow	Shows a profile of admin flow.
show policy-profile admin	Admin-Policy	Shows a profile of admin policy.

The following command can be used to show a certain rule by its name, all rules of a certain type, or all rules at once sorted by a rule type.

Command	Mode	Description
show { **flow** | **class** | **policy** } **admin** [*NAME*]	Enable Global Bridge	Shows the information relating to each rule, enter an admin rule name.
show { **flow** | **class** | **policy** } **admin detail** [*NAME*]		
show running-config { **admin-flow** | **admin-policy** }	All	Shows all configurations of admin rules.

7.5.9 Scheduling

To process incoming packets by the queue scheduler, the OLT provides the scheduling algorithm as Strict Priority Queuing (SP), Weighted Round Robin (WRR) and Deficit Round Robin (DRR).

Strict Priority Queuing (SP)

SPQ processes first more important data than the others. Since all data are processed by their priority, data with high priority can be processed fast but data without low priority might be delayed and piled up. This method has a strong point of providing the distinguished service with a simple way. However, if the packets having higher priority enter, the packets having lower priority are not processed.

The processing order in Strict Priority Queuing in case of entering packets having the Queue numbers as below

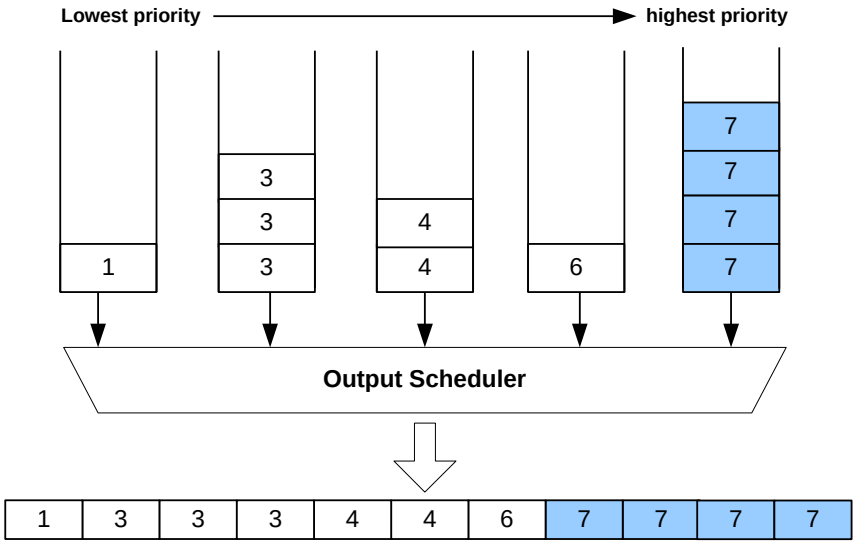


Fig. 7.10 Strict Priority Queuing

Deficit Round Robin (DRR)

DRR is a modified WRR. This can handle packets of variable size without knowing their mean size. A maximum packet size number is subtracted from the packet length, and packets that exceed that number are held back until the next visit of the scheduler.

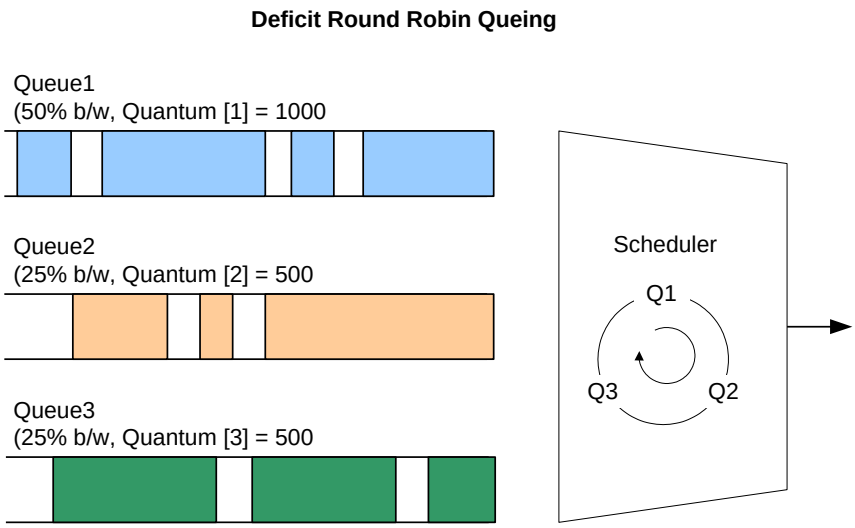


Fig. 7.11 Deficit Round Robin

Weighted Round Robin (WRR)

WRR processes packets as much as weight. Processing the packets that have higher priority is the same way as strict priority queuing. However, it passes to next stage after processing as configured weight so that it is possible to configure for packet process to the packets having higher priority. However, there's a limitation of providing differentiated service from those existing service.

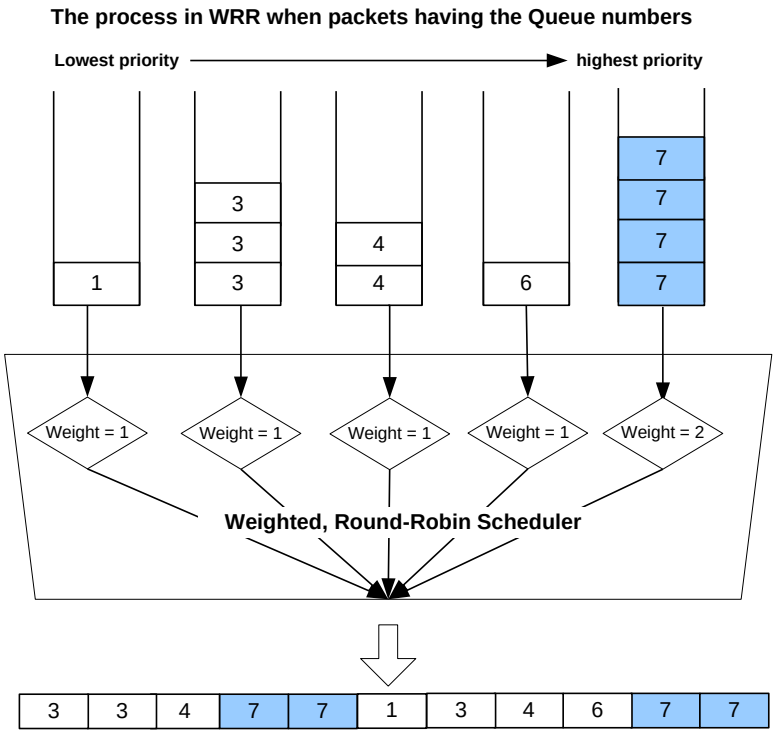


Fig. 7.12 Weighted Round Robin

7.5.9.1 Scheduling mode

To select a packet scheduling mode, use the following command.

Command	Mode	Description
qos scheduling-mode {**sp** | **wrr** | **drr**} *PORTS*	Global	Selects a packet scheduling mode for a ports: sp: strict priority queuing wrr: weighted round robin drr: deficit round robin PORTS: port numbers
qos cpu scheduling-mode {**sp** | **wrr**}		Sets CPU packet scheduling mode.

i The default scheduling mode is **WRR**. And it is possible to assign a different scheduling mode to each port.

7.5.9.2 Weight and Quantum

To set a weight for WRR scheduling mode, use the following command.

Command	Mode	Description
qos weight *PORTS* <0-7> {<1-127> | **unlimited**}	Global	Sets a weight for each port and queue: PORTS: port numbers 0-7: queue number 1-127: weight value (default: 1) unlimited: strict priority based queuing
qos cpu weight <0-7> {<1-127> | **unlimited**}		Sets a weight of queue for CPU packets: 0-7: queue number 1-127: weight value unlimited: strict priority based queuing

To set a quantum for DRR scheduling mode, use the following command.

Command	Mode	Description
qos quantum *PORTS* <0-7> {<1-127> | **unlimited**}	Global	Sets a quantum for each port and queue: PORTS: port numbers 0-7: queue number 1-127: quantum value (default: 1) unlimited: strict priority queuing

7.5.9.3 Maximum and Minimum Bandwidth

To set a maximum bandwidth, use the following command.

Command	Mode	Description
qos max-bandwidth *PORTS* <0-7> {*BANDWIDTH* | **unlimited**}	Global	Sets a maximum bandwidth for each port and queue: PORTS: port numbers 0-7: queue number BANDWIDTH: bandwidth in the unit of MB unlimited: unlimited bandwidth

To set a maximum bandwidth, use the following command.

Command	Mode	Description
qos min-bandwidth *PORTS* <0-7> {*BANDWIDTH* | **unlimited**}	Global	Sets a minimum bandwidth for each port and queue: PORTS: port numbers 0-7: queue number BANDWIDTH: bandwidth in the unit of MB (default: 0) unlimited: unlimited bandwidth

A maximum/minimum bandwidth can be set only in **DRR** scheduling mode.

7.5.9.4 DSCP-to-CoS Mapping

To configure DSCP-to-CoS mapping function for guranting DSCP-based QoS and marking the packet as the color, use the following command.

Command	Mode	Description
qos map dscp <0-63> **newdscp** <0-63> **cos** <0-7> **cng** {**green**| **yellow**| **red**}	Global	Sets the DSCP-to-CoS mapping with the color marking.
no qos map dscp <0-63>		Restores its DSCP-to-CoS mapping configuration to the default.

To display the DSCP-to-CoS configuration, use the following command.

Command	Mode	Description
show qos map dscp [<0-63>]	Enable Global Bridge	Shows the DSCP-to-CoS configuration.

To determine the 802.1p priority of incoming packets through a port using dscp-to-cos mapping table, use the following command.

Command	Mode	Description
port trust dscp *PORTS*	Bridge	Specifies the 802.1p priority using dscp-to-cos mapping table for incoming packets through a port.
no port trust dscp [*PORTS*]		Deletes a specified 802.1p priority.

To display the 802.1p priority the flow control information, use the following command.

Command	Mode	Description
show port trust dscp [*PORTS*]	Enable Global Bridge	Shows the 802.1p priority information

7.5.9.5 The Traffic of Queue

To display the traffic statistic information on each queue, use the following command.

Command	Mode	Description
show queue status *PORTS* [<0-7>]	Enable Global Bridge	Shows the traffic statistic information on each queue.

7.5.9.6 Displaying QoS

To display the configuration of QoS, enter following command.

Command	Mode	Description
show qos	Enable Global Bridge	Shows the configuration of QoS for all ports.
show qos *PORTS*		Shows the configuration of QoS per each port.
show qos cpu		Shows the configuration of QoS for CPU packets.

7.5.9.7 Random Early Detection (WRED)

The OLT supports Weighted Random Early Detection (WRED) which can selectively discard lower priority traffic when an interface gets congested. WRED provides differentiated performance characteristics for different classes of service. It minimizes the impact of dropping high priority traffic. WRED is based on the RED algorithm.

RED, which utilizes end-to-end flow-control of TCP, is a random packet dropping function when traffic reaches the user-given threshold even before it reaches maximum buffer size. If traffic amount reaches maximum buffer size, all packets can be dropped, which makes packet loss. Therefore, in order to prevent packet loss or unstable traffic transmission, user can restrict excessive traffic over buffer size by setting up a threshold. With RED function, packet loss is reduced and stable packet transmission can be acquired.

One of the drawbacks to implement RED function is that it randomly drops a large

number of packets, and is easy to drop high priority of packets. Unlike RED, WRED is not as random when dropping packets. WRED combines the capabilities of the RED algorithm with the IP precedence feature to provide for preferential traffic handling of high-priority packets.

To utilize WRED function, a start queue length value, end queue length value and drop probability are necessary.

- **WRED min-threshold (start queue length value)** is the starting point of random packet dropping.
- **WRED max-threshold (end queue length value)** is the point of complete dropping.
- **drop probability** indicates the percentage of packet dropping from the starting point of random packet dropping to the point of complete dropping. .

If probability is a large value, the amount of packets would be dropped. Therefore complete dropping point is slowly reached. On the other hand, if probability is small, a small amount of packets would be dropped. Therefore complete dropping point is quickly reached. If the probability value is 1, dropping packet would be none and the value is 100, all packets would be discarded from the point of start queue length value is reached.

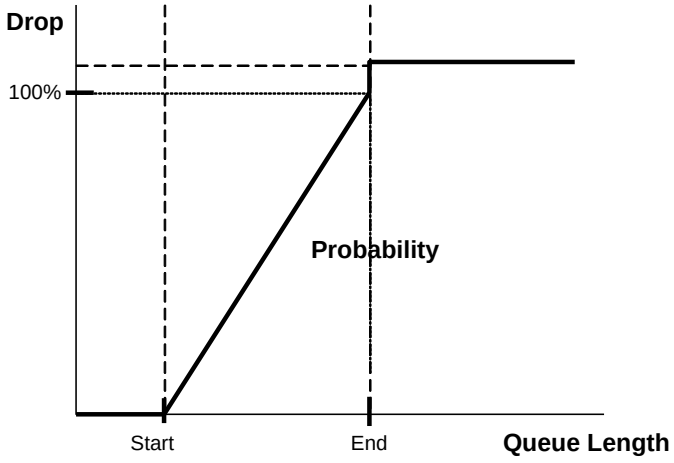


Fig. 7.13 WRED Packet Drop Probability

To configure WRED parameters, use the following command.

Command	Mode	Description
qos random-detect {**green** | **yellow** | **red** } <0-7> **min** <0-1000> **max** <0-10000> **probability** <0-100>	Global	Configures a WRED parameter values. 0-7: queue number min: WRED min-threshold max: WRED max-threshold 0-1000: minimum threshold to begin dropping (default: 32 cells) 0-10000: maximum threshold to drop all packets (default: 192 cells) 1-100: drop probability (default: 5%)
qos random-detect <0-7> **weight** <0-15>		Configures a WRED queue number and weight. 0-7: queue number

		1-15: queue weight (default:1)
no qos random-detect <0-7>		Deletes the configured WRED parameter value.

To enable/disable WRED function, use the following command.

Command	Mode	Description
qos random-detect enable	Global	Enables WRED function.
qos random-detect disable		Disables WRED function.

To display the WRED parameter values per queue number, use the following command.

Command	Mode	Description
show qos random-detect	Enable Global Bridge	Shows WRED function.

7.6 EFM OAM

EFM OAM capabilities are a need for Ethernet subscriber access link monitoring in L2, remote loopback and remote failure indication. EFM OAM uses a slow protocol frame which is called OAM Protocol Data Units (OAMPDUs). Using OAMPDUs, local DTE manages the remote DTE.

There are five EFM OAM operations for local DTE to manage remote DTE.

- **OAM Discovery**
  Local DTE exchanges OAM status information with remote DTE using OAMPDUs.
- **Remote Loopback**
  Local DTE diagnoses the connection of remote DTE using loopback control.
  - Enables the loopback status of remote DTE using OAMPDUs from local DTE.
  - Monitors the link condition by loopback function when local DTE receives back every packet it sends to remote DTE.
- **Link Monitoring**
  Local DTE monitors and informs remote DTE of the event notifications related to the link faults.
- **Remote Failure Indication**
  Local DTE indicates a loss of signal (Link Fault), unrecoverable errors (Dying Gasp) and undefined critical errors (Critical Event)
- **Variable Retrieval**
  Local DTE sends a variable request OAMPDU and gets a value of MIB variable for information retrieval of remote OAM port.

7.6.1 Enabling EFM OAM

To enable/disable EFM OAM function, use the following command.

Command	Mode	Description
oam efm enable *PORTS*	Global	Enables EFM OAM. PORTS: port number
oam efm disable *PORTS*		Disables EFM OAM. PORTS: port number

7.6.2 OAM Link Monitoring

To enable/disable the link monitoring function, use the following command.

Command	Mode	Description
oam efm link-monitor enable *PORTS*	Global	Enables link monitoring function. PORTS: port number
oam efm link-monitor disable *PORTS*		Disables link monitoring function. PORTS: port number

To specify an errored window size and threshold according to the event type, use the following command.

Command	Mode	Description
oam efm link-monitor frame window <10-600> **threshold** <0-65535> *PORTS*	Global	Specifies the window size and threshold in case of frame event. 10-600: window size (unit: 100msec, default:1 second) 0-65535: threshold value (default:1)
oam efm link-monitor frame-period window <1000-200000000> **threshold** <0-65535> *PORTS*		Specifies the window size and threshold in case of frame-period event. 1000-200000000: window size (default: 1000000 pkts) 0-65535: threshold value (default:1)
oam efm link-monitor symbol-period window <1-1000000> **threshold** <0-65535> *PORTS*		Specifies the window size and threshold in case of symbol-period event. 1-1000000: window size (default: 625 million) 0-65535: threshold value (default:1)
oam efm link-monitor frame-seconds-summary window <10-900> **threshold** <0-900> *PORTS*		Specifies the window size and threshold in case of frame-seconds-summary error event. 10-900: window size (default: 60 seconds) 0-900: threshold value (default:1)

To clear the collected statistics of EFM OAM link monitoring, use the following command.

Command	Mode	Description
clear oam efm link-monitor stats *PORTS*	Global	Clears the collected statistics of EFM OAM link monitoring. PORTS: port number

To configure how to handle the event notifications that the switch is received, use the following command.

Command	Mode	Description
oam efm link-monitor action syslog *PORTS*	Global	Generates a syslog message when event notifications are received. PORTS: port number
oam efm link-monitor action snmp-trap *PORTS*		Generates a snmp trap message when event notifications are received. PORTS: port number

7.6.3 EFM OAM Mode

To configure EFM OAM mode, use the following command.

Command	Mode	Description
oam efm mode {**active** | **passive**}	Global	Configures the mode of EFM OAM.

PORTS		PORTS: port number

i Both request and loopback can be available in the EFM OAM active mode. However, request or loopback is not available in the OAM passive mode.

7.6.4 OAM Loopback

For OAM loopback function, both the switch and the host should support OAM function. OAM loopback function enables Loopback function from the user's device to the host which connected to the user's device and operates it.

To enable/disable the remote loopback mode, use the following command.

Command	Mode	Description
oam efm remote-loopback permit *PORTS*	Global	Receives the loopback control commands from its remote peer switch. PORTS: port number
oam efm remote-loopback deny *PORTS*		Ignores the loopback control commands from its remote peer switch. (Default) PORTS: port number

To configure loopback function of the host connected to the switch, use the following command.

Command	Mode	Description
oam efm remote-loopback enable *PORTS*	Global	Enables loopback function of peer device.
oam efm remote-loopback disable *PORTS*		Disables loopback function of peer device.
oam efm remote-loopback test <1-100> *PORTS*		Starts to perform the test of loopback operation. 1-100: the number of test packets PORTS: port number

7.6.5 OAM Unidirection

When RX is impossible in OAM, it is possible to send the information by using TX. To enable/disable the function, use the following command.

Command	Mode	Description
oam efm unidir enable *PORTS*	Global	Sends the information by using TX. PORTS: port number
oam efm unidir disable *PORTS*		Disables to transmit the information by using TX. PORTS: port number

7.6.6 Displaying EFM OAM Configuration

To display OAM configuration, use the following command.

Command	Mode	Description
show oam efm	Enable Global	Shows EFM OAM configuration.
show oam efm link-monitor {**local** | **remote**} *PORTS*		Shows the link monitoring status and remote statistics on the port. PORTS: port number
show oam efm local *PORTS*		Shows local OAM configuration.
show oam efm remote *PORTS*		Shows remote OAM configuration.
show oam efm variable <0-255> <0-65535> *PORTS*		Shows remote OAM variable. 0-255: branch number 0-65535: leaf number

7.7 NetBIOS Filtering

NetBIOS (Network Basic Input/Output System) is a program that allows applications on different computers to communicate within a local area network (LAN). NetBIOS is used in Ethernet, included as part of NetBIOS Extended User Interface (NetBEUI). Resource and information in the same network can be shared with this protocol.

However, the more computers are used recently, the more strong security is required. To secure individual customer's information and prevent information leakages in the LAN environ-men, the OLT provides NetBIOS filtering function.

Without NetBIOS filtering, customer's data may be opened to each other even though the data should be kept. To keep customer's information and prevent sharing information in the above case, NetBIOS filtering is necessary.

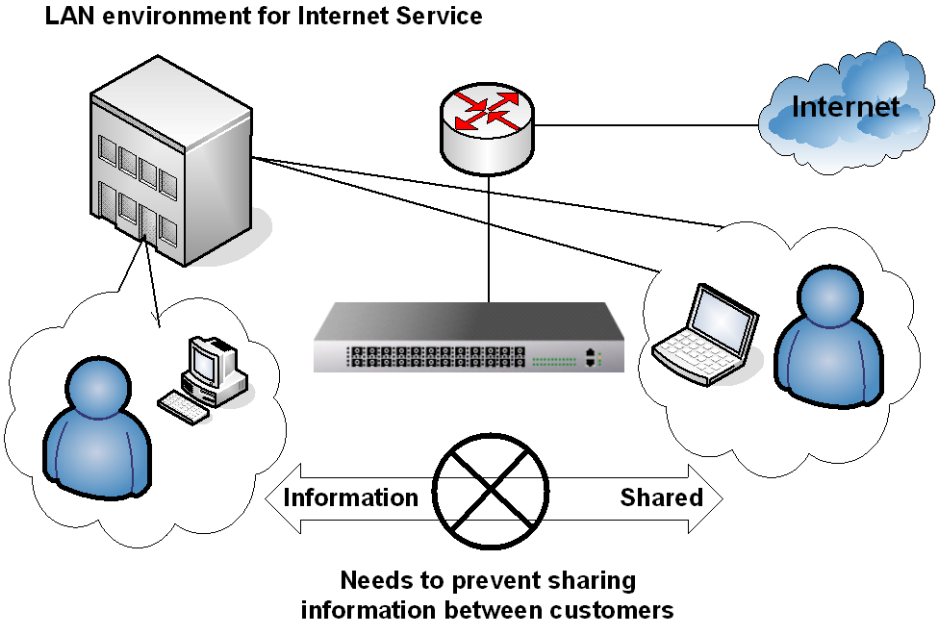


Fig. 7.14 NetBIOS Filtering

To enable/disable NetBIOS filtering, use the following command.

Command	Mode	Description
netbios-filter *PORTS*	Bridge	Configures NetBIOS filtering to a specified port.
no netbios-filter *PORTS*		Disables NetBIOS filtering from a specified port.

To display a configuration of NetBIOS filtering, use the following command.

Command	Mode	Description
show netbios-filter	Enable Global Bridge	Shows a configuration of NetBIOS filtering.

7.8 Martian Filtering

It is possible to block packets, which trying to bring different source IP out from same network. If packet brings different IP address, not its source IP address, then it is impossible to know it makes a trouble. Therefore, you would better prevent this kind of packet outgoing from your network. This function is named as Martian filter.

To enable/disable a Martian filtering, use the following command.

Command	Mode	Description
ip martian-filter *INTERFACE*	Global	Blocks packets which bring different source IP address from specified interface. INTERFACE: enter the interface name.
no ip martian-filter *INTERFACE*		Disables a configured Martian filter. INTERFACE: enter an interface name.

QoS and Martian filter cannot be used together.

7.9 Max Host

You can limit the number of users by configuring the maximum number of users also named as max hosts for each port. In this case, you need to consider not only the number of PCs in network but also devices such as switches in network.

Max-new-hosts is to limit the number of users by configuring the number of MAC addresses that can be learned on the system and on the port for a second. The number of MAC addresses that can be learned on the system has the priority.

To configure max new hosts, use the following command.

Command	Mode	Description
max-new-hosts *PORTS VALUE*	Bridge	The number of MAC addresses that can be learned on the port for a second. VALUE: maximum MAC number <1-2147483646>
max-new-hosts system *VALUE*		The number of MAC addresses that can be learned on the system for a second. VALUE: maximum MAC number <1-2147483646>

To delete configured max new hosts, use the following command.

Command	Mode	Description
no max-new-hosts [*PORTS*]	Bridge	Deletes the number of MAC addresses that can be learned on the port.
no max-new-hosts system		Deletes the number of MAC addresses that can be learned on the system.

To display configured max new hosts, use the following command.

Command	Mode	Description
show max-new-hosts	Enable Global Bridge	Shows the configured Max-new-hosts.

If MAC that already counted disappears before passing 1 second and starts learning again, it is not counted. In case the same MAC is detected on the other port also, it is not counted again. For example, if MAC that was learned on port 1 is detected on port 2, it is supposed that MAC moved to the port 2. So, it is deleted from the port 1 and learned on the port 2 but it is not counted.

7.10 Port Security

You can use the port security feature to restrict input to an interface by limiting and identifying MAC addresses of the PCs that are allowed to access the port. When you assign secure MAC addresses to a secure port, the port does not forward packets with source addresses outside the group of defined addresses. If you limit the number of secure MAC addresses to one and assign a single secure MAC address, the PC attached to that port is assured the full bandwidth of the port.

7.10.1 Port Security on Port

Step 1 Enable port security on the port.

Command	Mode	Description
port security *PORTS*	Bridge	Enables port security on the port.

Step 2 Set the maximum number of secure MAC addresses for the port.

Command	Mode	Description
port security *PORTS* **maximum** <1-16384>	Bridge	Sets the maximum number of secure MAC addresses for the port. (default: 1)

Step 3 Set the violation mode and the action to be taken.

Command	Mode	Description
port security *PORTS* **violation** {**shutdown** | **protect** | **restrict**}	Bridge	Selects a violation mode. (default: shutdown)

When configuring port security, note that the following information about port security violation modes:

- **protect** drops packets with unknown source addresses until you remove a sufficient number of secure MAC addresses to drop below the maximum value.
- **restrict** drops packets with unknown source addresses until you remove a sufficient number of secure MAC addresses to drop below the maximum value and causes the Security Violation counter to increment.
- **shutdown** puts the interface into the error-disabled state immediately and sends an SNMP trap notification.

Step 4 Enter a secure MAC address for the port.

Command	Mode	Description
port security *PORTS* **mac-address** *MAC-ADDR* **vlan** *NAME*	Bridge	Sets a secure MAC address for the port.

To disable the configuration of port secure, use the following command.

Command	Mode	Description
no port security *PORTS*	Bridge	Disables port security on the port.
no port security *PORTS* **mac-address** [*MAC-ADDR* **vlan** *NAME*]		Deletes a secure MAC address for the port.
no port security *PORTS* **maximum**		Returns to the default number of secure MAC addresses. (default: 1)
no port security *PORTS* **violation**		Returns to the violation mode to the default. (default: shutdown)

To reset the configuration of secure MAC address, use the following command.

Command	Mode	Description
clear port security *PORTS* **mac-address** [*MAC-ADDR* **vlan** *NAME*]	Bridge	Deletes the configuration of secure MAC address on specified port.

7.10.2 Port Security Aging

Port security aging is to set the aging time for all secure addresses on a port. Use this feature to remove and add PCs on a secure port without manually deleting the existing secure MAC addresses while still limiting the number of secure addresses on a port.

Command	Mode	Description
port security *PORTS* **aging static**	Bridge	Enables aging for configured secure addresses.
port security *PORTS* **aging time** <1-1440>		Configures aging time in minutes for the port. All the secure addresses age out exactly after the time.
port security *PORTS* **aging type** {**absolute** | **inactivity**}		Configures aging type.

- **absolute** all the secure addresses on this port age out exactly after the time (minutes) specified lapses and are removed from the secure address list.
- **inactivity** the secure addresses on this port age out only if there is no data traffic from the secure source addresses for the specified time period.

To disable the configuration of port secure aging, use the following command.

Command	Mode	Description
no port security *PORTS* **aging static**	Bridge	Disables aging for only statistically configured secure addresses.
no port security *PORTS* **aging time**		Disables port secure aging for all secure addresses on a port.
no port security *PORTS* **aging type**		Returns to the default condition. (absolute)

7.10.3 Displaying Port Security

To display the information of the port security, use the following command.

Command	Mode	Description
show port security [*PORTS*]	Enable Global Bridge	Shows the information of the port security.

7.11 Outband Management Port Security

The OLT provides the function that prevents users from accessing the outband management network via the subscriber interface. Using this function, in case that a certain packet's destination is MGMT interface—the OLT's outband management interface, the system discards that packet.

To protect the outband management network, use the following command.

Command	Mode	Description
ip_forwarding {**enable** | **disable**}	Interface	Configures the system not to forward packets via subscriber interface.

This function operates only for the MGMT interface, which is activated with the **no shutdown** command.

7.12 Max Host

You can limit the number of users by configuring the maximum number of users also named as max hosts for each Ethernet/PON port. In this case, you need to consider not only the number of PCs in the network but also devices such as switches in the network.

For the OLT, you have to block the port like MAC filtering before configuring max hosts. In case of ISPs, it is possible to arrange a billing plan for each user by using this configuration.

To specify the maximum number of hosts that can be attached to an Ethernet/PON interface, use the following command.

Command	Mode	Description
max-hosts *PORTS MAX_MAC*	Bridge	Specifies the maximum number of hosts that be attached to an Ethernet/PON port on this interface. PORTS: port number. MAX_MAC: the maximum number of hosts for a particular interface. Valid range is from 0 to 2147483646 hosts.
no max-hosts *PORTS*		Resets the allowable number of hosts attached to a

		particular interface to the default value of unlimited hosts.

To display the configured maximum number of hosts for interfaces, use the following command.

Command	Mode	Description
show max-hosts	Bridge/ Global	Shows the configured maximum number of hosts for the interfaces.

7.13 MAC Table

A dynamic MAC address is automatically registered in the MAC table, and it is removed if there is no access to/from the network element corresponding to the MAC address during the specified MAC aging time. On the other hand, a static MAC address is manually registered by user. This will not be removed regardless of the MAC aging time before removing it manually.

To manage a MAC table in the system, use the following command.

Command	Mode	Description
mac *NAME PORT MAC-ADDR*	Bridge	Specifies a static MAC address in the MAC table. NAME: bridge name PORT: port number MAC-ADDR: MAC address
mac aging-time <10-21474830>		Specifies MAC aging time: 10-21474830: aging time (default: 300 seconds)
mac move {**enable** | **disable**} *PORTS*		Sets the policy of handling a MAC address if a MAC address already learned on one port has moved to a different port. enable: MAC address is recorded/learned for the most recent arrival port and the previous entry is deleted disable: MAC address is not recorded/learned for the most recent arrival port and the previous entry is not deleted.

To remove the registered dynamic MAC addresses from the MAC table, use the following command.

Command	Mode	Description
clear mac [*NAME*]	Enable Global Bridge	Clears dynamic MAC addresses. NAME: bridge name
clear mac *NAME PORT*		Clears dynamic MAC addresses. PORT: port number
clear mac *NAME PORT MACADDR*		Clears dynamic MAC addresses. MACADDR: MAC address

To remove the static MAC addresses manually registered by user from the MAC table, use the following command.

Command	Mode	Description
no mac	Bridge	Deletes static MAC addresses.
no mac *NAME*		Deletes static MAC addresses, enter the bridge name.
no mac *NAME PORT*		Deletes static MAC addresses. NAME: bridge name
no mac *NAME PORT MACADDR*		Deletes a specified static MAC address. PORT: port number MACADDR: MAC address

To display the MAC table in the switch, use the following command.

Command	Mode	Description
show mac [*NAME*]	Enable Global Bridge	Shows switch MAC address, selection by port number (subscriber port only): NAME: bridge name PORT: port number
show mac *NAME PORT*		

i

There are more than a thousand of MAC addresses in MAC table, so it is difficult to find information you need at one sight. For that reason, the system shows a certain amount of addresses displaying –**more**– on standby status. Press any key to search more. After you find the information, you can go back to the system prompt without displaying the other table by pressing <**q**>.

7.14 MAC Filtering

It is possible to forward frame to MAC address of destination. Without specific performance degradation, maximum 4096 MAC addresses can be registered.

7.14.1 Default MAC Filter Policy

The basic policy of filtering based on system is set to allow all packets for each port. However, the basic policy can be changed for user's requests.

After configuring basic policy of filtering for all packets, use the following command.

Command	Mode	Description
mac-filter default-policy {**deny** | **permit**} *PORTS*	Bridge	Configures basic policy of MAC Filtering in specified port.

i By default, basic filtering policy provided by system is configured to permit all packets in each port.

Sample Configuration

This is an example of blocking all packets in port 6 to 7 and port 8.

```
SWTICH(bridge)#  mac-filter default-policy deny 6-8
SWTICH(bridge)# show mac-filter default-policy
-------------------------
  PORT POLICY | PORT POLICY
  ------------+------------
     1 PERMIT |    2 PERMIT
     3 PERMIT |    4 PERMIT
     5 PERMIT |    6 DENY
     7 DENY   |    8 DENY
     9 PERMIT |   10 PERMIT
    11 PERMIT |   12 PERMIT
    13 PERMIT |   14 PERMIT
    15 PERMIT |   16 PERMIT
    17 PERMIT |   18 PERMIT
SWTICH(bridge)#
```

7.14.2 Configuring MAC Filter Policy

You can add the policy to block or to allow some packets of specific address after configuring the basic policy of MAC Filtering. To add this policy, use the following commands in *Bridge Configuration* mode.

Command	Mode	Description
mac-filter add *MAC-ADDR* {**deny** | **permit**} [<1-4094>] [*PORTS*]	Bridge	Allows or blocks packet which brings a specified MAC address to specified port.

To delete MAC filtering policy, use the following command.

Command	Mode	Description
mac-filter del *SRC-MAC-ADDR* [<1-4094>]	Bridge	Deletes filtering policy for specified MAC address.

To delete MAC filtering function, use the following command.

Command	Mode	Description
no mac-filter	Bridge	Deletes all MAC filtering functions.

7.14.3 Listing MAC Filter Policy

If you need to make many MAC filtering policies at a time, it is hard to input command one by one. In this case, it is more convenient to save MAC filtering policies at "/etc/mfdb.conf" and display the list of MAC filtering policy. To view the list of MAC filtering policy at /etc/mfdb.conf, use the following command.

Command	Mode	Description
mac-filter list	Bridge	Shows the list of MAC filtering policy at /etc/mfdb.conf.

7.14.4 Displaying MAC Filter Policy

To show a configuration about MAC filter policy, use the following command.

Command	Mode	Description
show mac-filter	Enable Global Bridge	Shows a configured MAC filter policy.
show mac-filter default-policy		Shows the default MAC filter policy.

7.15 Address Resolution Protocol (ARP)

Devices connected to IP network have two addresses, LAN address and network address. LAN address is sometimes called as a data link address because it is used in Layer 2 level, but more commonly the address is known as a MAC address. A switch on Ethernet needs a 48-bit-MAC address to transmit packets. In this case, the process of finding a proper MAC address from the IP address is called an address resolution.

On the other hand, the progress of finding the proper IP address from the MAC address is called reverse address resolution. This product find its MAC addresses from the IP addresses through Address Resolution Protocol (ARP). ARP saves these addresses in ARP table for quick search. Referring to the IP addresses in ARP table, the packets containing the IP address are transmitted to network. When configuring the ARP table, it is possible to do it only in some specific interfaces.

7.15.1 ARP Table

Hosts typically have an ARP table, which is a cache of IP/MAC address mappings. The ARP Table automatically maps the IP address to the MAC address of a switch. In addition to address information, the table shows the age of the entry in the table, the encapsulation method, and the switch interface (VLAN ID) where packets are forwarded.

The OLT ARP saves IP/MAC addresses mappings in ARP table for quick search. Referring to the information in ARP table, packets attached IP address is transmitted to network. When configuring ARP table, it is possible to do it only in some specific interfaces.

7.15.1.1 Registering ARP Table

The contents of ARP table are automatically registered when MAC address corresponds to MAC address is founded. The network administrator could use MAC address of specific IP address in Network by registering on ARP table.

To specify a static ARP entry, use the following command.

Command	Mode	Description
arp *A.B.C.D MAC-ADDR*	Global	Specifies a static ARP entry. MAC-ADDR: MAC address.
arp *A.B.C.D MAC-ADDR INTERFACE*		Specifies a static ARP entry with an interface name. INTERFACE: interface name MAC-ADDR: MAC address
no arp [*A.B.C.D*]		Deletes static ARP entries.
no arp *A.B.C.D INTERFACE*		

To delete ARP entries, use the following command.

Command	Mode	Description
clear arp	Enable Global Bridge	Deletes all ARP entries.
clear arp *INTERFACE*		Deletes the ARP entries on a specified interface.

7.15.1.2 Displaying ARP Table

To display ARP table registered in switch, use one of the following command.

Command	Mode	Description
show arp	Enable Global Bridge	Shows ARP table. INTERFACE: interface name A.B.C.D: IP address
show arp {*INTERFACE* | *A.B.C.D*}		

The following is an example of displaying a current ARP table for all interfaces.

```
SWITCH# show arp
Flags : (C)completed entry (M)permanent entry (H)writed entry to chip
IP Address      Mac Address        Flags Mask   HW Type   Interface   Port
-------------------------------------------------------------------------------
10.56.146.100   f0:4d:a2:db:09:bb   C           ether     mgmt        --
10.56.146.254   b8:26:d4:2a:51:9e   C           ether     mgmt        --
192.168.253.253 00:a1:a1:12:34:43   C           ether     mbe0        --
192.168.254.254 00:a1:a1:12:34:44   C           ether     mbe1        --
-------------------------------------------------------------------------------
      C      CH      H      CM      CMH      Total       Iface
-------------------------------------------------------------------------------
      4       0      0       0       0         4     ALL INTERFACE
-------------------------------------------------------------------------------
SWITCH#
```

7.15.2 ARP Request Message Interval

To set the interval for sending ARP request packets from the switch to prevent the connected network devices to get overloaded, use the following command.

Command	Mode	Description
ip arp-request interval retrans <1-300>	Interface	Sets the number of seconds to delay before retransmitting the ARP request. 1-300: retry attempt interval of retransmission (default: 1 second)

To the configured interval of ARP request messages, use the following command.

Command	Mode	Description
no ip arp-request interval retrans	Interface	Deletes the configured interval of ARP request message.

7.15.3 ARP Alias

Although clients are joined in the same client switch, it may be impossible to communicate between them for security reasons. When you need to make them communicate each other, the OLT supports ARP alias, which responses the ARP request

from client net through the concentrating switch.

To register the address of client net range in ARP alias, use the following command.

Command	Mode	Description
arp alias *A.B.C.D A.B.C.D* [*XX:XX:XX:XX:XX:XX*]	Global	Registers the IP address range and MAC address in ARP alias to make the system response to an ARP request.
arp alias *A.B.C.D A.B.C.D* **vlan** *VLAN* **gateway** *GATEWAY*		Registers gateway IP address within IP address range to make the system response automatically MAC address of gateway. VLAN: 1-4094 GATEWAY: gateway IP address
no arp alias *A.B.C.D A.B.C.D*		Deletes the registered IP address range of ARP alias.

i Unless you input a MAC address, the MAC address of user's device will be used for ARP response.

To set aging time of gateway IP address in ARP alias, use the following command.

Command	Mode	Description
arp alias aging-time <5-2147483647>	Global	Sets the aging time of gateway IP address. 5-2147483647: aging time (default: 300 seconds)
no arp alias aging-time		Deletes the aging time of gateway IP address.

To display a registered ARP alias, use the following command.

Command	Mode	Description
show arp alias	Enable Global Bridge	Shows a registered ARP alias.

7.15.4 ARP Inspection

ARP provides IP communication by mapping an IP address to a MAC address. However, a malicious user can attack ARP caches of systems by intercepting the traffic intended for other hosts on the subnet. For example, Host B generates a broadcast message for all hosts within the broadcast domain to obtain the MAC address associated with the IP address of Host A. If Host C responses with an IP address of Host A (or B) and a MAC address of Host C, Host A and Host B can use Host C's MAC address as the destination MAC address for traffic intended for Host A and Host B.

ARP Inspection is a security feature that validates ARP packets in a network. It discards ARP packets with invalid IP-MAC address binding.

To activate/deactivate the ARP inspection function in the system, use the following command.

Command	Mode	Description
ip arp inspection vlan *VLANS*	Global	Activates ARP inspection on a specified VLAN. VLANS: VLAN ID (1-4094)
no ip arp inspection vlan *VLANS*		Deactivates ARP inspection on a specified VLAN.

7.15.4.1 ARP Access List

You can exclude a given range of IP addresses from the ARP inspection using ARP access lists. ARP access lists are created by the **arp access-list** command on the *Global Configuration* mode. ARP access list permits or denies the ARP packets of a given range of IP addresses.

To create/delete ARP access list (ACL), use the following command.

Command	Mode	Description
arp access-list *NAME*	Global	Opens ARP ACL configuration mode and creates an ARP access list. NAME: ARP access list name
no arp access-list *NAME*		Deletes an ARP access list.
arp access-list delete all		Deletes all ARP access lists.

After opening *ARP Access List Configuration* mode, the prompt changes from SWITCH(config)# to SWITCH(config-arp-acl[*NAME*])#. After opening *ARP ACL Configuration* mode, a range of IP addresses can be configured to apply ARP inspection.

i By default, ARP Access List discards the ARP packets of all IP addresses and MAC addresses.

To configure the range of IP address to deny ARP packets, use the following command.

Command	Mode	Description
deny ip any mac {**any** | **host** *MACADDR*}	ARP-ACL	Discards all ARP packets of all IP addresses with all MAC addresses which have not learned before on ARP inspection table or a specific MAC address any: ignores sender IP/MAC address host: sender host MACADDR: sender MAC address
deny ip host *A.B.C.D* **mac** {**any** | **host** *MACADDR*}		Discards ARP packets from a specific host. MACADDR: MAC address
deny ip range *A.B.C.D A.B.C.D* **mac any**		Discards ARP packets of a given range of IP addresses. A.B.C.D: start/end IP address of sender
deny ip *A.B.C.D/A* **mac** {**any** | **host** *MACADDR*}		Discards ARP packets of a sender IP network addresses. A.B.C.D/A: sender IP network address

To delete the configured range of IP address for discarding ARP packets, use the following command.

Command	Mode	Description
no deny ip any mac {**any** | **host** *MACADDR*}	ARP-ACL	Deletes a configured range of IP address to discard ARP packets. any: ignores sender MAC address host: sender host MACADDR: sender MAC address A.B.C.D: start/end IP address of sender A.B.C.D/A: sender IP network address
no deny ip host *A.B.C.D* **mac** {**any** | **host** *MACADDR*}		
no deny ip range *A.B.C.D A.B.C.D* **mac any**		
no deny ip *A.B.C.D/A* **mac** {**any** | **host** *MACADDR*}		

To specify the range of IP address to forward ARP packets, use the following command.

Command	Mode	Description
permit ip any mac {**any** | **host** *MACADDR*}	ARP-ACL	Permits ARP packets of all IP addresses with all MAC addresses which have not learned before on ARP inspection table or a specific MAC address. any: ignores sender MAC address host: sender host MACADDR: sender MAC address
permit ip host *A.B.C.D* **mac** {**any** | **host** *MACADDR*}		Permits ARP packets from a specific host. MACADDR: MAC address
permit ip range *A.B.C.D A.B.C.D* **mac any**		Permits ARP packets of a given range of IP addresses. A.B.C.D: start/end IP address of sender
permit ip *A.B.C.D/A* **mac** {**any** | **host** *MACADDR*}		Permits ARP packets of a sender IP network addresses. A.B.C.D/A: sender IP network address

To delete the configured ranged of IP address to permit ARP packets, use the following command.

Command	Mode	Description
no permit ip any mac {**any** | **host** *MACADDR*}	ARP-ACL	Deletes a configured range of IP address to permit ARP packets. any: ignores sender MAC address host: sender host MACADDR: sender MAC address A.B.C.D: start/end IP address of sender A.B.C.D/A: sender IP network address
no permit ip host *A.B.C.D* **mac** {**any** | **host** *MACADDR*}		
no permit ip range *A.B.C.D A.B.C.D* **mac any**		
no permit ip *A.B.C.D/A* **mac** {**any**		

| **host** *MACADDR*}		

By the following command, the ARP access list also refers to a DHCP snooping binding table to permit the ARP packets for DHCP users. This reference enables the system to permit ARP packets only for the IP addresses on the DHCP snooping binding table. The ARP access list with the DHCP snooping allows IP communications to users authorized by the DHCP snooping.

To permit/discard ARP packets for the users authorized by the DHCP snooping, use the following command.

Command	Mode	Description
permit dhcp-snoop-inspection	ARP-ACL	Permits ARP packets of users authorized by the DHCP snooping.
no permit dhcp-snoop-inspection		Discards a configured ARP packets of users authorized by the DHCP snooping.

To display the configured APR access lists, use the following command.

Command	Mode	Description
show arp access-list [*NAME*]	Global	Displays existing ARP access list names.

7.15.4.2 Enabling ARP Inspection Filtering

To enable/disable the ARP inspection filtering of a certain range of IP addresses from the ARP access list, use the following command.

Command	Mode	Description
ip arp inspection filter *NAME* **vlan** *VLANS*	Global	Enables ARP inspection filtering with a configured ARP access list on specified VLAN. NAME: ARP access list name
no ip arp inspection filter *NAME* **vlan** *VLANS*		Disables ARP inspection filtering with a configured ARP access list on specified VLAN.

i ARP inspection actually runs in the system after the configured ARP access list applies to specific VLAN using the **ip arp inspection filter** command.

7.15.4.3 ARP Address Validation

The OLT also provides the ARP validation feature. Regardless of a static ARP table, the ARP validation will discard ARP packets in the following cases:

- In case a sender MAC address of ARP packet does not match a source MAC address of Ethernet header.
- In case a target MAC address of ARP reply packet does not match a destination MAC address of Ethernet header.
- In case of a sender IP address of ARP packet or target IP address is 0.0.0.0 or

255.255.255.255 or one of multicast IP addresses.

To enable/disable the ARP validation, use the following command.

Command	Mode	Description
ip arp inspection validate {**src-mac** | **dst-mac** | **ip**}	Global	Enables the ARP validation with the following options. src-mac: source MAC address. dst-mac: destination MAC address. ip: source/destination IP address.
no ip arp inspection validate {**src-mac** | **dst-mac** | **ip**}		Disables the ARP validation.

i The **src-mac**, **dst-mac**, and **ip** options can be configured together.

7.15.4.4 ARP Inspection on Trust Port

The ARP inspection defines 2 trust states, trusted and untrusted. Incoming packets via trusted ports bypass the ARP inspection process, while those via untrusted ports go through the ARP inspection process. Normally, the ports connected to subscribers are configured as untrusted, while the ports connected to an upper network are configured as trusted.

To set a trust state on a port for the ARP inspection, use the following command.

Command	Mode	Description
ip arp inspection trust port *PORTS*	Global	Sets a trust state on a port as trusted PORTS: port number
no ip arp inspection trust port *PORTS*		Sets a trust state on a port as untrusted PORTS: port number

To display a configured trust port of the ARP inspection, use the following command.

Command	Mode	Description
show ip arp inspection trust [**port** *PORTS*]	Enable Global Bridge	Shows a configured trust port of the ARP inspection.

7.15.4.5 ARP Inspection Log-buffer

Log-buffer function shows the list of subscribers who have been used invalid fixed IP addresses. This function saves the information of users who are discarded by ARP inspection and generates periodic syslog messages.

Log-buffer function is automatically enabled with ARP inspection. If OLT receives invalid or denied ARP packets by ARP inspection, it creates the table of entries that include the information of port number, VLAN ID, source IP address, source MAC address and time. In addition, you can specify the maximum number of entries.

After one of entries is displayed as a syslog message, it is removed in the order in which the entries appear in the list.

To configure the options of log-buffer function, use the following command.

Command	Mode	Description
ip arp inspection log-buffer entries <0-1024>	Global	Specifies the number of entries in log-buffer. 0-1024: the max. number of entries (default: 32)
ip arp inspection log-buffer logs <0-1024> **interval** <0-86400>		Sets the interval for displaying syslog messages of entries. 0-1024: the number of syslog messages per specified interval (default: 5) 0-86400: interval value in second (default: 1 sec)

To delete the configured options of log-buffer function, use the following command.

Command	Mode	Description
no ip arp inspection log-buffer {**entries** | **logs**}	Global	Deletes the configured options of log-buffer function.

To display the configured log-buffer function and entries' information, use the following command.

Command	Mode	Description
show ip arp inspection log	Enable Global Bridge	Displays the configured log-buffer function.

To clear all of collected entries in the list, use the following command.

Command	Mode	Description
clear ip arp inspection log	Enable Global Bridge	Clears all of collected entires in the log-buffer list.

7.15.4.6 Displaying ARP Inspection

To display a status of the ARP inspection, use the following command.

Command	Mode	Description
show ip arp inspection [**vlan** *VLANS*]	Enable Global Bridge	Shows a status of the ARP inspection.
show ip arp inspection statistics [**vlan** *VLANS*]		Shows collected statistics of the ARP inspection.

To clear collected statistics of the ARP inspection, use the following command.

Command	Mode	Description
clear ip arp inspection statistics [**vlan** *VLANS*]	Enable Global Bridge	Clears collected statistics of the ARP inspection.

7.15.5 Gratuitous ARP

Gratuitous ARP is a broadcast packet like an ARP request. It containing IP address and MAC address of gateway, and the network is accessible even though IP addresses of specific host's gateway are repeatedly assigned to the other.

Configure Gratuitous ARP interval and transmission count using following commands. And configure transmission delivery-start in order to transmit Gratuitous ARP after ARP reply. Gratuitous ARP is transmitted after some time from transmitting ARP reply.

Command	Mode	Description
arp patrol *TIME COUNT* [*TIME*]	Global	Configures a gratuitous ARP. TIME: transmit interval COUNT: transmit count
no arp patrol		Disables a gratuitous ARP.

7.15.6 Proxy ARP

The OLT supports the proxy ARP. Proxy ARP is the technique in which one host, usually a router, answers ARP requests intended for another machine. By "faking" its identity, the router accepts responsibility for routing packets to the "real" destination. Proxy ARP can help the switches on a subnet reach remote subnets without configuring routing or a default gateway.

As shown in Fig. 7.15, the host A has a /16 subnet mask. What this means is that the host A believes that it is directly connected to all of network 172.16.0.0. When the host A needs to communicate with any switches if believes are directly connected, it will send an ARP request to the destination. Therefore, when the host A needs to send a packet to the host D, the host A believes that the host D is directly connected, so it sends an ARP request to the host D.

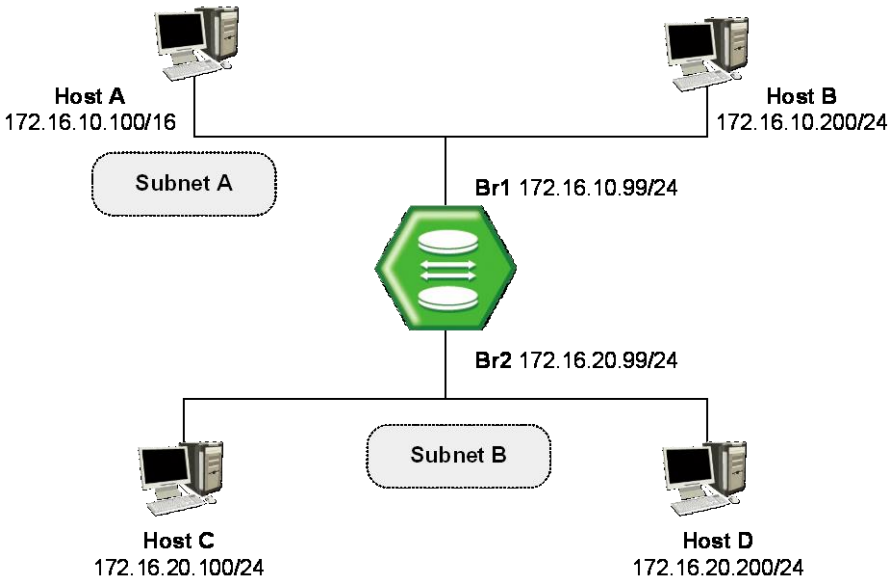


Fig. 7.15 Proxy ARP

The host A needs the MAC address of the host D to reach the host D. Therefore, the host A broadcasts an ARP request on the subnet A, including the OLT's br1 interface, but does not reach the host D. By default, the OLT does not forward broadcasts. Since the OLT knows that the target address (the host D's IP address) is on another subnet and can reach the host D, it will reply with its own MAC address to the host A.

The proxy ARP replies that the OLT sends to the host A. The proxy ARP reply packet is encapsulated in an Ethernet frame with its MAC address as the source address and the host A's MAC address as the destination address. The ARP replies are always unicast to the original requester. On receiving this ARP reply, the host A updates its ARP table.

From now on, the host A will forward all the packets that it wants to reach the host D to the MAC address of the OLT. Since the OLT knows how to reach the host D, the router forwards the packet to the host D. The ARP cache on the hosts in the subnet A is populated with the MAC address of the OLT for all the hosts on the subnet B. Hence, all packets destined to the subnet B are sent to the router. The OLT forwards those packets to the hosts in the subnet B.

To configure the interface to accept and respond to proxy ARP, use the following command on *Interface Configuration* mode.

Command	Mode	Description
ip proxy-arp	Interface	Enables the proxy ARP function on specific interface.
no ip proxy-arp		Disables the proxy ARP function.

7.16 IPv6 Neighbor Discovery(ND)

Neighbor discovery (ND) is specified in RFC 2464. ND combines Address Resolution Protocol (ARP) and ICMP router discovery and Redirect. With IPv4, we have no means to detect whether or not a neighbor is reachable. With ND protocol, a neighbor unreachability detection mechanism has been defined.

IPv6 nodes use neighbor discovery for the following purposes:
- To determine Layer 2 addresses of nodes on the same link
- To find neighboring routers that can forward their packets
- To keep track of which neighbor are reachable and which are not, and detect changed link-layer addresses

The neighbor discovery protocol consists of five ICMP messages:

- **Router Solicitation / Router Advertisement (RS & RA)**
  The routers send out Router Advertisement (RA) message in regular intervals. The hosts can request RA message by issuing a Router Solicitation message.
  RA message contains the information of link prefixes, link MTU, specific routers, and duration.
- **Neighbor Solicitation / Neighbor Advertisement (NS & NA)**
  These messages fulfill the functions that the link-layer address resolution in IPv4 and the neighbor unreachability detection mechanism. The IPv6 host sends Neighbor Solicitation message to discover the link-layer address of an on-link IPv6 node. IPv6 node sends the Neighbor Advertisement message in response to a NS and sends unsolicited NA to inform neighboring nodes of link-layer addresses.
- **ICMP redirect message**
  IPv6 router sends ICMP redirect message to inform an originating host of a better first-hop address for specific destination.

7.16.1 Stateful Auto Configuration

Router Advertisements sent from this interface have the Managed Address Configuration Flag or not. It decides that the hosts are thus permitted to use IPv6 stateless autoconfiguration to create global unicast addresses for themselves. This means that the attached hosts should use stateful autoconfiguration to obtain addresses if the flag is set.

To set the managed address configuration flag in IPv6 RA messages, use the following command.

Command	Mode	Description
ipv6 nd managed-config-flag	Interface	Sets the managed address configuration flag in RA.
no ipv6 nd managed-config-flag		Clears the managed address configuration flag from RA. (default)

To set the other stateful configuration flag in RA message, use the following command.

Command	Mode	Description
ipv6 nd other-config-flag	Interface	Sets the other stateful configuration flag in RA.
no ipv6 nd other-config-flag		Clears the other stateful configuration flag from RA. (default)

7.16.2 Configuring IPv6 Prefix

To configure how IPv6 prefixes are advertised in the IPv6 RA message, use the following command.

Command	Mode	Description
ipv6 nd prefix *X:X::X:X/M*	Interface	Configures how IPv6 prefixes are advertised in the RA message. X:X::X:X/M: IPv6 prefix 0-4294967295: valid lifetime 0-4294967295: preferred lifetime no-autoconfig: specifies prefix cannot be used for IPv6 autoconfiguration. off-link: specifies prefix to assigned to the link
ipv6 nd prefix *X:X::X:X/M* <0-4294967295> <0-4294967295> [**no-autoconfig** | **off-link**]		
no ipv6 nd prefix *X:X::X:X/M*		Deletes a configured how IPv6 prefixes are advertised in the RA message.

To configure existing IPv6 address on interface as ND prefix in the IPv6 RA message, use the following command.

Command	Mode	Description
ipv6 nd prefix default	Interface	Configures the existing IPv6 address assigned on an interface as ND prefix.
ipv6 nd prefix default <0-4294967295> <0-4294967295> [**no-autoconfig** | **off-link**]		Configures the existing IPv6 address assigned on an interface as ND prefix and sets its parameters.
no ipv6 nd prefix default		Clears a configured ND prefix using the existing IPv6 address of interface

7.16.3 Interval of RA Messages

To prevent synchronization with other IPv6 nodes, the actual value used should be randomly adjusted to within plus or minus 20 percent of the specified value. To configure the interval between IPv6 Router Advertisement transmissions from this interface, use the following command.

Command	Mode	Description
ipv6 nd ra-interval <3-1800> [<3-1350>]	Interface	Specifies the interval between IPv6 RA messages. (default: 600 seconds)

no ipv6 nd ra-interval		Deletes a configured interval between IPv6 RA messages

i The interval value should be less than or equal to the IPv6 Router Lifetime if this is a default router.

7.16.4 RA Destination Configuration

To configure the destination address of solicited RA (Router Advertisement) message which is supplied from source address of RS (Router Solicitation), use the following command.

Command	Mode	Description
ipv6 nd ra-destination rs	Interface	Configures the IPv6 router advertisement destination address. rs: router solicited source address
no ipv6 nd ra-destination rs		Deletes the configured IPv6 router advertisement destination address.

7.16.5 Router's Lifetime

This value is included in all IPv6 Router Advertisements sent out this interface. If the router is not a default router, this will have a value of zero. The default value is 1,800 seconds.

To configure the lifetime of a RA messages, use the following command.

Command	Mode	Description
ipv6 nd ra-lifetime <0-9000>	Interface	Specifies the lifetime of IPv6 RA message. (default: 1800 seconds)
no ipv6 nd ra-lifetime		Deletes a configured lifetime of IPv6 RA message

i If the router is a default router, this value will be non-zero and should not be less than the minimum Router Advertisement interval.

7.16.6 Reachable Time

RA reachable time is the amount of time that a remote IPv6 node is reachable for a specified time after a reachable confirmation event. The reachable time enables detecting unavailable neighbors. The configured reachable time is included in all router advertisements sent out of an interface so that nodes on the same link use the same time value.

To specify the reachable time that the switch can reach a remote IPv6 node after the reachability confirmation event has occurred, use the following command.

Command	Mode	Description
ipv6 nd reachable-time <0-	Interface	Specifies the reachable time. 0-3600000: IPv6 reachable time in milliseconds (A

3600000>		value of 0 indicates that the configured time is unspecified by this switch.)
no ipv6 nd reachable-time		Deletes a configured reachable time and restores the default time.

i

If the switch is configured with shorter reachable times, it enables detecting unavailable neighbors more quickly, however, shorter times consume more IPv6 network bandwidth and processing resources in all IPv6 network devices. We do not recommend configuring a short reachable time value.

For example, to configure the reachable time of 1000 milliseconds for Ethernet interface br2, enter the following commands:

```
SWITCH(config)# interface br2
SWITCH(config-if)# ipv6 nd reachable-time 1000
SWITCH(config-if)#
```

7.16.7 RA Suppression

If IPv6 unicast routing is enabled on an Ethernet interface, by default, this interface sends IPv6 router advertisement messages. However, by default, non-LAN interface types, for example, tunnel interfaces, do not send router advertisement messages.

To control transmission of IPv6 RA messages on the interface, use the following command.

Command	Mode	Description
ipv6 nd suppress-ra	Interface	Disables the sending of RA messages on an Ethernet interface.
no ipv6 nd suppress-ra		Sends RA messages on an interface.

7.16.8 Hop Limit

To configure the maximum number of hops used in RA messages and all IPv6 packets, use the following command.

Command	Mode	Description
ipv6 nd ra-hoplimit <0-255>	Interface	Configures the maximum number of hops in RA messages. 0-255: RA hop limit
no ipv6 nd ra-hoplimit		Returns the hop limit to its default value.

7.16.9 Retrans-time

To configure the interval between IPv6 neighbor solicitation retransmissions on an interface, use the following command.

Command	Mode	Description
ipv6 nd retrans-time <0-4294967295>	Interface	Specifies the interval between IPv6 neighbor solicitation retransmissions.

		0-4294967295: IPv6 NS retransmission time in milliseconds
no ipv6 nd retrans-time		Deletes a configured interval between IPv6 neighbor solicitation retransmissions.

7.16.10 ND Duplicate Address Detection (DAD)

To set the number of consecutive neighbor solicitation messages that are sent on an interface while duplicate address detection (DAD) is performed on the unicast IPv6 addresses of the interface, use the following command.

Command	Mode	Description
ipv6 nd dad attempts <0-600>	Interface	Configures the number of neighbor solicitation messages that are sent on an interface while DAD is performed on the unicast IPv6 addresses of the interface. 0-600: number of neighbor solicitation messages (A value of 0 disables DAD processing on the specified interface
no ipv6 nd dad attempts		Returns the number of messages to the default value.

7.16.11 Static IPv6 Neighbor Entry

The Neighbor Discovery (ND) protocol is a new messaging protocol that was created as part of IPv6 to perform a number of the tasks that ICMP and ARP accomplish in IPv4. Just like ARP, ND builds a cache of dynamic entries, and the administrator can configure the mapping between IPv6 address and MAC address to add static entries in the ND cache table.

To add a static entry in the ND cache table by specifying the mapping between an IPv6 address and a MAC address, use the following command.

Command	Mode	Description
ipv6 neighbor *X:X::X:X MACADDR*	Global	Sets a static neighbor entry, enter the IPv6 address and the MAC address. X:X::X:X: IPv6 address MACADDR: enter the MAC address.
ipv6 neighbor *X:X::X:X MACADDR INTERFACE*		Sets a static neighbor entry, enter the IPv6 address, MAC address and interface name. INTERFACE: enter an interface name. MACADDR: enter the MAC address.

To remove the configured static entry from the ND cache table, use the following command.

Command	Mode	Description
no ipv6 neighbor [*X:X::X:X*]	Global	Remove the configured static entry from the ND cache

no ipv6 neighbor *X:X::X:X INTERFACE*		table

7.16.12 Setting the Stale Timer

Reachability of the IPv6 neighbors is confirmed only after the stale timer has expired. For example, by setting the stale timer to 80000 seconds, users can specify that IPv6 neighbor reachability be confirmed every 80000 seconds.

To set the stale timer for IPv6 neighbor reachability confirmation, use the following command.

Command	Mode	Description
ipv6 neighbor stale-time <10-4294967295>	Global	Sets the stale timer for IPv6 neighbor reachability. Default: 86400 seconds
no ipv6 neighbor stale-time		Reverts the default stale timer.

7.16.13 IPv6 Neighbor Discovery (ND) Inspection

IPv6 Neighbor Discovery (ND) inspection feature can protect switches against IPv6 address spoofing. It provides IPv6 communication by mapping an IPv6 address to a MAC address. However, a malicious user can attack ND caches of system by intercepting the traffic intended for other hosts on the subnet. ND inspection is a security feature that validates ND packets in a network. It discards ND packets with invalid IP-MAC address binding.

To activate/deactivate the ND inspection function on a VLAN, use the following command.

Command	Mode	Description
ipv6 nd inspection vlan *VLANS*	Global	Activates ND inspection on a VLAN. VLANS: VLAN ID (1-4094)
no ipv6 nd inspection vlan *VLANS*		Deactivates ND inspection on a VLAN.

7.16.13.1 ND Access List

You can exclude a given range of IP addresses from the ND inspection using ND access lists. ND access lists are created by the **ipv6 nd access-list** command on the *Global Configuration* mode. ND access list permits or denies the ND packets of a given range of IPv6 addresses.

To create/delete ND access control list (ACL), use the following command.

Command	Mode	Description
ipv6 nd access-list *NAME*	Global	Opens ND ACL configuration mode and creates a ND access list. NAME: ND access list name
no ipv6 nd access-list *NAME*		Deletes a ND access list.
ipv6 nd access-list delete all		Deletes all ND access lists.

After opening *ND Access List Configuration* mode, the prompt changes from SWITCH(config)# to SWITCH(config-nd-acl[*NAME*])#. After opening *ND ACL Configuration* mode, a range of IPv6 addresses can be configured to apply ND inspection.

i By default, ND Access List discards the Neighbor Discovery protocol packets, of all IPv6 addresses and MAC addresses.

To specify the IPv6 address and MAC address to forward the ND messages, use the following command.

Command	Mode	Description
permit ipv6 {**host** *X:X::X:X* | *X:X::X:X/M* | **any**} **mac** {**any** | **host** *MACADDR*}	ND-ACL	Permits ND packets based on their IPv6 address and MAC address, which have not learned before on ND inspection table. mac any: ignores sender MAC address ipv6 any: ignores sender IPv6 address host: sender host X:X::X:X: sender IPv6 address X:X::X:X/M: sender IPv6 network address MACADDR: sender MAC address
permit ipv6 range *X:X::X:X X:X::X:X* **mac any**		Permits ND packets of a given range of IPv6 addresses. X:X::X:X: start/end IPv6 address of sender

To delete the configured range of IPv6 address or MAC address to permit ND packets, use the following command.

Command	Mode	Description
no permit ipv6 {**host** *X:X::X:X* | *X:X::X:X/M* | **any**} **mac** {**any** | **host** *MACADDR*}	ND-ACL	Deletes the configured range of IPv6 address to permit ND packets. any: ignores sender MAC address host: sender host MACADDR: sender MAC address X:X::X:X: start/end IPv6 address of sender X:X::X:X/M: sender IPv6 network address
no permit ipv6 range *X:X::X:X X:X::X:X* **mac any**		

To specify the IPv6 address and MAC address to deny ND packets, use the following command.

Command	Mode	Description
deny ipv6 {**host** *X:X::X:X* | *X:X::X:X/M* | **any**} **mac** {**any** | **host** *MACADDR*}	ND-ACL	Discards ND packets based on their IPv6 address and MAC address, which have not learned before on ND inspection table. mac any: ignores sender MAC address ipv6 any: ignores sender IPv6 address host: sender host

		X:X::X:X: sender IPv6 address X:X::X:X/M: sender IPv6 network address MACADDR: sender MAC address
deny ipv6 {**host** *X:X::X:X* | *X:X::X:X/M* | **any**} **mac pattern** *WORD* **offset** <0-5>		Discards ND packets based on their IPv6 address and MAC pattern, which have not learned before on ND inspection table. ipv6 any: ignores sender IPv6 address host: sender host X:X::X:X: sender IPv6 address X:X::X:X/M: sender IPv6 network address WORD: sender MAC pattern value 0-5: offset value
deny ipv6 range *X:X::X:X X:X::X:X* **mac any**		Discards ND packets of a given range of IPv6 addresses. X:X::X:X: start/end IPv6 address of sender

To delete the configured IPv6 address and MAC address for discarding ND packets, use the following command.

Command	Mode	Description
no deny ipv6 {**host** *X:X::X:X* | *X:X::X:X/M* | **any**} **mac** {**any** | **host** *MACADDR*}	ND-ACL	Deletes a configured range of IP address to discard ND packets. any: ignores sender MAC address host: sender host MACADDR: sender MAC address X:X::X:X: start/end IPv6 address of sender X:X::X:X/M: sender IPv6 network address
no deny ipv6 {**host** *X:X::X:X* | *X:X::X:X/M* | **any**} **mac pattern** *WORD* **offset** <0-5>		
no deny ipv6 range *X:X::X:X X:X::X:X* **mac any**		

By the following command, the ND access list also refers to a DHCP snooping binding table to permit the ND packets for DHCP users. This feature enables the system to permit ND packets only for the IPv6 addresses on the DHCP snooping binding table. The ND access list with the DHCP snooping allows IP communications to users authorized by the DHCP snooping. The source IP address and MAC address of each packet are checked against the table, and if a valid match is not found, the packet is dropped.

To permit/discard ND packets for the users authorized by the DHCPv6 snooping, use the following command.

Command	Mode	Description
permit dhcpv6-snoop-inspection	ND-ACL	Permits ND packets of users authorized by the DHCPv6 snooping.
no permit dhcpv6-snoop-inspection		Discards the configured ND packets of users authorized by the DHCPv6 snooping.

To display the configured ND access lists, use the following command.

Command	Mode	Description
show ipv6 nd access-list [*NAME*]	Global	Displays the existing ND access lists.

7.16.13.2 Enabling ND Inspection Filtering

To enable/disable the ND inspection filtering of a certain range of IPv6 addresses from the ND access list, use the following command.

Command	Mode	Description
ipv6 nd inspection filter *NAME* **vlan** *VLANS*	Global	Enables ND inspection filtering with the configured ND access list on the VLAN. NAME: ND access list name
no ipv6 nd inspection filter *NAME* **vlan** *VLANS*		Disables ND inspection filtering with a configured ND access list on specified VLAN.

i ND inspection actually runs in the system after the configured ND access list applies to specific VLAN ID using the **ip nd inspection filter** command.

7.16.13.3 ND Inspection on Trust Port

The ND inspection defines 2 trust states, trusted and untrusted. Incoming packets via trusted ports bypass the ND inspection process, while those via untrusted ports go through the ND inspection process. Normally, the ports connected to subscribers are configured as untrusted, while the ports connected to an upper network are configured as trusted.

To set a trust state on a port for the ND inspection, use the following command.

Command	Mode	Description
ipv6 nd inspection trust port *PORTS*	Global	Sets a trust state on a port as trusted PORTS: port number
no ipv6 nd inspection trust port *PORTS*		Sets a trust state on a port as untrusted PORTS: port number

To display the configured trust port of the ND inspection, use the following command.

Command	Mode	Description
show ipv6 nd inspection trust [**port** *PORTS*]	Enable Global Bridge	Shows the configured trust port of the ND inspection.

7.16.13.4 ND Inspection Log-buffer

Log-buffer function shows the list of subscribers who have been used invalid fixed IP addresses. This function saves the information of users who are discarded by ND inspection and generates periodic syslog messages.

Log-buffer function is automatically enabled with ND inspection. If OLT receives invalid or denied ND packets by ND inspection, it creates the table of entries that include the information of port number, VLAN ID, source IP address, source MAC address and time. In addition, you can specify the maximum number of entries.

After one of entries is displayed as a syslog message, it is removed in the order in which the entries appear in the list.

To configure the options of log-buffer function, use the following command.

Command	Mode	Description
ipv6 nd inspection log-buffer entries <0-1024>	Global	Specifies the number of entries in log-buffer. 0-1024: the max. number of entries (default: 32)
ipv6 nd inspection log-buffer logs <0-1024> **interval** <0-86400>		Sets the interval for displaying syslog messages of entries. 0-1024: the number of syslog messages per specified interval (default: 5) 0-86400: interval value in second (default: 1 second)

To delete the configured options of log-buffer function, use the following command.

Command	Mode	Description
no ipv6 nd inspection log-buffer {**entries** | **logs**}	Global	Deletes the configured options of log-buffer function.

To display the configured log-buffer function and entries' information, use the following command.

Command	Mode	Description
show ipv6 nd inspection log	Enable Global Bridge	Displays the configured log-buffer function.

To clear all of collected entries in the list, use the following command.

Command	Mode	Description
clear ipv6 nd inspection log	Enable Global Bridge	Clears all of collected entries in the log-buffer list.

7.16.13.5 ND Inspection Delay Time

This function sets the time before ND inspection starts to run. Before setting this feature, ND inspection should be enabled. ND inspection checks validity of incoming ND packets by using DHCP snooping binding table and denies the ND packets if they are not

identified in the table.

However, the OLT may be rebooted with any reason, then DHCP snooping binding table entries, which are dynamically learned from DHCP packets back and forth the OLT, would be lost. Thus, ND inspection should be delayed to start during some time so that DHCP snooping table can build entries. If no time is given, ND inspection sees empty snooping table and drop every ND packet.

To specify the ND inspection delay time, use the following command.

Command	Mode	Description
ipv6 dhcp snooping nd-inspection start <1-2147483637>	Global	Configures the ND inspection delay time. If reboot, ND inspection resumes after the time you configure. 1-2147483637: delay time (unit: second, default:1800 seconds)
no ipv6 dhcp snooping nd-inspection start		Delete the configured ND inspection delay time.

7.16.13.6 Displaying ND Inspection

To display a status of the ND inspection, use the following command.

Command	Mode	Description
show ipv6 nd inspection [**vlan** *VLANS*]	Enable Global Bridge	Shows a status of the ND inspection.
show ipv6 nd inspection statistics [**vlan** *VLANS*]		Shows collected statistics of the ND inspection.

To clear the collected statistics of the ND inspection, use the following command.

Command	Mode	Description
clear ipv6 nd inspection statistics [**vlan** *VLANS*]	Enable Global Bridge	Clears collected statistics of the ND inspection.

7.16.14 Gratuitous ND

Gratuitous ND is a broadcast packet like an ND request. It containing IPv6 address and MAC address of gateway, and the network is accessible even though IPv6 addresses of a specific host's gateway are repeatedly assigned to the other.

To configure the interval and transmission count for Gratuitous ND messages, use the following command. And set the transmission start-delivery time in order to transmit Gratuitous ND after ND reply. Gratuitous ND is transmitted after some time from transmitting ND reply.

Command	Mode	Description
ipv6 nd patrol *TIME COUNT* [*TIME*]	Global	Configures a gratuitous ND. TIME: transmit interval COUNT: the number of attempts to send Gratuitous ND

no ipv6 nd patrol		Disables the configured parameters of Gratuitous ND.

7.16.15 ND Alias

Although clients are joined in the same client switch, it may be impossible to communicate between them for security reasons. When you need to make them communicate each other, the OLT supports ND alias, which responses the ARP request from client net through the concentrating switch.

To register the IPv6 address of client net range in ND alias, use the following command.

Command	Mode	Description
nd alias *X:X::X:X X:X::X:X* [*XX:XX:XX:XX:XX:XX*]	Global	Registers the IPv6 address range and MAC address in ND alias to make the system response to an ND request.
nd alias *X:X::X:X X:X::X:X* **vlan** *VLAN* **gateway** *GATEWAY*		Registers gateway IPv6 address within IPv6 address range to make the system response automatically MAC address of gateway. VLAN: 1-4094 GATEWAY: gateway IPv6 address
no nd alias *X:X::X:X X:X::X:X*		Deletes the registered IPv6 address range of ND alias.

i Unless you input a MAC address, the MAC address of user's device will be used for ND response.

To set aging time of gateway IPv6 address in ND alias, use the following command.

Command	Mode	Description
nd alias aging-time <5-2147483647>	Global	Sets the aging time of gateway IPv6 address. 5-2147483647: aging time (default: 300 seconds)
no nd alias aging-time		Deletes the aging time of gateway IPv6 address.

To display a registered ND alias, use the following command.

Command	Mode	Description
show nd alias	Enable Global Bridge	Shows a registered ND alias.

7.16.16 Displaying Neighbor Discovery

To display IPv6 neighbor discovery cache information table, use the following command.

Command	Mode	Description

show ipv6 neighbors [{*X:X::X:X* | *X:X::X:X/M*}]	Enable Global Bridge	Shows IPv6 neighbors discovery cache information.
show ipv6 neighbors *INTERFACE*		

To clear IPv6 neighbor discovery cache information table, use the following command.

Command	Mode	Description
clear ipv6 neighbors [{*X:X::X:X* | *X:X::X:X/M*}]	Enable Global Bridge	Clears IPv6 neighbor discovery cache information.
clear ipv6 neighbors *INTERFACE*		

7.17 ICMP Message Control

ICMP stands for Internet Control Message Protocol. When it is impossible to transmit data or configure route for data, ICMP sends error message about it to host. The first 4 bytes of all ICMP messages are same, but the other parts are different according to type field value and code field value. There are fifteen values of field to distinguish each different ICMP message, and code field value helps to distinguish each type in detail.

The following table shows explanation for fifteen values of ICMP message type.

Type	Value	Type	Value
ICMP_ECHOREPLY	0	ICMP_DEST_UNREACH	3
ICMP_SOURCE_QUENCH	4	ICMP_REDIRECT	5
ICMP_ECHO	8	ICMP_TIME_EXCEEDED	11
ICMP_PARAMETERPROB	12	ICMP_TIMESTAMP	13
ICMP_TIMESTAMPREPLY	14	ICMP_INFO_REQUEST	15
ICMP_INFO_REPLY	16	ICMP_ADDRESS	17
ICMP_ADDRESSREPLY	18	-	-

Tab. 7.1 ICMP Message Type

The following figure shows simple ICMP message structure.

0 – 7	8 – 15	16 – 31
8-bit Type	8-bit Code	16-bit Checksum
(Contents Depend on Type and Code)		

Fig. 7.16 ICMP Message Structure

It is possible to control ICMP message through user's configuration. You can configure to block the echo reply message to the partner who is doing ping test to device and interval to transmit ICMP message.

7.17.1 Blocking Echo Reply Message

It is possible to configure block echo reply message to the partner who is doing ping test to switch. To block echo reply message, use the following command.

Command	Mode	Description
ip icmp ignore echo all	Global	Blocks echo reply message to all partners who are taking ping test to device.
ip icmp ignore echo broadcast		Blocks echo reply message to partner who is taking broadcast ping test to device.

To release the blocked echo reply message, use the following command.

Command	Mode	Description
no ip icmp ignore echo all	Global	Releases blocked echo reply message to all partners who are taking ping test to device.
no ip icmp ignore echo broadcast		Releases blocked echo reply message to partner who is taking broadcast ping test to device.

7.17.2 Interval for Transmit ICMP Message

User can configure the interval for transmit ICMP message. After you configure the interval, ICMP message will be blocked until the configured time based on the last message is up. For example, if you configure the interval as 1 second, ICMP will not be sent within 1 second after the last message has been sent.

To configure interval to transmit ICMP message, the administrator should configure the type of message and the interval time.

Use the following command, to configure the interval for transmit ICMP message.

Command	Mode	Description
ip icmp interval rate-mask *MASK*	Global	Configures the interval for transmit ICMP message. MASK: user should input hexadecimal value until 0xFFFFFFFF. The default is 0x1818.

If mask that is input as hexadecimal number is calculated as binary number “1” means “Status ON”, “0” means “Status OFF”. In binary number, if the digit showed as “1” matches with the value of ICMP message. It means ICMP Message is selected as “Status ON”. Digit value starts from 0.

For example, if hexadecimal number “8” is changed as binary number, it is “1000”. In 1000, 0 digit is “0” and 1 digit is “0”, 2 digit is “0” and 3 digit is “1”. The digit showed as “1” is “3” and ICMP_DEST_UNREACH means ICMP value is “3”. Therefore, ICMP_DEST_UNREACH is chosen the message of limiting the transmission time.

Default is 0x1818. If 1818 as hexadecimal number is changed as binary number, it is 1100000011000. By calculating from 0 digit, 3 digit, 4 digit, 11 digit, 12 digit is “1” and it is “STATUS ON”. Therefore, the message that corresponds to 3, 4, 11, and 12 is chosen as the message limiting the transmission rate.

Tab. 7.2 shows the result of mask calculation of default value.

Type	Status
ICMP_ECHOREPLY (0)	OFF
ICMP_DEST_UNREACH (3)	ON
ICMP_SOURCE_QUENCH (4)	ON
ICMP_REDIRECT (5)	OFF
ICMP_ECHO (8)	OFF
ICMP_TIME_EXCEEDED (11)	ON
ICMP_PARAMETE	ON

RPROB (12)	
ICMP_TIMESTAMP (13)	OFF
ICMP_TIMESTAMPREPLY (14)	OFF
ICMP_INFO_REQUEST (15)	OFF
ICMP_INFO_REPLY (16)	OFF
ICMP_ADDRESS (17)	OFF
ICMP_ADDRESSREPLY (18)	OFF

Tab. 7.2 Mask Calculation of Default Value

To configure the limited ICMP transmission time, use the following command.

Command	Mode	Description
ip icmp interval rate-limit *INTERVAL*	Global	Configures a limited ICMP transmission time. INTERVAL: 0-2000000000 (unit: 10 ms)

i The default ICMP interval is 1 second (100 ms).

To return to default ICMP configuration, use the following command.

Command	Mode	Description
ip icmp interval default	Global	Returns to default configuration.

To display ICMP interval configuration, use the following command.

Command	Mode	Description
show ip icmp interval	Enable Global Bridge	Shows ICMP interval configuration.

7.17.3 ICMP Destination Unreachable Message

If the switch receives a packet that has an unknown protocol or no route to the destination address, the switch sends an ICMP unreachable message to its source address. What if too many ICMP unreachable messages should be sent from the switch, it might cause slow down the system operation.

To enable/disable generation of ICMP unreachable messages, use the following command.

Command	Mode	Description
ip unreachables	Interface	Enables sending ICMP unreachable messages on the interface.
no ip unreachables		Disables sending ICMP unreachable messages on the interface.

7.17.4 ICMP Redirect Message

ICMP redirect messages are used when a router recognizes a packet arriving on an interface and the best route is out that same interface. In that case the router sends an ICMP redirect message back to the source telling about a better router on the same subnet.

To enable/disable generation of ICMP redirect messages, use the following command.

Command	Mode	Description
ip redirects	Interface	Enables sending ICMP redirect messages on the interface. (default)
no ip redirects		Disables sending ICMP redirect messages on the interface.

7.18 TCP Flag Control

Transmission Control Protocol (TCP) header includes six kinds of flags that are URG, ACK, PSH, RST, SYN, and FIN. For the OLT, you can configure RST and SYN as the below.

7.18.1 RST Configuration

RST sends a message when TCP connection cannot be done to a person who tries to make it. However, it is also possible to configure to block the message. This function will help prevent that hackers can find impossible connections.

To configure not to send the message that informs TCP connection cannot be done, use the following command.

Command	Mode	Description
ip tcp ignore rst-unknown	Global	Configures to block the message that informs TCP connection cannot be done.
no ip tcp ignore rst-unknown		Disables the unknown RST ignoring.

7.18.2 SYN Configuration

SYN sets up TCP connection. The OLT transmits cookies with SYN to a person who tries to make TCP connection. Only when transmitted cookies are returned, it is possible to permit TCP connection. This function prevents connection overcrowding because of accessed users who are not using and helps the other users use service.

To permit connection only when transmitted cookies are returned after sending cookies with SYN, use the following command.

Command	Mode	Description
ip tcp syncookies	Global	Permits only when transmitted cookies are returned after sending cookies with SYN.
no ip tcp syncookies		Disables configuration to permit only when transmitted cookies are returned after sending cookies with SYN.

7.19 The Utilization on L3 table

To display the urtilization of packets in use on L3 table, LPM entries and L3 interfaces, use the following command.

Command	Mode	Description
show ip tables summary	Enable Global	Shows the usage of L3 interface, host, LPM, ECMP entries.

To specify the L3 table aging time, use the following command.

Command	Mode	Description
ip tables aging-time <10-4294967295>	Global	Specifies the L3 table aging time (default: 300s).

7.20 Packet Dump

Failures in network can occurr by certain symptom. Each symptom can be traced to one or more problems by using specific troubleshooting tools. The OLT switch provides the debug command to dump packet. Use debug commands only for problem isolation. Do not use it to monitor normal network operation. The debug commands produce a large amount of processor overhead.

7.20.1 Packet Dump by Protocol

You can see packets about BOOTPS, DHCP, ARP and ICMP using the following command.

Command	Mode	Description
debug packet {**interface** *INTERFACE* | **port** *PORTS*} **protocol** {**bootps** | **dhcp** | **arp** | **icmp**} {**src-ip** *A.B.C.D* | **dest-ip** *A.B.C.D*}	Enable Global	Shows packet dump by protocol.
debug packet {**interface** *INTERFACE* | **port** *PORTS*} **host** {**src-ip** *A.B.C.D* | **dest-ip** *A.B.C.D*} {**src-port** <1-65535> | **dest-port** <1-65535>}		Shows host packet dump.
debug packet {**interface** *INTERFACE* | **port** *PORTS*} **multicast** {**src-ip** *A.B.C.D* | **dest-ip** *A.B.C.D*}		Shows multicast packet dump.

7.20.2 Packet Dump with Option

You can verify packets with tcpdump options using the following command.

Command	Mode	Description
debug packet *OPTION*	Enable Global	Shows packet dump using options.

The following table shows the options for packet dump.

Option	Description
-a	Change Network & Broadcast address to name.
-d	Change the complied packet-matching code to readable letters and close it
-e	Output link-level header of each line
-f	Output outer internet address as symbol
-l	Buffer output data in line. This is useful when other application tries to receive data from tcpdump.
-n	Do not translate all address (e.g. port, host address)
-N	When output host name, do not print domain.
-O	Do not run packet-matching code optimizer. This option is used to find bug in optimizer
-p	Interface is not remained in promiscuous mode
-q	Reduce output quantity of protocol information. Therefore, output line is shorter.
-S	Output TCP sequence number not relative but absolute
-t	Time is not displayed on each output line
-v	Display more information
-w	Save the captured packets in a file instead of output
-x	Display each packet as hex code
-c *NUMBER*	Close the debug after receive packets as many as the number
-F *FILE*	Receive file as filter expression. All additional expressions on command line are ignored.
-i *INTERFACE*	Designate the interface where the intended packets are transmitted. If not designated, it automatically select a interface which has the lowest number within the system interfaces (Loopback is excepted)
-r FILE	Read packets from the file which created by '-w' option.
-s *SNAPLEN*	This is used to configure sample packet except the 68 byte default value. The 68 byte is appropriate value for IP, ICMP, TCP and UDP, but it can truncate protocol information of Name server or NFS packets. If sample size is long, the system should take more time to inspect and packets can be dropped for small buffer size. On the contrary, if the sample size is small, information can be leaked as the amount. Therefore, user should adjust the size as header size of protocol.
-T TYPE	Display the selected packets by conditional expression as the intended type. rpc (Remote Procedure Call) rtp (Real-time Transport Protocol) rtcp (Real-time Transport Control Protocol) vat (Visual Audio Tool) wb (distributed White Board)
EXPRESSION	Conditional expression

Tab. 7.5 Options for Packet Dump

7.20.3 Debug Packet Dump

The OLT provides network debugging function to prevent system overhead for unknown packet inflow. Monitoring process checks CPU load per 5 seconds. If there is more traffic than threshold, user can capture packets using tcpdump and save it to file. You can download the dump file with the name of file-number.dump after FP connection to the system. See the dumped packet contents with a packet analyze program. To debug packet dump, use the following command.

Command	Mode	Description
debug packet log *COUNT VALUE TIME* [<1-10>]	Enable Global	Shows dump file according to a condition. COUNT: packet counting VALUE: CPU threshold 1-10: file number
no debug packet log		Deletes the information of packet dump log.

i

You can save a current configuration with the **write memory** command. However, the dump file will not be saved.

7.20.4 Displaying Dump Packets

To display the dump packets, use the following command.

Command	Mode	Description
show dump packets	Enable/Global	Shows the dump packets.

7.20.5 Dump File

To back up a dump file using FTP or TFTP, use the following command.

Command	Mode	Description
copy {**ftp** | **tftp**} **dumpfile upload** [*FILE-NAME*]	Enable	Uploads a dump file to FTP or TFTP server with the name configured by user.

i

To access FTP to back up the configuration or use the backup file, you should know FTP user ID and the password. To back up the dump file through FTP, you can recognize the file transmission because hash function is automatically turned on.

To delete a dump file, use the following command.

Command	Mode	Description
delete dumpfile [*FILENAME*]	Enable	Deletes a specified dump file. FILENAME: dump file name

To display a list of dump files, use the following command.

Command	Mode	Description

show dumpfile-list	Enable	Shows a current startup configuration.

7.21 Access List

An IP access list (ACL) is a filter that enables you to restrict specific IP traffic. If you create an ACL entry to filter multicast packets based on their destination IP address, the OLT can deny the packets matching to the destination IP address, a multicast address.

There are three types of IP ACLs you can configure:

- Standard Access List
- Extended Access List
- Named Access List

Standard ACLs uses IP addresses (whether they are source address or not) for matching conditions. On the other hand, Extended ACLs define detailed filters with source IP, source mask, destination IP, and destination mask. More concrete filtering could be done with the extended ACL. IP ACLs also can be named with any characters and the numbers not defined in both standard and extended ACLs.

In most cases, you can simply define ACLs in *Global Configuration* mode. If you want to apply them to any of L3 functions, you can perform it where the actual access control should be made. However, ARP has an exception. ARP has an access list itself, and you cannot define an access list in the *Global Configuration* mode.

Processing ACLs

An ACL entry has several statements. That is, an ACL entry 1 can have multiple filtering statements (conditions) as the following:

```
SWITCH(config)# access-list 1 deny 10.55.193.109
SWITCH(config)# access-list 1 permit 10.55.193.109 0.0.0.255
SWITCH(config)# access-list 1 deny any
```

Traffic that comes into the switch is compared to ACL entries based on the order that the entries have been created in the switch. New entries are added to the end of the list. The switch continues to look until it has a match. If no matches are found when the switch reaches the end of the list, the traffic is permitted. Likewise, if a couple of statements exist within one ACL entry and traffic comes in, the switch looks through the statements in the order that they are created. If the traffic hits the first condition, the switch processes as described in the first condition and next conditions are ignored.

```
SWITCH(config)# access-list 1 deny 10.55.193.109
SWITCH(config)# access-list 1 permit 10.55.193.109 0.0.0.255
SWITCH(config)# access-list 1 deny any
```

Wildcard Bits

Masks are used with IP addresses in IP ACLs to specify a range of IP addresses. Compared to subnet mask, masks for IP ACLs are the reverse. The mask bits 0.0.0.255 in IP ACL are same as 255.255.255.0 in subnet mask, for instance. This is called a wildcard mask or an inverse mask, because 1 and 0 in the binary format means the opposite of what they mean in a subnet mask; 0 meaning “check” and 1 meaning “ignore.”

IP Address	Wildcard Bits	Addresses that ACL controls

10.55.10.2	0.0.0.255	10.55.10.1 – 10.55.10.255
10.55.10.2	0.0.0.0	10.55.10.2

Tab. 7.3 Examples of Wildcard Masking

If you put 10.55.10.2 and 0.0.0.255 for an IP address and wildcard mask to permit, all traffic that begins with 10.55.10.1 to 10.55.10.255 (10.55.10.0/24) are accepted. If you set any IP address with wildcard bits 0.0.0.0, it indicates the IP address itself that should be processed.

7.21.1 Standard Access List

To create a standard IP address-based access list entry, use the following command.

Command	Mode	Description
access-list {<1-99> | <1300-1999>} {**deny** | **permit**} *A.B.C.D* [*WILDCARD-BITS*]	Global	Specifies a deny or permit statement of the standard ACL with IP addresses and wildcard bits 1-99: IP standard access list 1300-1999: IP standard access list (extended range) deny: denies packets if conditions are matched. permit: permits packets if conditions are matched. A.B.C.D: IP address to match WILDCARD-BITS: bits for use of wildcard masking
access-list {<1-99> | <1300-1999>} {**deny** | **permit**} **any**		Specifies a deny or permit statement of the standard ACL with any source host. any: any source host
access-list {<1-99> | <1300-1999>} {**deny** | **permit**} **host** *A.B.C.D*		Specifies a deny or permit statement of the standard ACL with a specific host. A.B.C.D: host address to match
access-list {<1-99> | <1300-1999>} **remark** *LINE*		Adds comments for the standard ACL. LINE: access list entry comments up to 100 characters

i Add entries to the list by repeating the command for different IP addresses.

To delete an existing standard IP address-based access list entry, use the following command.

Command	Mode	Description
no access-list {<1-99> | <1300-1999>} {**deny** | **permit**} *A.B.C.D* [*WILDCARD-BITS*]	Global	Deletes an entry of the standard ACL.
no access-list {<1-99> | <1300-		

1999>} {**deny** | **permit**} **any**		
no access-list {<1-99> | <1300-1999>} {**deny** | **permit**} **host** *A.B.C.D*		
no access-list {<1-99> | <1300-1999>} **remark** *LINE*		

Sample Configuration

This is an example of creating the standard ACL entries.

```
SWITCH(config)# access-list 5 permit 10.55.10.2 0.0.0.255
SWITCH(config)# access-list 5 deny 10.55.1.1 0.0.0.255
SWITCH(config)#
```

7.21.2 Extended Access List

To create an extended IP address-based access list entry, use the following command.

Command	Mode	Description
access-list {<100-199> | <2000-2699>} {**deny** | **permit**} **ip** *A.B.C.D WILDCARD-BITS A.B.C.D WILDCARD-BITS*	Global	Specifies a deny or permit statement of the extended ACL with source/destination addresses and their wild masks. 100-199: IP extended access list 2000-2699: IP extended access list (extended range) deny: denies packet if conditions are matched. permit: permits packet if conditions are matched. ip: any Internet Protocol A.B.C.D: source/destination IP address to match WILDCARD-BITS: bits for use of source/destination IP address wildcard masking
access-list {<100-199> | <2000-2699>} {**deny** | **permit**} **ip host** *A.B.C.D A.B.C.D WILDCARD-BITS*		Specifies a deny or permit statement of the extended ACL with a single source host and other variables. host: single source host A.B.C.D: source/destination IP address of a host to match WILDCARD-BITS: bits for use of host destination IP address wildcard masking

Command	Mode	Description
access-list {<100-199> | <2000-2699>} {**deny** | **permit**} **ip host** *A.B.C.D* **any**	Global	Specifies a deny or permit statement of the extended ACL with a single source host and other variables. host: single source host A.B.C.D: source IP address of a host to match any: destination host
access-list {<100-199> | <2000-		Specifies a deny or permit statement of the extended

Command	Mode	Description
2699>} {**deny** | **permit**} **ip host** *A.B.C.D* **host** *A.B.C.D*		ACL with a single source host and other variables. host: single source/destination host A.B.C.D: source/destination IP address of a host to match
access-list {<100-199> | <2000-2699>} {**deny** | **permit**} **ip any** *A.B.C.D WILDCARD-BITS*		Specifies a deny or permit statement of the extended ACL with any source host and other variables. any: any source host A.B.C.D: destination IP address to match WILDCARD-BITS: bits for use of destination IP address wildcard masking
access-list {<100-199> | <2000-2699>} {**deny** | **permit**} **ip any any**		Specifies a deny or permit statement of the extended ACL with any source host and other variables. any: any source host any: any destination host
access-list {<100-199> | <2000-2699>} {**deny** | **permit**} **ip any host** *A.B.C.D*		Specifies a deny or permit statement of the extended ACL with any source host and other variables. any: any source host host: single destination host A.B.C.D: destination IP address to match
access-list {<100-199> | <2000-2699>} **remark** *LINE*		Adds comments for the extended ACL. LINE: access list entry comments up to 100 characters

i

Add entries to the list by repeating the command for different IP addresses.

To delete an existing extended IP address-based access list entry, use the following command.

Command	Mode	Description
no access-list {<100-199> | <2000-2699>} {**deny** | **permit**} **ip** *A.B.C.D WILDCARD-BITS A.B.C.D WILDCARD-BITS*	Global	Deletes an entry of the extended ACL.
no access-list {<100-199> | <2000-2699>} {**deny** | **permit**} **ip host** *A.B.C.D A.B.C.D WILDCARD-BITS*		
no access-list {<100-199> | <2000-2699>} {**deny** | **permit**} **ip host** *A.B.C.D* **any**		

Command	Mode	Description
no access-list {<100-199> | <2000-2699>} {**deny** | **permit**} **ip host** *A.B.C.D* **host** *A.B.C.D*	Global	Deletes an entry of the extended ACL.
no access-list {<100-199> |		

Command	Mode	Description
<2000-2699>} {**deny** | **permit**} **ip any** *A.B.C.D A.B.C.D WILDCARD-BITS*		
no access-list {<100-199> | <2000-2699>} {**deny** | **permit**} **ip any any**		
no access-list {<100-199> | <2000-2699>} {**deny** | **permit**} **ip any host** *A.B.C.D*		
no access-list {<100-199> | <2000-2699>} **remark** *LINE*		

Sample Configuration

This is an example of creating the extended ACL entries.

```
SWITCH(config)# access-list 100 permit ip 10.55.10.2 0.0.0.255 10.55.193.5
0.0.0.255
SWITCH(config)# access-list 100 deny ip 10.12.154.1 0.0.0.255 10.12.202.1
0.0.0.255
SWITCH(config)#
```

7.21.3 Named Access List

It defines an IP access list by name and any numeric characters that have not been defined from both standard ACL and extended ACL.

To create a named IP access list entry, use the following command.

Command	Mode	Description
access-list *WORD* {**deny** | **permit**} *A.B.C.D/M* [**exact-match**]	Global	Specifies the named ACL entry with a prefix. WORD: access list name deny: denies packet if conditions are matched. permit: permits packet if conditions are matched. A.B.C.D/M: prefix to match exact-match: exact match against the prefixes
access-list *WORD* {**deny** | **permit**} **any**		Specifies the named ACL with any destination IP address. WORD: access list name deny: denies packet if conditions are matched. permit: permits packet if conditions are matched. any: any destination IP address
access-list *WORD* **remark** *LINE*		Adds comments for the named ACL. LINE: access list comments up to 100 characters

i Add entries to the list by repeating the command for different IP addresses.

To delete an entry of the named ACL, use the following command.

Command	Mode	Description
no access-list *WORD* {**deny** | **permit**} *A.B.C.D/M* [**exact-match**]	Global	Deletes an entry of the named ACL.
no access-list *WORD* {**deny** | **permit**} **any**		
no access-list *WORD* **remark** *LINE*		

Sample Configuration

This is an example of creating a named ACL entry.

```
SWITCH(config)# access-list sample_ACL permit 10.55.193.109/24
SWITCH(config)#
```

7.21.4 Access List Range

To add a user-defined range of the access lists for convenience, use the following command.

Command	Mode	Description
access-list-range {<1-1024> | *WORD*} {**deny | permit**} *A.B.C.D A.B.C.D*	Global	Applies the user-defined access list range and specifies those packets to reject/forward. 1-1024: IP standard access list range WORD: IP access-list-range name deny: denies access of packet if conditions are matched. permit: permits access of packet if conditions are matched. A.B.C.D: start/end IP address to specify the range any: any source address
access-list-range {<1-1024> | *WORD*} {**deny | permit**} **any**		

To delete a configured range of access list entries, use the following command.

Command	Mode	Description
no access-list-range {<1-1024> | *WORD*} [{**deny | permit**} *A.B.C.D A.B.C.D*]	Global	Deletes a configured range of access lists for rejecting/forwarding those packets. 1-1024: IP standard access list range WORD: IP access-list-range name A.B.C.D: start/end IP address to specify the range any: any source address
no access-list-range {<1-1024> | *WORD*} [{**deny | permit**} **any**]		

To write comments for the specified access list range, use the following command.

Command	Mode	Description
access-list-range {<1-1024> |	Global	Writes comments for the specified ACL range.

WORD} **remark** *LINE*		1-1024: IP standard access list range WORD: IP access-list-range name LINE: access list entry comments up to 100 characters
no access-list-range {<1-1024> | *WORD*} **remark** [*LINE*]		Deletes the comments for the specific ACL range.

7.21.5 Named Access List for IPv6 address

To create a named IPv6 access list entry, use the following command.

Command	Mode	Description
ipv6 access-list *WORD* {**deny | permit**} *X:X::X:X/M* [**exact-match**]	Global	Specifies the named ACL entry with a prefix. WORD: access list name deny: denies access of packet if conditions are matched. permit: permits access of packet if conditions are matched. X:X::X:X/M : prefix to match exact-match: exact match against the prefixes
ipv6 access-list *WORD* {**deny | permit**} **any**		Specifies the named ACL with any destination IP address. WORD: access list name any: any destination IP address
ipv6 access-list *WORD* **remark** *LINE*		Writes comments for the named ACL. LINE: access list entry comments up to 100 characters

i Add entries to the list by repeating the command for different IPv6 addresses.

Use the no access-list command to delete an entry in the named ACL.

Command	Mode	Description
no ipv6 access-list *WORD* {**deny | permit**} *X:X::X:X/M* [**exact-match**]	Global	Deletes an entry of the named ACL.
no ipv6 access-list *WORD* {**deny | permit**} **any**		
no ipv6 access-list *WORD* **remark** [*LINE*]		

To display the existing Access List entries, use the following command.

Command	Mode	Description
show ipv6 access-list	Enable Global Bridge	Shows the existing ACL entries. WORD: IPv6 access list name
show ipv6 access-list *WORD*		

7.21.6 Displaying Access List Entries

To display the existing ACL entries, use the following command.

Command	Mode	Description
show access-list	Enable Global Bridge	Shows the existing ACL entries.
show ip access-list		
show access-list-range		Shows the existing IP access range lists. 1-99: IP standard access list 1300-1999: IP standard access list (extended range) 100-199: IP extended access list 2000-2699: IP extended access list (extended range) WORD: access list name
show ip access-list-range [<1-99> | <100-199> | <1300-1999> | <2000-2699> | WORD]		
show ip access-list {<1-99> | <100-199> | <1300-1999> | <2000-2699> | WORD}		Shows the existing ACL entries for a given ACL type. 1-99: IP standard access list 1300-1999: IP standard access list (extended range) 100-199: IP extended access list 2000-2699: IP extended access list (extended range) WORD: access list name

Sample Configuration

This is an example of displaying the configured ACL entries.

```
SWITCH(config)# show ip access-list
Standard IP access list 5
   permit 10.55.10.0, wildcard bits 0.0.0.255
   deny 10.55.1.0, wildcard bits 0.0.0.255
Extended IP access list 100
   permit ip 10.55.10.0 0.0.0.255 10.55.193.0 0.0.0.255
   deny ip 10.12.154.0 0.0.0.255 10.12.202.0 0.0.0.255
ZebOS IP access list sample_ACL
   permit 10.55.193.109/24
SWITCH(config)#
```

8 System Main Functions

8.1 Virtual Local Area Network (VLAN)

The first step in setting up your bridging network is to define VLAN on your switch. VLAN is a bridged network that is logically segmented by customer or function. Each VLAN contains a group of ports called VLAN members. On the VLAN network, packets received on a port are forwarded only to the ports that belong to the same VLAN as the receiving port. Network devices in different VLANs cannot communicate with one another without a Layer 3 switching device to route traffic between the VLANs. VLAN reduces the amount of broadcast traffic so that flow control could be realized. It also has security benefits by completely separating traffics between different VLANs.

Enlarged Network Bandwidth

Users belonged in each different VLAN can use more enlarged bandwidth than no VLAN composition because they do not receive unnecessary Broadcast information. A properly implemented VLAN will restrict multicast and unknown unicast traffic to only those links necessary to only those links necessary to reach members of the VLAN associated with that multicast (or unknown unicast) traffic.

Cost-Effective Way

When you use VLAN to prevent unnecessary traffic loading because of broadcast, you can get cost-effective network composition since switch is not needed.

Enhanced Security

When using a shared-bandwidth LAN, there is no inherent protection provided against unwanted eavesdropping. In addition to eavesdropping, a malicious user on a shared LAN can also induce problems by sending lots of traffic to specific targeted users or network as a whole. The only cure is to physically isolate the offending user. By creating logical partitions with VLAN technology, we further enhance the protections against both unwanted eavesdropping and spurious transmissions. As depicted in Figure, a properly implemented port-based VLAN allows free communication among the members of a given VLAN, but does not forward traffic among switch ports associated with members of different VLANs. That is, a VLAN configuration restricts traffic flow to a proper subnet comprising exactly those links connecting members of the VLAN. Users can eavesdrop only on the multicast and unknown unicast traffic within their own VLAN: presumably the configured VLAN comprises a set of logically related users.

User Mobility

By defining a VLAN based on the addresses of the member stations, we can define a workgroup independent of the physical location of its members. Unicast and multicast traffic (including server advertisements) will propagate to all members of the VLAN so that they can communicate freely among themselves.

8.1.1 Port-based VLAN

The simplest implicit mapping rule is known as port-based VLAN. A frame is assigned to a VLAN based solely on the switch port on which the frame arrives. In the example depicted in Fig. 8.1, frames arriving on ports 1 through 4 are assigned to VLAN 1, frame from ports 5 through 8 are assigned to VLAN 2, and frames from ports 9 through 12 are assigned to VLAN 3.

Stations within a given VLAN can freely communicate among themselves using either unicast or multicast addressing. No communication is possible at the Data Link layer between stations connected to ports that are members of different VLANs. Communication among devices in separate VLANs can be accomplished at higher layers of the architecture, for example, by using a Network layer router with connections to two or more VLANs.

Multicast traffic, or traffic destined for an unknown unicast address arriving on any port, will be flooded only to those ports that are part of the same VLAN. This provides the desired traffic isolation and bandwidth preservation. The use of port-based VLANs effectively partitions a single switch into multiple sub-switches, one for each VLAN.

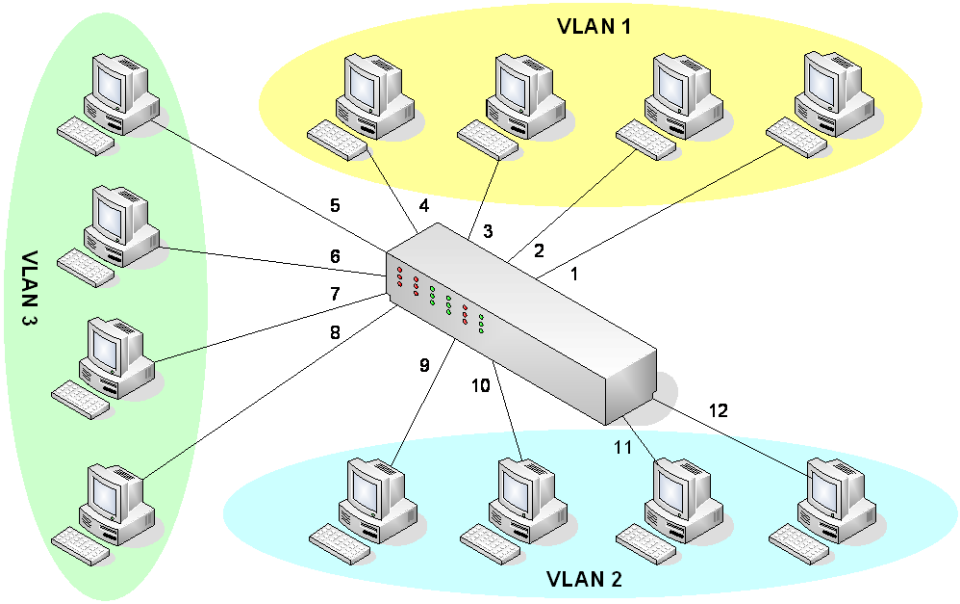


Fig. 8.1 Port-based VLAN

The IEEE 802.1Q based ports on the switches support simultaneous tagged and untagged traffic. An 802.1Q port is assigned a default port VLAN ID (PVID), and all untagged traffic is assumed to belong to the port default PVID. Thus, the ports participating in the VLANs accept packets bearing VLAN tags and transmit them to the port VLAN ID.

The below functions are explained.

- Creating VLAN
- Specifying PVID
- Adding Port to VLAN
- Deleting VLAN

8.1.1.1 Creating VLAN

To configure VLAN on user's network, use the following command.

Command	Mode	Description
vlan create *VLANS*	Bridge	Creates new VLAN by assigning VLAN ID: VLANS: VLAN ID (1-4094, multiple entries possible)

i The variable VLANS is a particular set of bridged interfaces. Frames are bridged only among interfaces in the same VLAN.

8.1.1.2 Specifying PVID

By default, PVID 1 is specified to all ports. You can also configure a PVID. To configure a PVID in a port, use the following command.

Command	Mode	Description
vlan pvid *PORTS PVIDS*	Bridge	Configures a PVID: PORTS: port number PVIDS: PVID (1-4094, multiple entries possible)

8.1.1.3 Adding Port to VLAN

To assign a port to VLAN, use the following command.

Command	Mode	Description
vlan add *VLANS PORTS* {**tagged** | **untagged**}	Bridge	Assigns a port to VLAN: VLANS: VLAN ID (1-4094)
vlan del *VLANS PORTS*		Deletes associated ports from specified VLAN: VLANS: VLAN ID (1-4094)

i When you assign several ports to VLAN, you have to enter each port separated by a comma without space or use dash mark "-" to arrange port range.

i If you try to have more than '1000' processes executed by a command, you meet a limit block with "Too many to process" error message by system policy as follows:

```
SWITCH(bridge)# vlan add 3-4090 1-24 tagged
% Too many to process(user-input/maximum:98112/1000)
SWITCH(bridge)#
```

By using a command above, it creates 4088 VLANs, and registers each created VLAN to individual ports from 1 to 24 with tagged option repeatedly. It indicates that you try to run 98112 (4088 x 24) actions in the system. The system processes individually the values within a specified range.

If you keep the number of processes under 1000, you can create multiple VLANs and specify which ports are tagged(or untagged) by a command.

```
SWITCH(bridge)# vlan add 161-200 1-24 tagged
```

```
SWITCH(bridge)#
```

8.1.1.4 Deleting VLAN

To delete VLAN, use the following command.

Command	Mode	Description
no vlan *VLANS*	Bridge	Deletes VLAN, enter the VLAN ID to be deleted.

i When you delete a VLAN, all ports must be removed from the VLAN; the VLAN must be empty.

8.1.2 Protocol-based VLAN

User can use a VLAN mapping that associates a set of processes within stations to a VLAN rather than the stations themselves. Consider a network comprising devices supporting multiple protocol suites. Each device may have an IP protocol stack, an AppleTalk protocol stack, an IPX protocol stack and so on.

If we configure VLAN-aware switches such that they can associate a frame with a VLAN based on a combination of the station's MAC source address and the protocol stack in use, we can create separate VLANs for each set of protocol-specific applications.

To configure a protocol-based VLAN, follow these steps.

1. Configure VLAN groups for the protocols you want to use.
2. Create a protocol group for each of the protocols you want to assign to a VLAN.
3. Then map the protocol for each interface to the appropriate VLAN.

Command	Mode	Description
vlan pvid *PORTS* **ethertype** *ETHERTYPE VLANS*	Bridge	Adds a port with a protocol-based VLAN. PORTS: port number ETHERTYPE: Ethernet type (e.g. 0x800) VLANS: VLAN ID (1-4094)
no vlan pvid *PORTS* **ethertype** [*ETHERTYPE*]		Removes a port from a protocol-based VLAN.

Because Protocol Based VLAN and normal VLAN run at the same time, Protocol Based VLAN operates only matched situation comparing below two cases.

1. When Untagged Frame comes in and matches with Protocol VLAN Table, tags PVID which configured on Protocol VLAN. But in no matched situation, tags PVID which configured on and operates VLAN.
2. When Tagged Frame comes in and VID is 0, it switches by Protocol VLAN Table. But if VID is not 0, it switches by normal VLAN Table.

8.1.3 MAC-based VLAN

The OLT can assign a frame to a VLAN based on the source MAC address in the received frames. Using this, all frames emitted by a given end station will be assigned to the same VLAN, regardless of the port on which the frame arrives. This is useful for mobility application.

To configure a MAC-based VLAN, follow these steps.

1. Create VLAN groups for the MAC addresses you want to use.
2. Map the MAC address to the appropriate VLAN.

Command	Mode	Description
vlan macbase *MAC-ADDR VLANS*	Bridge	Adds a specified MAC address to a MAC-based VLAN. MAC-ADDR: MAC address of end station VLANS: VLAN ID (1-4094)
no vlan macbase *MAC-ADDR*		Removes a specified MAC address from a specified MAC address

8.1.4 Subnet-based VLAN

An IP address contains two parts: a subnet identifier and a station identifier. The OLT performs two operations to create IP subnet-based VLANs.

- Parse the protocol type to determine if the frame encapsulates an IP datagram.
- Examine and extract the IP subnet portion of the IP Source Address in the encapsulated datagram.

Once it is known that a given frame carries an IP datagram belonging to a given subnet, the switch can transmit the frame as needed within the confines of the subnet to which it belongs. If a device with a given IP address moves within the VLAN-aware network, the boundaries of its IP subnet can automatically adjust to accommodate the station's address.

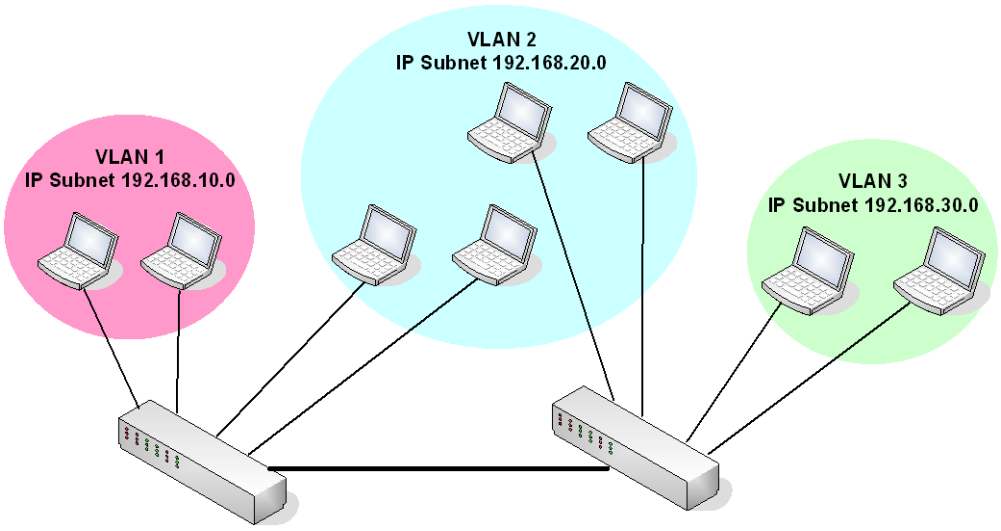


Fig. 8.2 Subnet-based VLAN

To configure subnet-based VLAN, use the following command.

Command	Mode	Description
vlan subnet *A.B.C.D/M VLANS*	Bridge	Configures subnet based VLAN. VLANS: VLAN ID (1-4094)
ipv6 vlan subnet *X:X::X:X/M VLANS*		

To clear subnet-based VLAN configuration, use the following command.

Command	Mode	Description
no vlan subnet [*A.B.C.D/M*]	Bridge	Clears configured VLAN based on subnet.
no ipv6 vlan subnet [*X:X::X:X/M*]		

To display the subnet-based VLAN configuration, use the following command.

Command	Mode	Description
show vlan subnet	Enable Global Bridge	Clears configured VLAN based on subnet.
show ipv6 vlan subnet		

8.1.5 Tagged VLAN

In a VLAN environment, a frame's association with a given VLAN is soft; the fact that a given frame exists on some physical cable does not imply its membership in any particular VLAN. VLAN association is determined by a set of rules applied to the frames by VLAN-aware stations and/or switches.

There are two methods for identifying the VLAN membership of a given frame:

- Parse the frame and apply the membership rules (implicit tagging).
- Provide an explicit VLAN identifier within the frame itself.

VLAN Tag

A VLAN tag is a predefined field in a frame that carries the VLAN identifier for that frame. VLAN tags are always applied by a VLAN-aware device. VLAN-tagging provides a number of benefits, but also carries some disadvantages.

Advantages	Disadvantages
VLAN association rules only need to be applied once.	Tags can only be interpreted by VLAN aware devices.
Only edge switches need to know the VLAN association rules.	Edge switches must strip tags before forwarding frames to legacy devices or VLAN-unaware domains.
Core switches can get higher performance by operating on an explicit VLAN identifier.	Insertion or removal of a tag requires recalculation of the FCS, possibly compromising frame integrity.

VLAN-aware end stations can further reduce the performance load of edge switches.	Tag insertion may increase the length of a frame beyond the maximum allowed by legacy equipment.

Tab. 8.1 Advantages and Disadvantages of Tagged VLAN

Mapping Frames to VLAN

From the perspective the VLAN-aware devices, the distinguishing characteristic of a VLAN is the means used to map a given frame to that VLAN. In the case of tagged frame, the mapping is simple – the tag contains the VLAN identifier for the frame, and the frame is assumed to belong to the indicated VLAN. That's all there is to it.

To configure the tagged VLAN, use the following command.

Command	Mode	Description
vlan add *VLANS PORTS* **tagged**	Bridge	Configures tagged VLAN on a port: VLANS: VLAN ID (1-4094) PORTS: port number

8.1.6 VLAN Cross-connect

To create a VLAN, use the following command.

Command	Mode	Description
vlan create *VLAN_NAME* [**eline**]	Bridge	Creates a VLAN. eline: Enables E-line option VLAN_NAME:vlan name (ex. NAME | X | X-Y)

To forward packets via configuration of VLAN cross-connect, use the following command.

Command	Mode	Description
vlan cross-connect *FIR_PORT* SEC_*PORT* **out-vid** *VLANS* [**in-vid** *VLAN*]	Bridge	Configures a VLAN cross-connect. FIR_PORT: first port number. SEC_PORT: second port number VLAN: VLAN ID (1-4094).
no vlan cross-connect *FIR_PORT* SEC_*PORT* **out-vid** *VLANS* [**in-vid** *VLAN*]		Deletes a VLAN cross-conect configuration.

To display the configuration of VLAN cross-connect, use the following command.

Command	Mode	Description
show vlan cross-connect	Enable Global Bridge	Displays configured VLAN corss-connect.

8.1.7 VLAN Description

To specify a VLAN description, use the following command.

Command	Mode	Description
vlan description *VLANS DESC*	Bridge	Specifies a VLAN description. VLANS: VLAN ID (1-4094) DESC: description
no vlan description *VLANS*		Deletes a specified description.

To display a specified VLAN description, use the following command.

Command	Mode	Description
show vlan description	Enable Global Bridge	Shows a specified VLAN description.

8.1.8 VLAN Precedence

To make precedence between MAC address and Subnet based VLAN, you can choose one of both with below command.

Command	Mode	Description
vlan precedence {**mac** | **subnet**}	Bridge	Configure precedence between MAC based VLAN and Subnet based VLAN.

8.1.9 Displaying VLAN Information

User can display the VLAN information about Port based VLAN, Protocol based VLAN, MAC based VLAN, Subnet based VLAN and QinQ.

Command	Mode	Description
show vlan [*VLANS*]	Enable Global Bridge	Shows all VLAN configurations.
show vlan description		Shows a description for specific VLAN.
show vlan dot1q-tunnel		Shows QinQ configuration.
show vlan protocol		Shows VLAN based on protocol.
show vlan macbase		Shows VLAN based on MAC address.
show vlan subnet		Shows VLAN based on subnet.
show vlan port *PORTS*		Shows VLAN based on the port.
show port protected		Shows port isolation configuration.

8.1.10 QinQ VLAN Mapping

QinQ or Double Tagging is one way for tunneling between several networks.

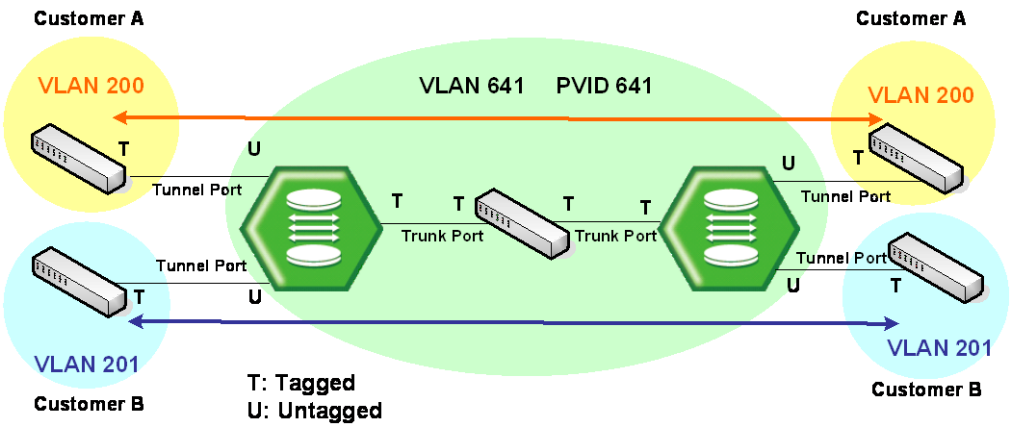


Fig. 8.3 Example of QinQ Configuration

If QinQ is configured on the OLT, it transmits packets adding another Tag to original Tag. Customer A group and customer B group can guarantee security because telecommunication is done between each VLANs at Double Tagging part.

Double tagging is implemented with another VLAN tag in Ethernet frame header.

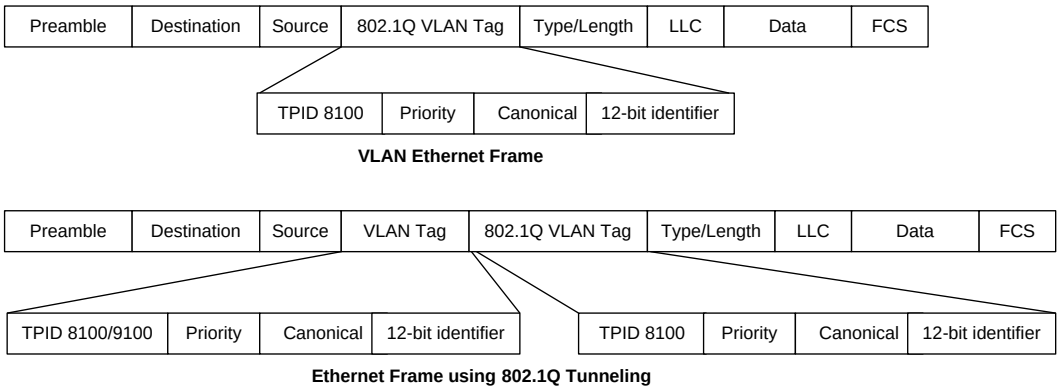


Fig. 8.4 QinQ Frame

Port which connected with Service Provider is Uplink port (internal), and which connected with customer is Access port (external).

Tunnel Port

By tunnel port we mean a LAN port that is configured to offer 802.1Q-tunneling support. A tunnel port is always connected to the end customer, and the input traffic to a tunnel port is always 802.1Q tagged traffic.

The different customer VLANs existing in the traffic to a tunnel port shall be preserved when the traffic is carried across the network

Trunk Port

By trunk port we mean a LAN port that is configured to operate as an inter-switch link/port, able of carrying double-tagged traffic. A trunk port is always connected to another trunk

port on a different switch. Switching shall be performed between trunk ports and tunnels ports and between different trunk ports.

Network-Network Interface (NNI) Port
NNI port has multiple SVLANs associated. Only frames tagged with those SVLAN are forwarded on that port.

User Network Interface (UNI) Port
UNI port has an associated QinQ table that maps CVLANs with SVLANs.Configuring UNI/NNI Port

To configure the UNI/NNI port, use the following command.

Command	Mode	Description
vlan dot1q-tunnel enable *PORTS*	Bridge	Enables QinQ port and configures an UNI port. PORTS: qinq port to be enabled
vlan dot1q-tunnel disable *PORTS*		Disables QinQ port.(default) PORTS: qinq port to be disabled

8.1.10.1 TPID Configuration

TPID (Tag Protocol Identifier) is a kind of Tag protocol, and it indicates the currently used tag information. User can change the TPID. By default the port which is configured as 802.1q (0x8100) cannot work as VLAN member.

To set TPID on a QinQ port, use the following command.

Command	Mode	Description
vlan dot1q-tunnel { **outer** | **inner**} **tpid** *TPID*	Bridge	Configures TPID. outer: outer Ethertype inner: inner Ethertype

8.1.10.2 One-to-One VLAN Mapping between S-VID and C-VID

To configure one-to-one VLAN mapping and translation, use the following command.

Command	Mode	Description
vlan dot1q-tunnel ingress mapping *PORTS* **c-vid** <1-4094> **trans-s-vid** <1-4094>	Bridge	Configures 1:1 VLAN mapping for UNI port and translates C-VLAN tag of incoming Single Inner Tagged (SIT) packets to S-VLAN tag. PORTS: UNI port number
vlan dot1q-tunnel ingress mapping *PORTS* **c-vid** <1-4094> **trans-s-vid** <1-4094> **same-c-vid**		Configures VLAN mapping for UNI port and adds S-VLAN tag of incoming Single Inner Tagged (SIT) packets with the given C-VLAN tag.
vlan dot1q-tunnel egress mapping *PORTS* **s-vid** <1-4094> **trans-c-vid** <1-4094>		Configures 1:1 VLAN mapping for UNI port and translates S-VLAN tag of outgoing Single Outer Tagged (SOT) packets to C-VLAN tag.
vlan dot1q-tunnel ingress range-mapping *PORTS* **c-vid** <1-4094>		Configures 1:1 VLAN mapping for UNI port and translates multiple C-VLAN tags of incoming Single

trans-s-vid <1-4094>		Inner Tagged (SIT) packets to S-VLAN tag. PORTS: UNI port number
vlan dot1q-tunnel ingress range-mapping *PORTS* **c-vid** <1-4094> **trans-s-vid** <1-4094> **same-c-vid**		Configures 1:1 VLAN mapping for UNI port and adds S-VLAN tag of incoming packets in the given C-VLAN range.
vlan dot1q-tunnel ingress mapping *PORTS* **s-vid** <1-4094> **trans-s-vid** <1-4094>		Configures 1:1 VLAN mapping for NNI port and translates multiple S-VLAN tags of incoming Single Outer Tagged (SOT) packets to S-VLAN tag. PORTS: NNI port number
vlan dot1q-tunnel egress mapping *PORTS* **s-vid** <1-4094> **trans-s-vid** <1-4094>		Configures 1:1 VLAN mapping for NNI port and translates multiple S-VLAN tags of outgoing Single Outer Tagged (SOT) packets to S-VLAN tag. PORTS: NNI port number
vlan dot1q-tunnel ingress range-mapping *PORTS* **s-vid** <1-4094> **trans-s-vid** <1-4094>		Configures 1:1 VLAN mapping for NNI port and translates multiple S-VLAN tags of incoming Single Inner Tagged (SIT) packets to S-VLAN tag.

To delete the configured one-to-one VLAN mapping and translation, use the following command.

Command	Mode	Description
no vlan dot1q-tunnel ingress mapping *PORTS* **c-vid** <1-4094> **trans-s-vid**	Bridge	Deletes the configured 1:1 VLAN mapping and translation.
no vlan dot1q-tunnel egress mapping *PORTS* **s-vid** <1-4094> **trans-c-vid**		
no vlan dot1q-tunnel ingress range-mapping *PORTS* **c-vid** <1-4094> **trans-s-vid**		
no vlan dot1q-tunnel {**ingress** | **egress**} **mapping** *PORTS* **s-vid** <1-4094> **trans-s-vid**		
no vlan dot1q-tunnel ingress range-mapping *PORTS* **s-vid** <1-4094> **trans-s-vid**		

8.1.10.3 One-to-Two VLAN Mapping between S-VID and C-VID

To configure one-to-two VLAN mapping and translation, use the following command.

Command	Mode	Description
vlan dot1q-tunnel ingress mapping *PORTS* **s-vid** <1-4094> **trans-s-vid** <1-4094> **trans-c-vid** <1-4094>	Bridge	Configures 1:2 VLAN mapping for NNI port and translates incoming Single Outer Tagged (SOT) packet with given S-VLAN tag to Double Tagged (DT) packet by adding S-VLAN and C-VLAN tags. PORTS: NNI port number
vlan dot1q-tunnel egress mapping *PORTS* **s-vid** <1-4094>		Configures 1:2 VLAN mapping for NNI port and translates outgoing Single Outer Tagged (SOT) packet

trans-s-vid <1-4094> **trans-c-vid** <1-4094>		with given S-VLAN tag to Double Tagged (DT) packet by adding S-VLAN and C-VLAN tags. PORTS: NNI port number
vlan dot1q-tunnel ingress range-mapping *PORTS* **s-vid** <1-4094> **trans-s-vid** <1-4094> **trans-c-vid** <1-4094>		Configures 1:2 VLAN mapping for NNI port and translates incoming Single Outer Tagged (SOT) packet in the given S-VLAN range to Double Tagged (DT) packet by adding S-VLAN and C-VLAN tags.

To delete the configured one-to-two VLAN mapping and translation, use the following command.

Command	Mode	Description
no vlan dot1q-tunnel ingress mapping *PORTS* **s-vid** <1-4094> **trans-s-vid trans-c-vid**	Bridge	Deletes the configured 1:2 VLAN mapping and translation.
no vlan dot1q-tunnel egress mapping *PORTS* **s-vid** <1-4094> **trans-s-vid trans-c-vid**		
no vlan dot1q-tunnel ingress range-mapping *PORTS* **s-vid** <1-4094> **trans-s-vid trans-c-vid**		

8.1.10.4 Two-to-One VLAN Mapping between S-VID and C-VID

To configure two-to-one VLAN mapping and translation, use the following command.

Command	Mode	Description
vlan dot1q-tunnel ingress mapping *PORTS* **s-vid** <1-4094> **c-vid** <1-4094> **trans-s-vid** <1-4094>	Bridge	Configures 2:1 VLAN mapping for NNI port and translates S-VLAN and C-VLAN tags of incoming Double Tagged (DT) packets to one S-VLAN tag.
vlan dot1q-tunnel egress mapping *PORTS* **s-vid** <1-4094> **c-vid** <1-4094> **trans-s-vid** <1-4094>		Configures 2:1 VLAN mapping for NNI port and translates S-VLAN and C-VLAN tags of outgoing Double Tagged (DT) packets to S-VLAN tag.
vlan dot1q-tunnel egress mapping *PORTS* **s-vid** <1-4094> **c-vid** <1-4094> **same-c-vid**		Configures 2:1 VLAN mapping for UNI port and removes S-VLAN tag from outgoing Double Tagged (DT) packet with the given S-VLAN and C-VLAN tags.

To delete the configured two-to-one VLAN mapping and translation, use the following command.

Command	Mode	Description
no vlan dot1q-tunnel ingress mapping *PORTS* **s-vid** <1-4094> **c-vid** <1-4094>	Bridge	Deletes the configured 2:1 VLAN mapping and translation.
no vlan dot1q-tunnel egress		

mapping *PORTS* **s-vid** <1-4094> **c-vid** <1-4094>		

8.1.10.5 Two-to-Two VLAN Mapping between S-VID and C-VID

To configure two-to-two VLAN mapping and translation, use the following command.

Command	Mode	Description
vlan dot1q-tunnel ingress mapping *PORTS* **internal s-vid** <1-4094> **c-vid** <1-4094> **external s-vid** <1-4094> **c-vid** <1-4094>	Bridge	Configures 2:2 VLAN mapping for NNI port and translates internal S-VLAN and C-VLAN tags of incoming 802.1q tunneling packets to external S-VLAN and C-VLAN tags.
vlan dot1q-tunnel egress mapping *PORTS* **external s-vid** <1-4094> **c-vid** <1-4094> **internal s-vid** <1-4094> **c-vid** <1-4094>		Configures 2:2 VLAN mapping for NNI port and translates external S-VLAN and C-VLAN tags of outgoing 802.1q tunneling packets to internal S-VLAN and C-VLAN tags.

To delete the configured two-to-two VLAN mapping and translation, use the following command.

Command	Mode	Description
no vlan dot1q-tunnel ingress mapping *PORTS* **internal s-vid** <1-4094> **c-vid** <1-4094>	Bridge	Deletes the configured 2:2 VLAN mapping and translation.
no vlan dot1q-tunnel egress mapping *PORTS* **external s-vid** <1-4094> **c-vid** <1-4094>		

8.1.10.6 Double Tagging Operation

Step 1
If there is no SPVLAN Tag on received packet, SPVLAN Tag is added.
SPVLAN Tag = TPID : Configured TPID
VID : PVID of input port

Step 2
If a received packet is tagged with CVLAN, the switch transmits it to uplink port changing to SPVLAN + CVLAN. When TPID value of received packet is same with TPID of port, it recognizes as SPVLAN, and if not as CVLAN.

Step 3
If Egress port is Access port (Access port is configured as Untagged), remove SPVLAN. If egress port is uplink port, transmit as it is.

Step 4
The OLT switch has 0x8100 TPID value as default and other values are used as hexadecimal number.

8.1.10.7 Double Tagging Configuration

Step 1
Designate the QinQ port.

Command	Mode	Description
vlan dot1q-tunnel enable *PORTS*	Bridge	Configures a qinq port. PORTS: qinq port to be enabled

Step 2
Configure the same PVID with the VLAN of peer network on the designated qinq port.

Command	Mode	Description
vlan pvid *PORTS* <1-4094>	Bridge	Configure a pvid. PORTS: qinq port to be enabled 1-4094: PVID

To disable double tagging, use the following command

Command	Mode	Description
vlan dot1q-tunnel disable *PORTS*	Bridge	Disables the qinq port. PORTS: qinq port to be disabled

i

When you configure Double tagging on the OLT, consider the below attention list.

- DT and HTLS cannot be configured at the same time. (If switch should operate as DT, HTSL has to be disabled.)
- TPID value of all ports on switch is same.
- Access Port should be configured as Untagged, and Uplink port as Tagged.
- Ignore all tag information of port which comes from untagged port (Access Port).
- Port with DT function should be able to configure Jumbo function also

8.1.10.8 Inner Tag Configuration

To put the configured C-VLAN tag in the inner tag field of incoming untagged packet on a port, use the following command.

Command	Mode	Description
vlan dot1q-tunnel ingress push c-vid *PORTS* <1-4094>	Bridge	Puts the configured C-VLAN tag in the inner tag field of incoming packet on an ingress port
no vlan dot1q-tunnel ingress push c-vid *PORTS*		Disables the C-VLAN inner tagging on an ingress port.

To remove the C-VLAN inner tag from the outgoing packet on a port, use the following command.

Command	Mode	Description
vlan dot1q-tunnel egress pop c-vid *PORTS*	Bridge	Removes C-VLAN inner tag from the outgoing packet on an egress port
no vlan dot1q-tunnel egress pop c-vid *PORTS*		Disables the C-VLAN inner tag removal on an egress port.

8.1.10.9 Displaying VLAN Mapping and Translation

To display the configured VLAN mapping and translation, use the following command.

Command	Mode	Description
show vlan dot1q-tunnel {**ingress** | **egress**} **mapping** [*PORTS*]	Enable Global Bridge	Shows the configured VLAN mapping.
show vlan dot1q-tunnel		Shows the status of UNI/NNI ports.

8.1.11 Layer 2 Isolation

Private VLAN is a kind of LAN Security function using by Cisco products, and it can be classified to Private VLAN and Private edge. Currently, there is no standard of it.

Private VLAN Edge

Private VLAN edge (protected port) is a function in local switch. That is, it cannot work on between two different switches with protected ports. A protected port cannot transmit any traffic to other protected ports.

Private VLAN

Private VLAN provides L2 isolation within the same Broadcast Domain ports. That means another VLAN is created within a VLAN. There are three type of VLAN mode.

- **Promiscuous**: A promiscuous port can communicate with all interfaces, including the isolated and community ports within a PVLAN.
- **Isolated**: An isolated port has complete Layer 2 separation from the other ports within the same PVLAN, but not from the promiscuous ports. PVLANs block all traffic to isolated ports except traffic from promiscuous ports. Traffic from isolated port is forwarded only to promiscuous ports.
- **Community**: Community ports communicate among themselves and with their promiscuous ports. These interfaces are separated at Layer 2 from all other interfaces in other communities or isolated ports within their PVLAN.

The difference between Private VLAN and Private VLAN edge is that PVLAN edge guarantees security for the ports in a VLAN using protected port and PVLAN guarantees port security by creating sub-VLAN with the three types (Promiscuous, Isolation, and Community). And because PVLAN edge can work on local switch, the isolation between two switches is impossible.

The OLT provides Private VLAN function like Private VLAN edge of Cisco product. Because it does not create any sub-VLAN, port security is provided by port isolation. If

you want to configure Private VLAN on the OLT switch, refer to Port Isolation configuration.

8.1.11.1 Port Isolation

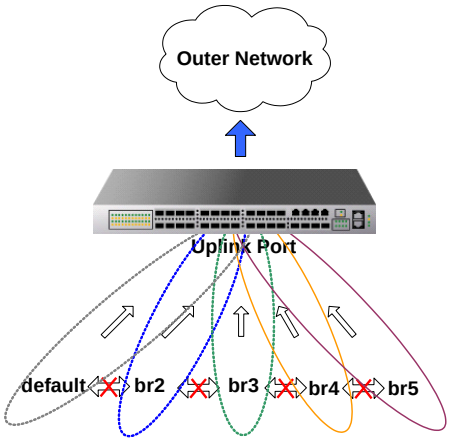
The Port Isolation feature is a method that restricts L2 switching between isolated ports in a VLAN. However, flows between isolated port and non-isolated port are not restricted. If you use the **port protected** command, packet cannot be transmitted between protected ports. However, to non-protected ports, communication is possible.

To configure Port Isolation, use the following command.

Command	Mode	Description
port protected *PORTS*	Bridge	Enables port isolation.
no port protected [*PORTS*]		Disables port isolation.

8.1.11.2 Shared VLAN

This chapter is only for Layer 2 switch operation. Because there is no routing information in Layer 2 switch, each VLAN cannot communicate. Especially, the uplink port should receive packets from all VLANs. Therefore, when you configure the OLT as Layer 2 switch, the uplink ports must be included in all VLANs.




```
SWITCH(bridge)# show vlan
                                u: untagged port, t: tagged port
-----------------------------------------------------------------
                        |         1         2         3         4
     Name( VID| FID) |123456789012345678901234567890123456789012
-----------------------------------------------------------------
 default(   1|   1)  |u...uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu
     br2(   2|   2)  |.u....................u.................
     br3(   3|   3)  |..u...................u.................
     br4(   4|   4)  |...u..................u.................
     br5(   5|   5)  |....u.................u.................
SWITCH(bridge)#
```

Fig. 8.5 Outgoing Packets under Layer 2 Shared VLAN Environment

As above configuration with untagged packet, if an untagged packet comes into port 1, it is added with **tag 1** for PVID 1. In addition, the uplink port 24 is also included in the default VLAN; it can transmit to port 24.

However, a problem can occur for coming down untagged packets to uplink ports. If an untagged packet comes to uplink ports from outer network, the system does not know which PVID it has and where should it forward.

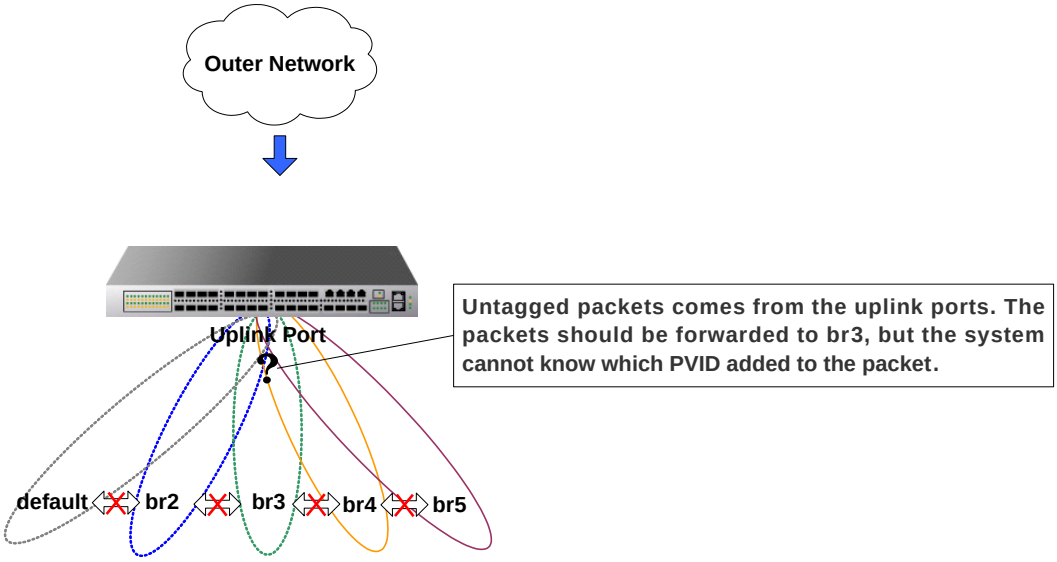
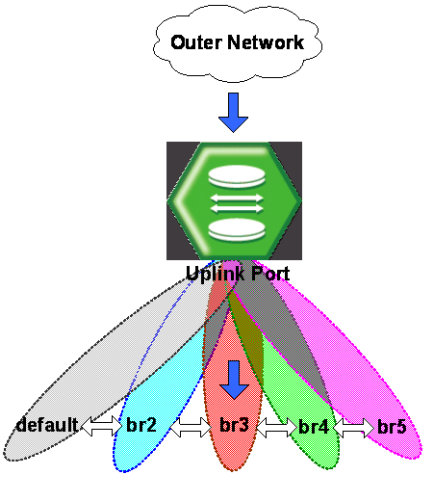


Fig. 8.6 Incoming Packets under Layer 2 Shared VLAN Environment (1)

To transmit the untagged packet from uplink port to subscriber, a new VLAN should create including all subscriber ports and uplink ports. This makes the uplink ports to recognize all other ports.

FID helps this packet forwarding. FDB is MAC Address Table that recorded in CPU. FDB table is made of FID (FDB Identification). Because the same FID is managed in the same MAC table, it can recognize how to process packet forwarding. If the FID is not same, the system cannot know the information from MAC table and floods the packets.




```
SWITCH(bridge)# show vlan
                          u: untagged port, t: tagged port
-----------------------------------------------------------------
                 |          1         2         3         4
    Name( VID|  FID) |123456789012345678901234567890123456789012
-----------------|-----------------------------------------------
 default(   1|    6) |u...uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu
     br2(   2|    6) |.u......................u..................
     br3(   3|    6) |..u....................u..................
     br4(   4|    6) |...u...................u..................
     br5(   5|    6) |....u..................u..................
     br6(   6|    6) |uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu
SWITCH(bridge)#
```

Fig. 8.7 Incoming Packets under Layer 2 Shared VLAN Environment (2)

In conclusion, to use the OLT as Layer 2 switch, user should add the uplink port to all VLANs and create new VLAN including all ports. If the communication between each VLAN is needed, FID should be same.

To configure FID, use the following command.

Command	Mode	Description
vlan fid *VLANS FID*	Bridge	Configures FID.

8.1.12 Sample Configuration

Sample Configuration 1: Configuring Port-based VLAN

The following is assigning br50, br3, and br4 to port 2, port 3, and port 4.

```
SWITCH(bridge)# vlan create br50
SWITCH(bridge)# vlan create br51
SWITCH(bridge)# vlan create br200
SWITCH(bridge)# vlan create br250
SWITCH(bridge)# vlan create br500
SWITCH(bridge)# vlan add br50 5/1,6/1 untagged
SWITCH(bridge)# vlan add br51 5/2,6/2 untagged
SWITCH(bridge)# vlan add br200 t/1-t/16 tagged
SWITCH(bridge)# vlan add br250 t/1-t/16 tagged
SWITCH(bridge)# vlan add br500 t/1-t/16 tagged
SWITCH(bridge)# vlan pvid 5/1,6/1 50
SWITCH(bridge)# vlan pvid 5/2,6/2 51
SWITCH(bridge)# vlan pvid t/1-t/16 1
SWITCH(bridge)# show vlan
```

Sample Configuration 2: Deleting Port-based VLAN

The following is deleting br3 among configured VLAN.

```
SWITCH(bridge)# vlan del br3 3
SWITCH(bridge)# exit
SWITCH(config)# interface br3
SWITCH(interface)# shutdown
SWITCH(interface)# exit
SWITCH(config)# bridge
SWITCH(bridge)# no vlan br3
SWITCH(bridge)# show vlan
                      u: untagged port, t: tagged port
      ----------------------------------------------------------------
                        |         1         2         3         4
         Name( VID| FID) |123456789012345678901234567890123456789012
      ----------------------------------------------------------------
       default(   1|   1) |u...uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu
           br2(   2|   2) |.u.........................................
           br4(   4|   4) |...u.......................................
SWITCH(bridge)#
```

Sample Configuration 3: Configuring QinQ

Port 10 of SWITCH 1 and port 11 of SWITCH 2 are connected to the network where different VLANs are configured. To communicate without changing VLAN configuration of SWITCH 1 and SWITCH 2 which communicate with PVID 10, configure it as follows.

i You should configure the ports connected to network communicating with PVID 11 as

Tagged VLAN port.

< SWITCH 1 >

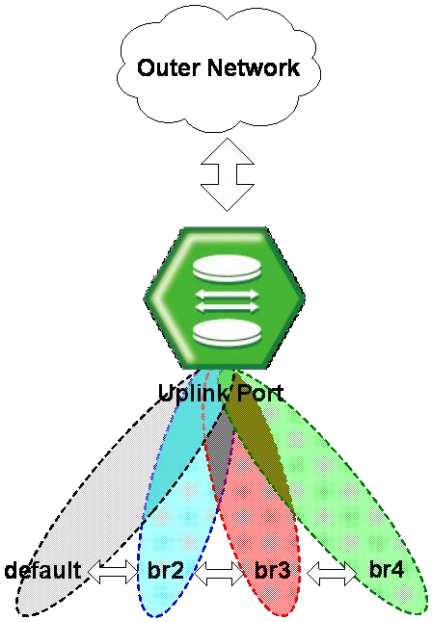
```
SWITCH(bridge)# vlan dot1q-tunnel enable 10
SWITCH(bridge)# vlan pvid 10 11
SWITCH(bridge)# show vlan dot1q-tunnel
          Tag Protocol Id : 0x8100 (d: double-tagging port)
        ----------------------------------------------------
              |        1        2        3        4
          Port |123456789012345678901234567890123456789012
        ----------------------------------------------------
          dtag  .........d................................
SWITCH(bridge)#
```

< SWITCH 2 >

```
SWITCH(bridge)# vlan dot1q-tunnel enable 11
SWITCH(bridge)# vlan pvid 11 11
SWITCH(bridge)# show vlan dot1q-tunnel
          Tag Protocol Id : 0x8100 (d: double-tagging port)
        ----------------------------------------------------
              |        1        2        3        4
          Port |123456789012345678901234567890123456789012
        ----------------------------------------------------
          dtag  ..........d...............................
SWITCH(bridge)#
```

Sample Configuration 5: Configuring Shared VLAN with FID

Configure br2, br3, br4 in the OLT configured Layer 2 environment and port 24 as Uplink port is configured. To transmit untagged packet through Uplink port rightly, follow below configuration.




```
SWITCH(bridge)# vlan create br2
SWITCH(bridge)# vlan create br3
SWITCH(bridge)# vlan create br4
SWITCH(bridge)# vlan del default 3-8
SWITCH(bridge)# vlan add br2 3,4 untagged
SWITCH(bridge)# vlan add br3 5,6 untagged
SWITCH(bridge)# vlan add br4 7,8 untagged
SWITCH(bridge)# vlan add br2 24 untagged
SWITCH(bridge)# vlan add br3 24 untagged
SWITCH(bridge)# vlan add br4 24 untagged
SWITCH(bridge)# vlan create br5
SWITCH(bridge)# vlan add br5 1-42 untagged
SWITCH(bridge)# vlan fid 1-5 5
SWITCH(bridge)# show vlan
                        u: untagged port, t: tagged port
      ------------------------------------------------------------------
                        |         1         2         3         4
         Name( VID| FID) |123456789012345678901234567890123456789012
      ------------------------------------------------------------------
       default(   1|   5) |uu......uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu
           br2(   2|   5) |..uu....................u..................
           br3(   3|   5) |....uu..................u..................
           br4(   4|   5) |......uu................u..................
           br5(   5|   5) |uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu
SWITCH(bridge)#
```

8.2 Link Aggregation (LAG)

Link aggregation complying with IEEE 802.3ad bundles several physical ports together to one logical port so that you can get enlarged bandwidth.

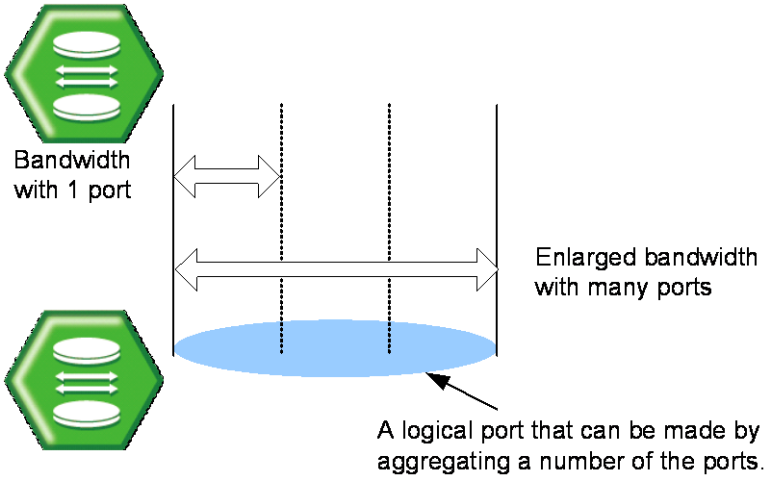


Fig. 8.8 Link Aggregation

The OLT supports two kinds of link aggregation as port trunk and LACP. There is a little difference in these two ways. In case of port trunking, it is quite troublesome to set the configuration manually and the rate to adjust to the network environment changes when connecting to the switch using logical port. On the other hand, in case of LACP, once you specify LACP member ports between the switches, the ports will be automatically aggregated by LACP without manually configuring the aggregated ports.

8.2.1 Port Trunk

Port trunking enables you to dynamically group the similarly configured interfaces into a single logical link (aggregate port) to increase bandwidth, while reducing the traffic congestion.

8.2.1.1 Configuring Port Trunk

To create a logical port by aggregating the ports, use the following command.

Command	Mode	Description
trunk *GID PORTS*	Bridge	Adds a port to the aggregation group. GID: trunk group ID <0-7>
trunk active-link *GID* <1-8>		Specifies the number of minimum active member ports within a Trunk group. A Trunk group is automatically disabled if the operational member ports fall at the same value or below the configured number. 1-8: the number of minimum active member ports (default:1)
trunk distmode *GID* {**dstip** | **dstmac** | **srcdstip** | **srcdstmac** |		Selects the distribution mode for a specified

srcip | **srcmac**}		aggregation group. (default: srcdstmac)

i

It is possible to input 0 to 7 to the trunk group ID because the OLT supports 8 logical aggregated ports, and the group ID of port trunk and the aggregator number of LACP cannot coexist.

If packets enter to logical port aggregating several ports and there is no way to decide packet route, the packets could be gathered on particular member port so that it is not possible to use logical port effectively. Therefore, the OLT is configured to decide the way of packet route in order to divide on member port effectively when packets enter. It is decided with source IP address, destination IP address, source MAC address, destination MAC address and the user could get information of packets to decided packet route.

The followings are the simple descriptions for the distribution modes:

- **dstip**: destination IP address
- **dstmac**: destination MAC address
- **srcdstip**: source and destination IP address
- **srcdstmac**: source and destination MAC address
- **srcip**: source IP address
- **srcmac**: source MAC address

The port designated as a member port of port trunk is automatically deleted from existing VLAN. Therefore, if the member port and aggregated port exist in different VLAN each other, VLAN configuration should be changed for their aggregation.

8.2.1.2 Disabling Port Trunk

To disable the configured port trunk, use the following command.

Command	Mode	Description
no trunk *GID PORTS*	Bridge	Releases a configured trunk port.
no trunk distmode *GID*		

i

If a port is deleted from a logical port or the port trunk is disabled, the port will be added to the default VLAN.

8.2.1.3 Displaying Port Trunk

To display a configuration of port trunk, use the following command.

Command	Mode	Description
show trunk	Enable Global Bridge	Shows a configuration for trunk.

8.2.2 Link Aggregation Control Protocol (LACP)

Link aggregation control protocol (LACP) is the function of using wider bandwidth by aggregating more than two ports as a logical port as previously stated port trunk function.

If the aggregated port by port trunk is in different VLAN from the VLAN where the existing member port originally belongs to, it should be moved to VLAN where the existing member port belongs to. However, the integrated port configured by LACP is automatically added to appropriate VLAN.

i LACP can generate up to 8 aggregators whose number value could be 0 to 7. The group ID of port trunk and the aggregator number of LACP cannot be configured with the same value.

The following explains how to configure LACP.

- Configuring LACP
- Distribution Mode
- Operation Mode
- Priority of Switch
- Manual Aggregation
- BPDU Transmission Rate
- Administrational Key
- Port Priority
-

Displaying LACP Configuration

8.2.2.1 Configuring LACP

Step 1 Activate LACP function, using the following command.

Command	Mode	Description
lacp aggregator *AGGREGATIONS*	Bridge	Enables LACP of designated Aggregator-number: AGGREGATIONS: select aggregator ID that should be enabled for LACP (valid value from 0 to 7).

Step 2 Configure the physical port that is a member of aggregated port. In order to configure the member port, use the following command.

Command	Mode	Description
lacp port *PORTS*	Bridge	Configures physical port that is member port of aggregator; select the port number(s) that should be enabled for LACP.

To disable LACP and delete the configuration of LACP, use the following command.

Command	Mode	Description
no lacp aggregator *AGGREGATIONS*	Bridge	Disables LACP for designated Aggregator-number, select the aggregator ID that should be disabled for LACP.

no lacp port *PORTS*		Deletes member port of Aggregator, select the port number(s) that should be disabled for LACP.

8.2.2.2 Distribution Mode

If packets enter to logical port aggregating several ports and there's no way to decide packet route, the packets could be gathered on particular member port so that it is not possible to use logical port effectively.

Therefore, the OLT is configured to decide the way of packet route in order to distribute (or forward) packets to the member port effectively when packets enter. It is decided with Source IP address, destination IP address, source MAC address, destination MAC address and the user could get information of packets to decided packet route. **dstip** is destination IP address and **dstmac** means destination MAC address.

i For the OLT, a source destination MAC address is basically used to decide packet route.

After configuring an LACP aggregator, you should configure the distribution mode. The following is the command for configuring the distribution mode of the LACP aggregator.

Command	Mode	Description
lacp aggregator distmode *AGGREGETIONS* {**srcmac** | **dstmac** | **srcdstmac** | **srcip** | **dstip** | **srcdstip**}	Bridge	Configures the distribution mode of the LACP aggregator: AGGREGATIONS: aggregator ID(0-7) srcmac: source MAC address dstmac: destination MAC address srcdstmac: source/destination MAC address (default) srcip: source IP address dstip: destination IP address srcdstip: source/destination IP address

To delete a configured distribution mode, use the following command.

Command	Mode	Description
no lacp aggregator distmode *AGGREGETIONS*	Bridge	Deletes a configured distribution mode.

8.2.2.3 Operation Mode

After configuring the member port, configure the LACP operation mode of the member port. This defines the operation way for starting LACP operation. You can select the operation mode between the active and passive mode.

The active mode allows the system to start LACP operation regardless of other connected devices. On the other hand, the passive mode allows the system to start LACP operation only when receiving LACP messages from other connected devices.

⚠ In case of an LACP connection between 2 switches, if the member ports of both switches are configured as the passive mode, the link between the switches cannot be established.

To configure the operation mode of the member port, use the following command.

Command	Mode	Description
lacp port activity *PORTS* {**active** | **passive**}	Bridge	Configures the operation mode of the member port. (default: active)

To delete the configured operation mode of the member port, use the following command.

Command	Mode	Description
no lacp port activity *PORTS*	Bridge	Deletes the configured operation mode of the member port.

8.2.2.4 Priority of Switch

In case the member ports of connected switches are configured as Active mode (LACP system enabled), it is required to configure which switch would be a standard for it. For this case, the user could configure the priority on switch. The following is the command of configuring the priority of the switch in LACP function.

Command	Mode	Description
lacp system priority <1-65535>	Bridge	Sets the priority of the switch in LACP function, enter the switch system priority. (default: 32768)

To delete the priority of configured switch, use the following command.

Command	Mode	Description
no lacp system priority	Bridge	Clears the priority of the configured switch.

8.2.2.5 Manual Aggregation

The port configured as member port is basically configured to aggregate to LACP. However, even though the configuration as member port is not released, they could operate as independent port without being aggregated to LACP. These independent ports cannot be configured as trunk port because they are independent from being aggregated to LACP under the condition of being configured as member port.

To configure member port to aggregate to LACP, use the following command.

Command	Mode	Description
lacp port aggregation *PORTS* {**aggregatable** | **individual**}	Bridge	Configures the property of a specified member port for LACP. (default: aggregatable) AGGREGATIONS: aggregator number 1-8: minimum active member count
lacp port *PORTS* **aggregator** *AGGREGATIONS* [**active-link** *<1-8>*]		

To clear aggregated to LACP of configured member port, use the following command.

Command	Mode	Description
no lacp port aggregation *PORTS*	Bridge	Deletes the configured property of a specified member port for LACP.

8.2.2.6 BPDU Transmission Rate

Member port transmits BPDU with its information. For the OLT, it is possible to configure the BPDU transmission rate, use the following command.

Command	Mode	Description
lacp port timeout *PORTS* {**short** | **long**}	Bridge	Configures BPDU transmission rate: PORTS: select the port number. short: short timeout (1 sec) long: long timeout (30 sec: default)

To clear BPDU transmission rate, use the following command (clear means long timeout).

Command	Mode	Description
no lacp port timeout *PORTS*	Bridge	Clears BPDU transmission rate of configured member port, select the port number.

8.2.2.7 Administrational Key

Member port of LACP has key value. All member ports in one aggregator have same key values. To make the aggregator consisted of specified member ports, configure the different key value with the key value of another port.

Command	Mode	Description
lacp port admin-key *PORTS* <1-15>	Bridge	Configures the key value of a member port: PORTS: select the port number. 1-15: key value (default: 1)

To delete the key value of a specified member port, use the following command.

Command	Mode	Description
no lacp port admin-key *PORTS*	Bridge	Deletes the key value of a specified member port, select the member port number.

8.2.2.8 Port Priority

To configure priority of an LACP member port, use the following command.

Command	Mode	Description
lacp port priority *PORTS* <1-65535>	Bridge	Sets the LACP priority of a member port, select the port number. (default: 32768)

To delete the configured port priority of the member port, use the following command.

Command	Mode	Description
no lacp port priority *PORTS*	Bridge	Deletes the configured port priority of a selected member port, select the member port number.

8.2.2.9 Displaying LACP Configuration

To display a configured LACP, use the following command.

Command	Mode	Description
show lacp	Enable Global Bridge	Shows the information of lacp configuration.
show lacp aggregator		Shows the information of aggregated port.
show lacp aggregator *AGGREGATIONS*		Shows the information of selected aggregated port.
show lacp port		Shows the information of member port.
show lacp port *PORTS*		Shows the information of appropriated member port.
show lacp statistics		Shows aggregator statistics.

To clear LACP statistics information, use the following command.

Command	Mode	Description
clear lacp statistic	Enable Global Bridge	Clears the collected statistics.

8.3 Spanning Tree Protocol (STP)

The local area network (LAN), which is composed of double paths like token ring, has the advantage that it is possible to access in case of disconnection with one path. However there is another problem called a loop when you always use the double paths.

The loop may occur when double paths are used for the link redundancy between switches and one sends unknown unicast or multicast packet that causes endless packet floating on the LAN like loop topology. That superfluous traffic eventually can result in network fault. It causes superfluous data transmission and network fault.

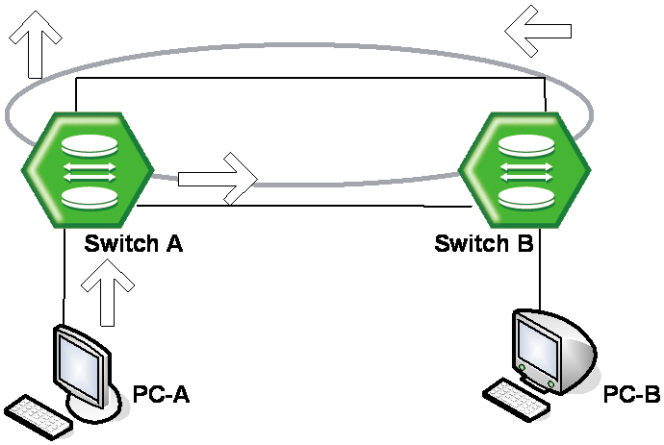


Fig. 8.9 Example of Loop

The spanning tree protocol (STP) is the function to prevent the loop in LAN with more than two paths and to utilize the double paths efficiently. It is defined in IEEE 802.1d. If the STP is configured in the system, there is no loop since it chooses more efficient path of them and blocks the other path. In other words, when SWITCH C in the below figure sends packet to SWITCH B, path 1 is chosen and path 2 is blocked.

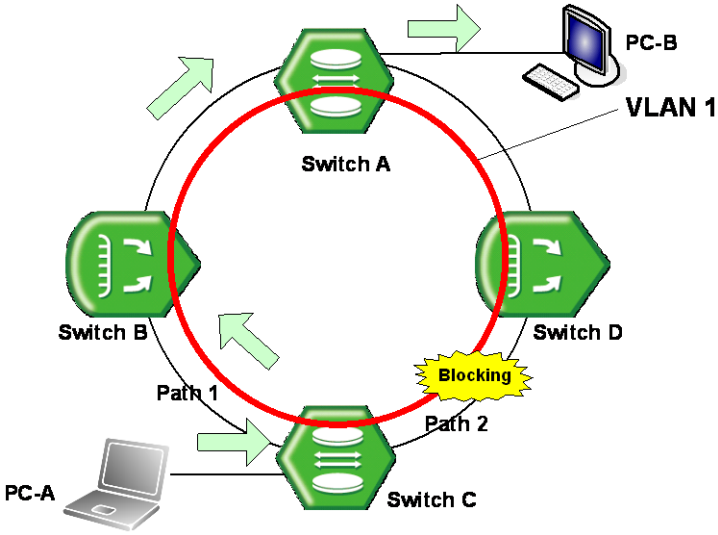


Fig. 8.10 Principle of Spanning Tree Protocol

Meanwhile, the rapid spanning tree protocol (RSTP) defined in IEEE 802.1w dramatically reduces the time of network convergence on the spanning tree protocol (STP). It is easy and fast to configure new protocol. The IEEE 802.1w also supports backward compatibility with IEEE 802.1d.

8.3.1 STP Operation

The 802.1d STP defines port state as blocking, listening, learning, and forwarding. When STP is configured in LAN with double paths, switches exchange their information including the bridge ID.

It is named as BPDU (Bridge Protocol Data Unit). Switches decide port state based on the exchanged BPDU and automatically decide an optimized path to communicate with the root switch.

8.3.1.1 Root Switch

The most important information to decide the root switch is bridge ID. A bridge ID is composed of 2 bytes-priority and 6 bytes-MAC address. The root switch has the lowest bridge ID.

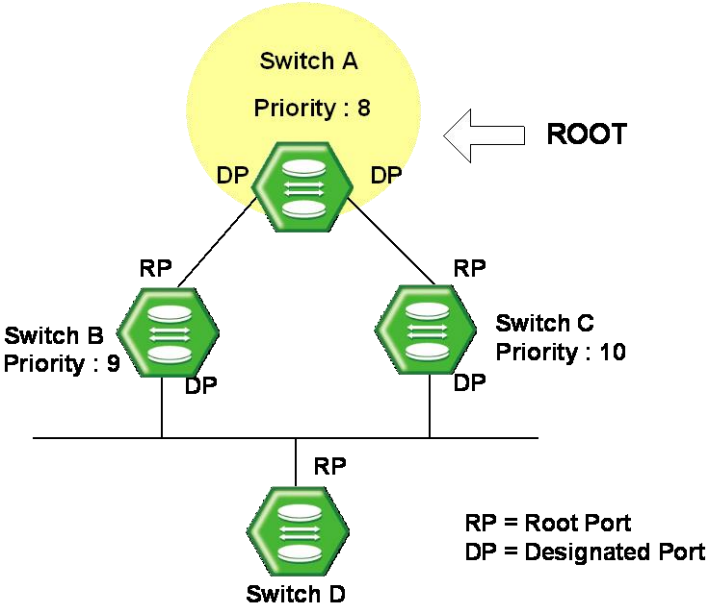


Fig. 8.11 Root Switch

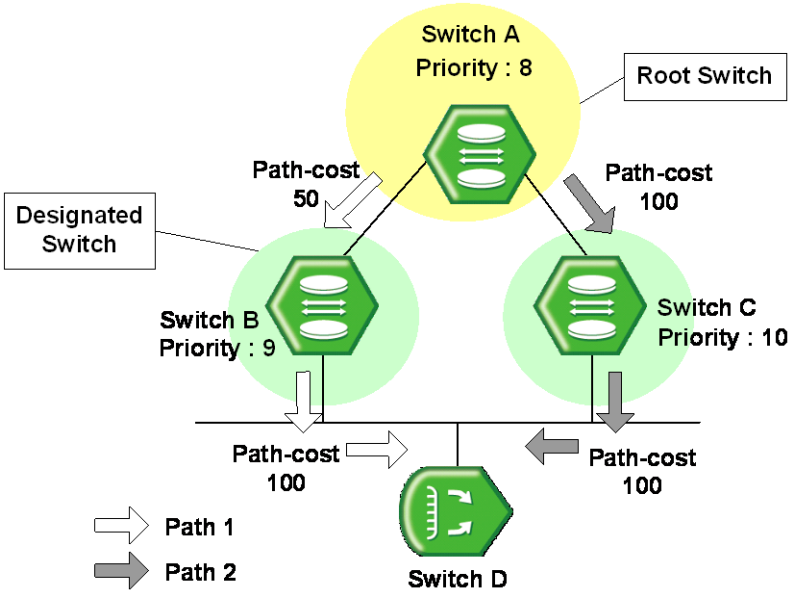
After configuring STP, these switches exchange their information. The priority of SWITCH A is 8, the priority of SWITCH B is 9, and the priority of SWITCH C is 10. In this case, SWITCH A is automatically configured as the root switch.

8.3.1.2 Designated Switch

After deciding the root switch, while SWITCH A transmits packets to SWITCH C, SWITCH

A compares the exchanged BPDU to decide the path to link. The critical information to decide path is the path-cost. The path-cost depends on the transmit rate of the LAN interface, and the path with the lower path-cost is selected.

The standard to decide designated switch is total root path-cost which is added with path-cost to the root. The path-cost depends on the transmit rate of the switch LAN interface, and the switch with lower path-cost is selected as designated switch.



(PATH 1 = 50 + 100 = 150, PATH 2 = 100 + 100 = 200, PATH 1 < PATH 2, ∴ **PATH 1 selected**

Fig. 8.12 Designated Switch

In case of the above figure with SWITCH A sending packet, the path-cost of PATH 1 is 150 and the path-cost of PATH 2 is total 200(100 + 100 ; path-cost of SWITCH A to C + path-cost of SWITCH C to D). Therefore the PATH 1 with lower path-cost is chosen. In this case, the port connected to the Root switch is named the Root port. In the above figure, the port of SWITCH C connected to SWITCH A as Root switch is the Root port. There can be only one Root port on the equipment.

The switch with lower path-cost is selected to be designated switch. If the root path-costs are same, bridge IDs are compared.

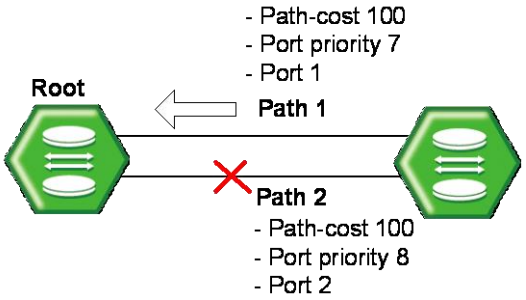
8.3.1.3 Designated Port and Root Port

Root Port is the port in the active topology that provides connectivity from the Desig-nated Switch toward the root. Designated Port is the port in the active topology used to forward traffic away from the root onto the link. That is, except the root port in each switch, the selected port to communicate is desig-nated port. The other ports, except root port and designated port, are named blocked port.

8.3.1.4 Port Priority

If the path-costs of two paths are same, decisions are based on port-priorities. In the figure below, suppose that two switches are connected. Since the path-costs of two paths are both 100, their port priorities are compared and the port with smaller port priority is selected to transmit the packet.

i All these functions are automatically performed by BPDU, which is the bridge information exchange between switches to activate or disable a specific port. It is also possible to configure BPDU to modify the root switch or the path manually.



(path-cost of PATH 1 = path-cost of PATH 2 = 100 ∴ unable to compare
PATH 1 port priority = 7, PATH 2 port priority = 8, PATH 1 < PATH 2, ∴ **PATH 1 is chosen**)

Fig. 8.13 Port Priority

Port States

Each port on a switch can be in one of five states.

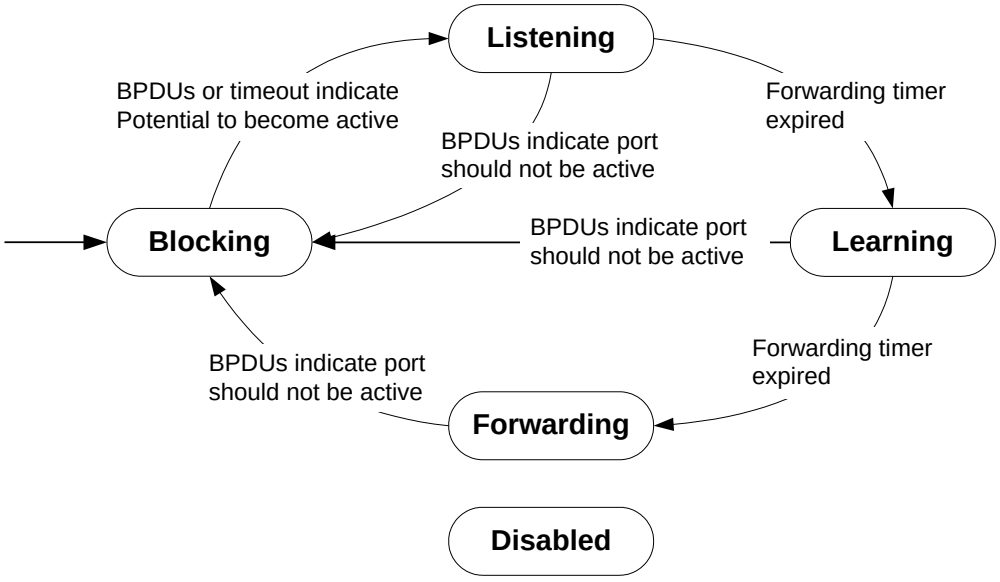


Fig. 8.14 Port States

- **Blocking**
  A port that is enabled, however neither a Designated port nor a Root port, will be in the blocking state. A blocking port will not receive or forward data frames, nor will it transmit BPDUs, but instead it will listen to other's BPDUs to determine if and when the port should consider becoming active in the spanning tree.
- **Listening**
  The port is still not forwarding data traffic, but is listening to BPDUs in order to compute the spanning tree. The port is comparing its own information (path cost, Bridge Identifier, Port Identifier) with the information received from other candidates and deciding which is best suited for inclusion in the spanning tree.
- **Learning**
  The port is preparing to forward data traffic. The port waits for a period of time to build its MAC address table before actually forwarding data traffic. This time is the forwarding delay.
- **Forwarding**
  After learning address, it is allowed to forward data frame. This is the steady state for a switch port in the active spanning tree.
- **Disabled**
  When disabled, a port will neither receive nor transmit data or BPDUs. A port is in this state because it is broken or disabled by administrator.

8.3.2 RSTP Operation

STP or RSTP is configured on network where Loop can be created. However, RSTP is more rapidly progressed than STP at the stage of reaching to the last topology. This section describes how the RSTP more improved than STP works. It contains the below sections.

- Port States
- BPDU Policy
- Rapid Network Convergence
- Compatibility with 802.1d

8.3.2.1 Port States

RSTP defines port states as discarding, learning, and forwarding. Blocking of 802.1d and listening is combined into discarding. Same as STP, root port and designated port are decided by port state. But a port in blocking state is divided into alternate port and backup port. An alternate port means a port blocking BPDUs of priority of high numerical value from other switches, and a backup port means a port blocking BPDUs of priority of high numerical value from another port of same equipment.

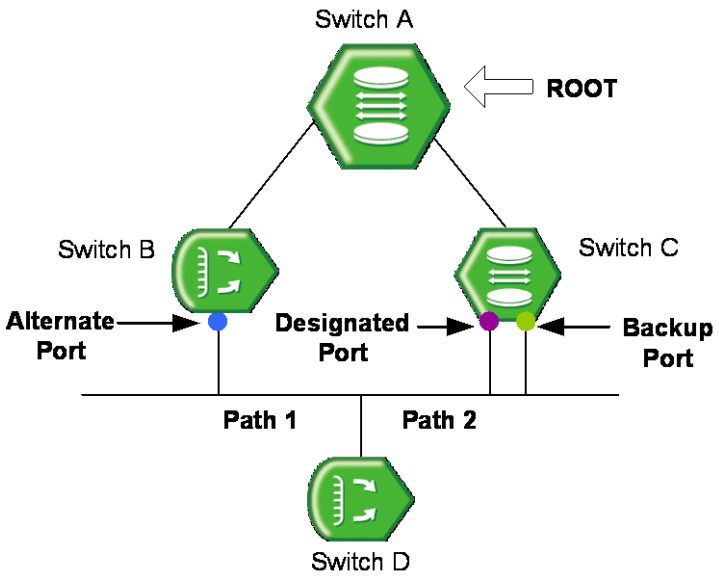


Fig. 8.15 Alternate Port and Backup port

The difference of between alternate port and backup port is that an alternate port can alternate the path of packet when there is a problem between Root switch and SWITCH C but Backup port cannot provide stable connection in that case.

8.3.2.2 BPDU Policy

In 802.1d, only the root switch forwards BPDU following Hello-time. However in 802.1w, not only root switch but also all the other switches forward BPDU following Hello-time. In 802w, BPDU is forwared more frequently than the interval of transmitting BPDU by the root switch in 802.1d.

If low BPDU is received from the root switch or the designated switch, it is immediately accepted. For example, suppose that the root switch is disconnected from the switch B in the figure below. Then, the switch B is considered to be the root due to the disconnection, and it forwards BPDU.

In this case, the switch C transmits BPDU including the root information to the switch B. Thus, SWITCH B configures a port connected to SWITCH C as the new root port.

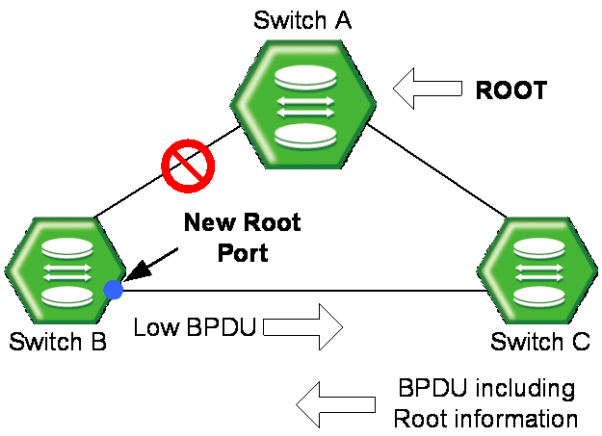


Fig. 8.16 Example of Receiving Low BPDU

8.3.2.3 Rapid Network Convergence

In the figure below, a new link is connected between SWITCH A and the root. Root and SWITCH A are not directly connected, but indirectly connected through SWITCH D. After SWITCH A is newly connected to the root, packets cannot be transmitted between the ports because the state of two switches becomes listening, and no loop is created.

In this state, if the root transmits BPDU to SWITCH A, SWITCH A transmits new BPDU to SWITCH B and SWITCH C, then SWITCH C transmits new BPDU to SWITCH D. SWITCH D, which received BPDU from SWITCH C, turns the port connected to SWITCH C into blocking state to prevent the loop after the new link.

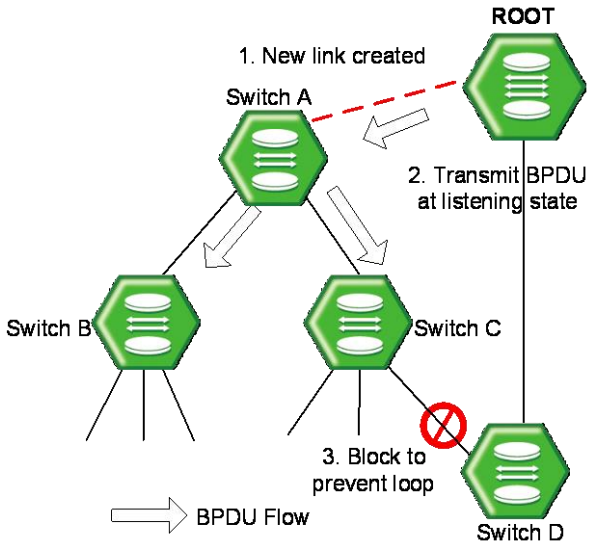


Fig. 8.17 Convergence of 802.1d Network

This is a very epochal way of preventing a loop. The matter is that communication is SWITCH D and SWITCH C is blocked. Then, right after the connection, it is possible to transmit BPDU although packets can not be transmitted and received between SWITCH A and the root.

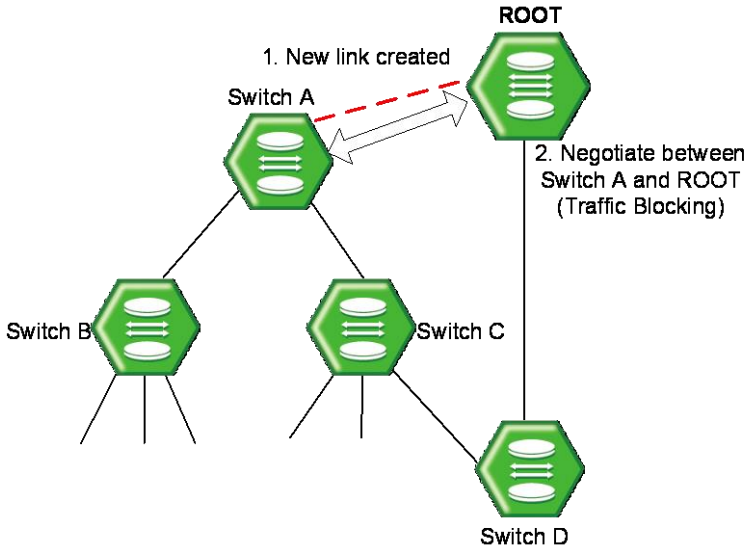


Fig. 8.18 Network Convergence of 802.1w (1)

SWITCH A negotiates with the root through BPDU. To make link between SWITCH A and the root, the state of non-edge designated port of SWITCH C is changed to blocking. Although SWITCH A is connected to the root, loop will not be generated because SWITCH A is blocked to SWITCH B and SWITCH C. In this state, BPDU from the root is transmitted to SWITCH B and SWITCH C through SWITCH A. To configure the forwarding state of SWITCH A, SWITCH A negotiates with SWITCH B and SWITCH C.

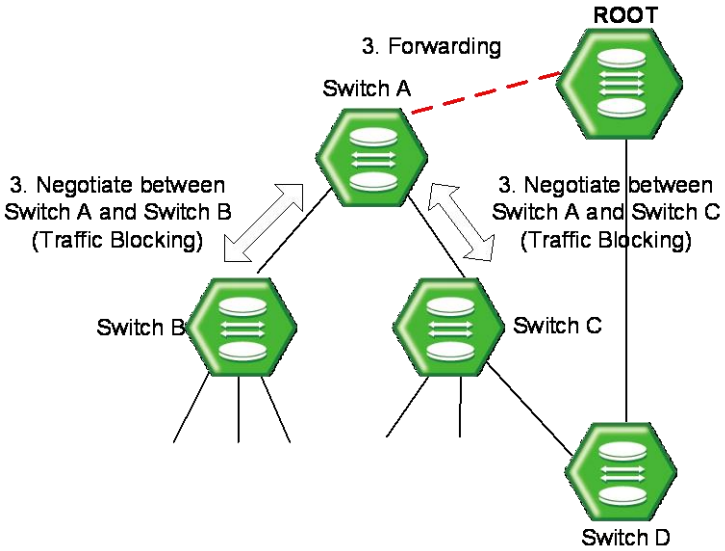


Fig. 8.19 Network Convergence of 802.1w (2)

SWITCH B has only edge-designated port. Edge-designated does not cause loop, so it is defined in 802.1w to be changed to forwarding state. Therefore, SWITCH B does not need to block specific port to the forwarding state of SWITCH A. However since SWITCH C has a port connected to SWITCH D, the port should be in the blocking state.

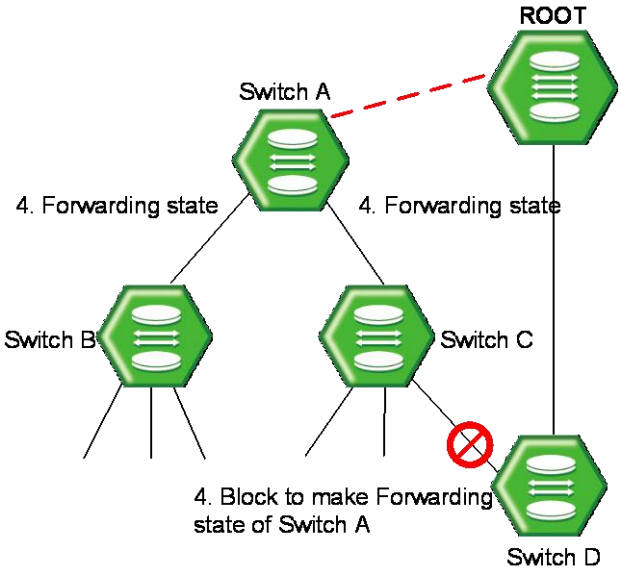


Fig. 8.20 Network Convergece of 802.1w (3)

It is same with 802.1d to block the connection of SWITCH D and SWITCH C. However, 802.1w does not need any configured time to negotiate between switches to make the forwarding state of specific port. So it is progressed very fast. During the progress to the port forwarding state, listening and learning are not needed. The negotiations use BPDU.

8.3.2.4 Compatibility with 802.1d

RSTP internally includes STP, so it has compatibility with 802.1d. Therefore, RSTP can recognize the BPDU of STP. However, STP cannot recognize the BPDU of RSTP. For example, assume that SWITCH A and SWITCH B are operated as RSTP and that SWITCH A is connected to SWITCH C as the designated switch. If SWITCH C is with 802.1d ignoring the BPDU of RSTP, it is interpreted as not connected to any switch or segment.

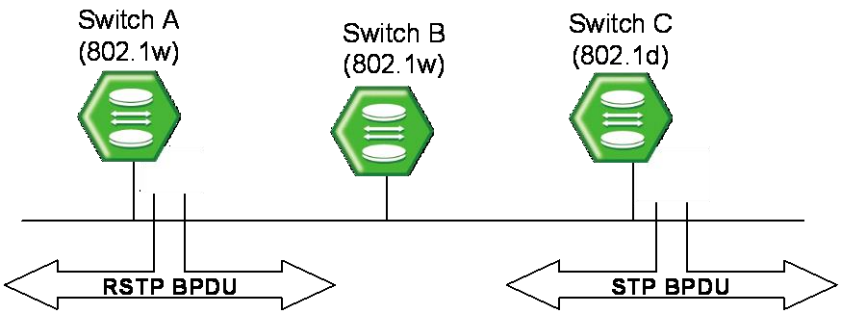


Fig. 8.21 Compatibility with 802.1d (1)

However, SWITCH A converts the port receiving BPDU into RSTP of 802.1d because it can read the BPDU of SWITCH C. Then SWITCH C can read BPDU of SWITCH A and accepts SWITCH A as the designated switch.

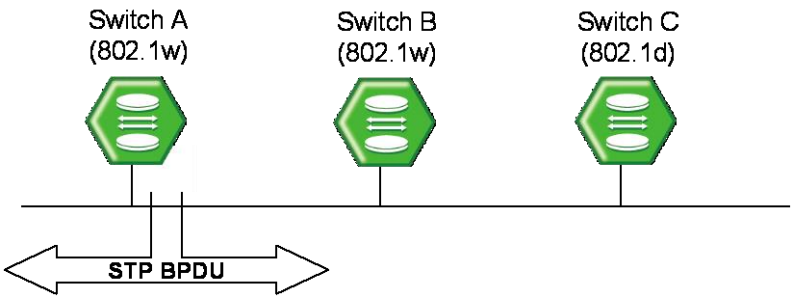


Fig. 8.22 Compatibility with 802.1d (2)

8.3.3 MSTP Operation

To operate the network more effectively, the OLT uses MSTP (Multiple Spanning-Tree Protocol). It constitutes the network with VLAN subdividing logically the existing LAN domain and configures the route by VLAN or VLAN group instead of existing routing protocol.

Operation

This section explains how STP/MSTP operate differently on the LAN. Suppose to configure 100 VLANs in the switch A, B, and C. In case of STP, there's only an STP on all of VLANs and it does not provide multiple Instances.

While existing STP is a protocol to prevent Loop in a LAN, domain establishes STP per VLAN in order to realize the routing suitable to the VLAN environment.

It does not need to calculate all STPs for several VLANs so that traffic overload could be reduced. By reducing unnecessary overload and providing multiple transmission routes for data forwarding, load balancing is realized and multiple VLANs are provided through Instances.

8.3.3.1 MSTP

In MSTP, VLAN is classified to the groups with the same Configuration ID. Configuration ID is composed of Revision name, Region name and VLAN/Instance mapping. Therefore, to have the same Configuration ID, all of the tree conditions should be the same. VLAN classified with the same Configuration ID is called MST region. In a region, there's only an STP so that it is possible to reduce the number of STP compared with PVSTP. There's no limitation for the region in a network environment, however it is possible to generate Instances up to 64 (1 to 64). Spanning-tree operating in each region is IST (Internal Spanning-Tree). CST is applied by connecting each spanning-tree of region. Instance 0 means that there is not any Instance generated from grouping VLAN, that is, it does not operate as MSTP. Therefore Instance 0 exists on all the ports of the equipment. After starting MSTP, all the switches in CST exchanges BPDU and CST root is decided by comparing their BPDU. The switches that don't operate with MSTP have Instance 0 so that they can also join BPDU exchanges. The operation of deciding CST Root is called CIST (Common & Internal Spanning-Tree).

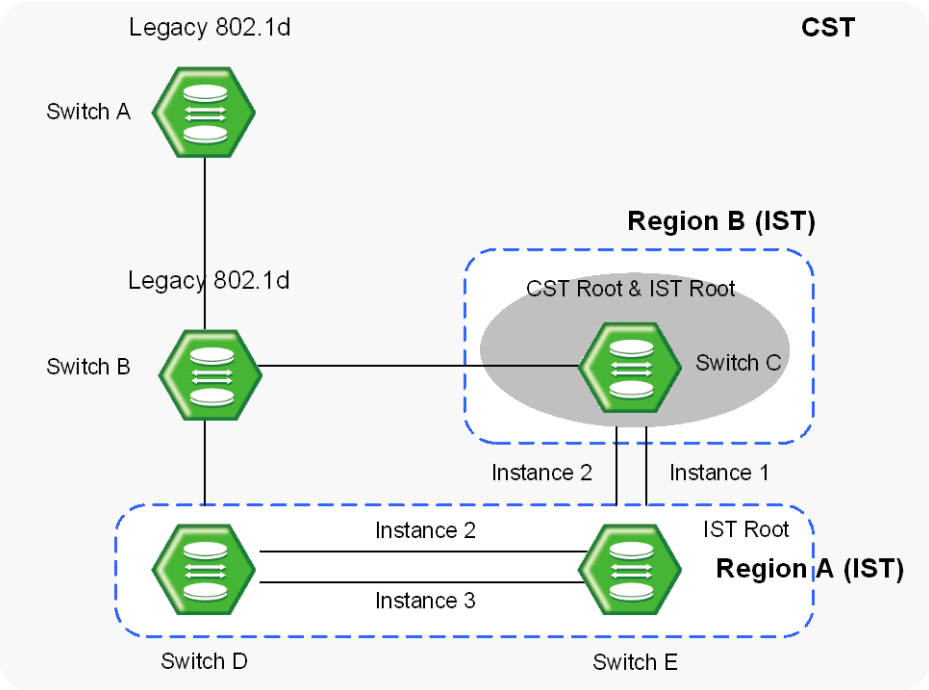


Fig. 8.23 CST and IST of MSTP (1)

In CST, A and B are the switches operating with STP, and C, D and E are those operating with MSTP. First, in CST, CIST is established to decide CST Root. After CST root is decided, the closest switch to CST root is decided as the IST root of the region. Here, the

CST root in IST is IST root.

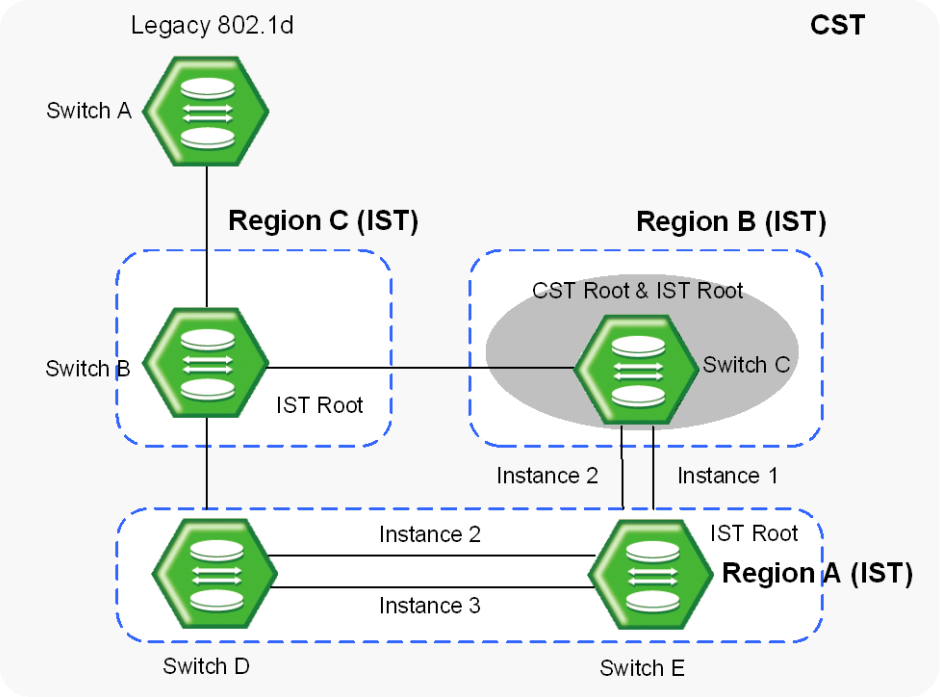


Fig. 8.24 CST and IST of MSTP (2)

In the above situation, if B operates with MSTP, B will send its BPDU to CST root and IST root in order to request itself to be CST root. However, if any BPDU with higher priority than that of B is sent, B cannot be CST root.

8.3.4 STP Mode

First of all, you need to enable STP function. You cannot configure any parameters related to Spanning Tree Protocol without this command.

To enable STP function on the OLT, use the following command.

Command	Mode	Description
spanning-tree	Bridge	Enables STP function.

To disable STP function from the system, use the following command.

Command	Mode	Description
no spanning-tree	Bridge	Disables STP function.

To select the spanning tree mode, use the following command.

Command	Mode	Description
spanning-tree mode { **mst** | **rapid-pvst** | **stp** | **rstp**}	Bridge	Configures a spanning-tree mode: mst: Multiple Spanning Tree Protocol (default) rapid-pvst: Per-vlan Rapid STP

To delete the configured spanning tree mode, use the following command.

Command	Mode	Description
no spanning-tree mode	Bridge	Deleted a configured spanning tree mode. (default: MSTP)

8.3.5 STP Basic Configuration

To configure STP, use the following steps.

Step 1
Enable STP function using the **spanning-tree** command.

Step 2
Configure detail options if specific commands are required.

8.3.5.1 Path-cost Method

After deciding a root switch, you need to decide to which route you will forward the packet. To do this, the standard is a path-cost.

Generally, a path cost depends on the transmission speed of LAN interface in the switch. The following table shows the path cost according to the transmit rate of LAN interface.

You can use same commands to configure STP and RSTP, but their path-costs are totally different. Please be careful not to make mistake.

Transmit Rate (bps)	Path-cost
4M	250
10M	100
100M	19
1G	4
10G	2

Tab. 8.2 STP Path-cost (short)

Transmit Rate (bps)	Path-cost
4M	20000000
10M	2000000
100M	200000
1G	20000
10G	2000

Tab. 8.3 RSTP Path-cost (long)

To decide the path-cost calculation method, use the following command.

Command	Mode	Description
spanning-tree pathcost method long	Bridge	Selects the method for calculating a RSTP path-cost: long: 32 bits of RSTP path-cost (IEEE 802.1D-2004).
spanning-tree pathcost method short		Selects the method for calculating a STP path-cost: short: 16bits of STP path-cost (IEEE 802.1D-1998).

To display the configured method for calculating the path-cost, use the following command.

Command	Mode	Description
show spanning-tree pathcost method	Bridge Global	Shows the configured method for calculating the path-cost.

To delete a configured method for caculating the path-cost and return the configuration to the default, use the following command.

Command	Mode	Description
no spanning-tree pathcost method	Bridge	Deletes the configured method of path-cost. (default: long)

When the route decided by path-cost gets overloading, you would better take another route. Considering these situations, it is possible to configure the path-cost of root port so that user can configure a route manually. To specify the path-cost value, use the following command.

Command	Mode	Description
spanning-tree port *PORTS* **cost** <1-200000000>	Bridge	Configures path-cost to configure route: PORTS: port number. 1-200000000: the path cost value.
no spanning-tree port *PORTS* **cost**		Deletes the configured path-cost, enter the port number.

8.3.5.2 Edge Ports

Edge ports are defined that the ports are connected to a nonbridging device. There are no switches or spanning-tree bridges directly connected to the edge port. To configure all ports as edge ports globally, use the following command.

Command	Mode	Description
spanning-tree edgeport default	Bridge	Configures all ports as edge ports: PORTS: port number
no spanning-tree edgeport default		Deleted a configured edge ports for all ports. (default)

To configure a specified port as edge port, use the following command.

Command	Mode	Description
spanning-tree port *PORTS* **edgeport enable**	Bridge	Configures specified port as edge port. PORTS: port number.
spanning-tree port *PORTS* **edgeport disable**		Disables edge port for specified port. PORTS: port number
no spanning-tree port *PORTS* **edgeport**		

8.3.5.3 BPDU Transmit hold count

You can configure the BPDU burst size by changing the transmit hold count value. To configure the transmit hold-count, use the following command.

Command	Mode	Description
spanning-tree transmit hold-count <1-20>	Bridge	Sets the number of BPDUs that can be sent before pausing for 1 second: 1-20: BPDU transmit hold-count value (default:6)
no spanning-tree transmit hold-count		Deletes a configured transmit hold-count value and returns to the default setting.

⚠ If you change this parameter to a higher value can have a significant impact on CPU utilization, especially in Rapid-PVST mode. We recommend that you maintain the default setting.

8.3.5.4 Port Priority

When all conditions of two switches are same, the last standard to decide route is port-

priority. It is also possible to configure port priority so that user can configure route manually. To configure the port-priority, use the following command.

Command	Mode	Description
spanning-tree port *PORTS* **port-priority** <0-240>	Bridge	Configures port priority. PORTS: port number 0-240: port priority in increments of 16 (default:128)
no spanning-tree port *PORTS* **port-priority**		Deleted a configured port priority.

8.3.5.5 Link Type

A port that operates in full-duplex is assumed to be point-to-point link type, while a half-duplex is considered as a shared port. .

To configure the link type of port, use the following command.

Command	Mode	Description
spanning-tree port *PORTS* **link-type** {**point-to-point** | **shared**}	Bridge	Specifies a link-type for a designated port PORTS: port number point-to-point: full-duplex shared: half-duplex

To delete a configured link type of port, use the following command.

Command	Mode	Description
no spanning-tree port *PORTS* **link-type**	Bridge	Deletes a configured link type.

8.3.5.6 Enabling STP configuration on the Port

To enable/disable a STP daemon by applying STP configurations to the port, use the following command.

Command	Mode	Description
spanning-tree port *PORTS* **enable**	Bridge	Enables STP function on the port
spanning-tree port *PORTS* **disable**		Disables STP function on the port.

8.3.5.7 Displaying Configuration

To display the configurations of STP, use the following command.

Command	Mode	Description
show spanning-tree	Enable Global Bridge	Shows all configurations of STP
show spanning-tree active [**detail**]	Bridge	Shows STP information on active interface: detail: detailed STP information (as option).
show spanning-tree blockedport		Shows information of the blocked ports
show spanning-tree detail [**active**]		Shows detailed information of STP.
show spanning-tree inconsistentports		Shows information of root-inconsistency state.
show spanning-tree bridge [**address** | **detail** | **forward-time** | **hello-time** | **id** | **max-age** | **protocol** | **priority** [**system-id**]]		Shows information of the bridge status and configuration
show spanning-tree root [**address** | **cost** | **detail** | **forward-time** | **hello-time** | **id** | **max-age** | **port** | **priority** [**system-id**]]		Shows the status and configuration for the root bridge.
show spanning-tree port *PORTS* [**active** [**detail**] | **cost** | **detail** [**active**] | **edgeport** | **inconsistency** | **rootcost** | **state** | **priority**]		Shows STP information of specified port.
show spanning-tree summary [**totals**]		Shows a summary of STP: totals: the total lines of STP

8.3.6 Configuring MSTP

To configure MSTP, use the following steps.

Step 1
Enable STP function using the **spanning-tree** command.

Step 2
Select a MSTP mode using the **spanning-tree mode mst** command.

Step 3
Configure detail options if specific commands are required.

Step 4

Enable a MSTP daemon using the **spanning-tree mst** command.

8.3.6.1 MST Region

To set the configuration ID of MST region in detail, you need to open *MSTP Configuration* mode first. To open *MSTP Configuration* mode, use the following command.

Command	Mode	Description
spanning-tree mst configuration	Bridge	Opens *MSTP Configuration* mode.

After opening *MSTP Configuration* mode, the prompt changes from SWITCH(bridge)# to SWITCH(config-mst)#.

To delete all configations from *MSTP Configuration* mode, use the following command.

Command	Mode	Description
no spanning-tree mst configuration	Bridge	Deletes all configurations on *MSTP Configuration* mode, returns to the default values.

If MSTP is established in the OLT, decide a MSTP region the switch is going to belong to by configuring the MST configuration ID. Configuration ID contains a region name, revision, and a VLAN map.

To set the configuration ID, use the following command on *MSTP Configuration* mode.

Command	Mode	Description
name *NAME*	MST-config	Sets the MSTP region name: NAME: the name of MSTP region.
instance <1-64> **vlan** *VLANS*		Maps the specified vlans to an MSTP instance: 1-64: select an instance ID number. VLANS: VLAN ID (1-4094)
revision <0-65535>		Specifies a revision number: 0-65535: the MSTP configuration revision number.

i In case of configuring STP and RSTP, you do not need to set the configuration ID. If you try to set configuration ID on STP or RSTP, an error message will be displayed.

i You can create the MSTP regions without limit on the network. But the instance id numbers of each region should not be over 64.

To delete the configuration ID setting, use the following command.

Command	Mode	Description
no name	MST-config	Deletes the name of MSTP region
no instance <1-64> **vlan** *VLANS*		Deletes part of vlan-mapping, select the instance ID number and vlan id to remove from the specified instance 1-64: instance ID number VLANS: VLAN ID (1-4094)
no revision		Deletes the configured revision number.

After configuring the configuration ID in the OLT, you should apply the configuration to the switch. After changing or deleting the configuration, you must apply it to the switch. If not, it does not being reflected into the switch.

To apply the configuration to the system, use the following command.

Command	Mode	Description
apply	MST-config	Apllies the configuration of the region to the system.

i After deleting the configured configuration ID, apply it to the system using the above command.

To display the current and edited configuration on *MSTP Configuration* mode, use the following command.

Command	Mode	Description
show current	MSTP	Shows the current configuration as it is used to run MSTP
show pending		Shows the edited configuration of MSTP.
show		Shows all configurations of MSTP

For example, after setting the configuration ID, if you apply it to the switch with the **apply** command, you can check the configuration ID with the **show current** command.

However, if the user did not use the **apply** command to apply the configurations to the switch, the configuration could be checked with the **show pending** command.

8.3.6.2 Enabling MSTP configuration

To enable/disable a MSTP daemon by applying MSTP configurations to the system, use the following command.

Command	Mode	Description
spanning-tree mst	Bridge	Enables MSTP function on the system
no spanning-tree mst		Disables MSTP function on the system.

8.3.6.3 Root Switch

To establish MSTP function, a root switch should be chosen first. In MSTP, a root switch is called as IST root switch. Each switch has its own bridge ID, and one of the switchs on same LAN is chosen as a root switch by comparing with their bridge IDs. However, you can configure the priority and make it more likely that the switch will be chosen as the root switch. The switch having the lowest priority becomes the root switch.

To configure the priority for an MSTP instance number, use the following command.

Command	Mode	Description
spanning-tree mst <0-64> **priority** <0-61440>	Bridge	Configures the priority of the switch: 0-64: MSTP instance ID number. 0-61440: priority value in increments of 4096 (default: 32768)
no spanning-tree mst <0-64> **priority**		Clears the Priority of the switch, enter the instance number.

i If you configure a priority of STP or RSTP in the OLT, you should configure MSTP instance ID number as 0.

8.3.6.4 Path-cost

After deciding a root swich, you need to decide to which route you will forward the packet. To do this, the standard is a path-cost. By the path-cost of root port, you can configure a route manually. To configure the path-cost value for specified instance number in MSTP, use the following command.

Command	Mode	Description
spanning-tree mst <0-64> **port** *PORTS* **cost** <1-200000000>	Bridge	Configures path-cost for specified MSTP instance number: 0-64: MSTP instance ID number. 1-200000000: the path cost value.
no spanning-tree mst <0-64> **port** *PORTS* **cost**		Deletes a configured path-cost.

8.3.6.5 Port Priority

When all conditions of two routes of switch are same, the last standard to decide a route is port-priority. You can configure port priority and select a route manually.

To configure a port priority for MSTP instance, use the following command.

Command	Mode	Description
spanning-tree mst <0-64> **port** *PORTS* **port-priority** <0-240>	Bridge	Configures the port priority of MSTP instance. 0-64: MSTP instance ID number PORTS: port number 0-240: port priority in increments of 16 (default:128)
no spanning-tree mst <0-64> **port** *PORTS* **port-priority**		Deletes a configured port priority of MSTP instance.

8.3.6.6 Displaying Configuration

To display the configuration of MSTP, use the following command.

Command	Mode	Description
show spanning-tree mst <1-64>	Enable Global Bridge	Shows all configurations of a specific MSTP instance: 1-64: MSTP instance ID number
show spanning-tree mst <1-64> **active** [**detail**]	Bridge	Shows information of a specific MSTP instance on active interface: 1-64: MSTP instance ID number. detail: detailed MSTP information (as option).
show spanning-tree mst <1-64> **blockedport**		Shows information of the blocked ports
show spanning-tree mst <1-64> **detail** [**active**]		Shows detailed information of the specific MSTP instance: 1-64: MSTP instance ID number.
show spanning-tree mst <1-64> **inconsistentports**		Shows information of root-inconsistency state. 1-64: MSTP instance ID number.
show spanning-tree mst <1-64> **bridge** [**address** | **detail** | **forward-time** | **hello-time** | **id** | **max-age** | **protocol** | **priority** | **priority [system-id]**]		Shows information of the bridge status and configuration of a specific MSTP instance 1-64: MSTP instance ID number.
show spanning-tree mst <1-64> **root** [**address** | **cost** | **detail** | **forward-time** | **hello-time** | **id** | **max-age** | **port** | **priority** | **priority [system-id]**]		Shows the status and configuration for the root bridge of a specifiec MSTP instance. 1-64: MSTP instance ID number.
show spanning-tree mst <1-64> **port** *PORTS* [**active** [**detail**] | **cost** | **detail** [**active**] | **edgeport** | **inconsistency** | **rootcost** | **state** | **priority**]		Shows information of MSTP instance for specified port. 1-64: MSTP instance ID number.
show spanning-tree mst configuration [**digest**]		Shows information of the region configuration: digest: MD5 digest included in the current MSTCI
show spanning-tree mst <1-64> **summary** [**totals**]		Shows a summary of a specific MSTP instance: totals: the total lines of MSTP

8.3.7 Configuring PVSTP

STP and RSPT are designed with one VLAN in the network. If a port becomes blocking state, the physical port itself is blocked. But PVSTP (Per VLAN Spanning Tree Protocol) and PVRSTP (Per VLAN Rapid Spanning Tree Protocol) maintains spanning tree instance for each VLAN in the network. Because PVSTP treats each VLAN as a separate network, it has the ability to load balance traffic by forwarding some VLANs on one trunk and other VLANs. PVRSTP provides the same functionality as PVSTP with enhancement.

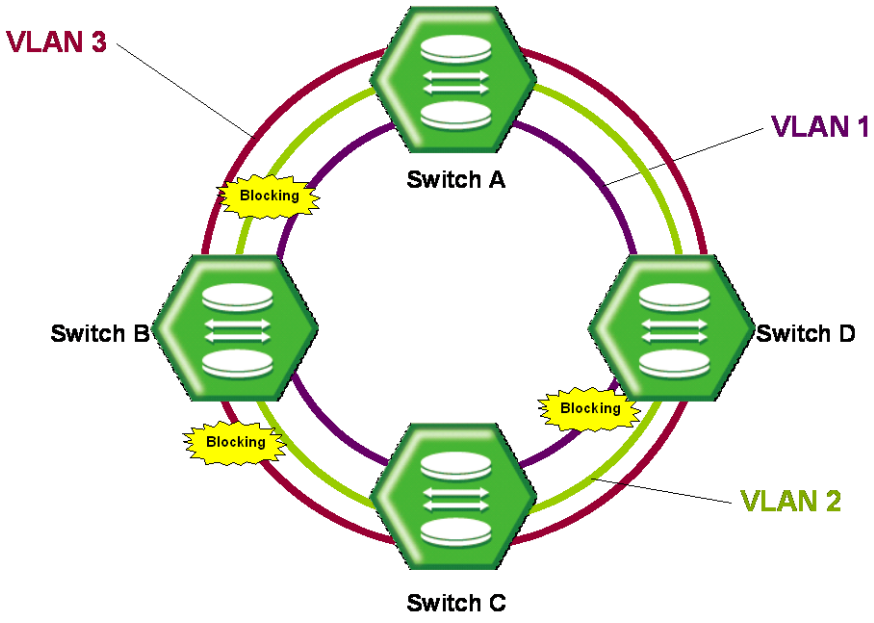


Fig. 8.25 Example of PVSTP

To configure PVSTP, use the following steps.

Step 1
Enable STP function using the **spanning-tree** command.

Step 2
Decide PVSTP mode using the **spanning-tree mode rapid-pvst** command.

Step 3
Enable PVSTP function using the **spanning-tree vlan** *VLANS* command.

Step 4
Configure detail options if specific commands are required.

8.3.7.1 Enabling PVSTP

To enable PVSTP function, use the following command.

Command	Mode	Description
spanning-tree vlan *VLANS*	Bridge	Activates PVSTP function. VLANS: VLAN ID (1-4094)

PVSTP is activated after selecting PVSTP mode using **spanning-tree mode rapid-pvst** command. In PVSTP, you can configure the current VLAN only. If you input VLAN that does not exist, error message is displayed.

For the switches in LAN where dual path does not exist, Loop does not generate even though STP function is not configured.

To disable a configured PVSTP, use the following command.

Command	Mode	Description
no spanning-tree vlan *VLANS*	Bridge	Disables PVSTP in VLAN. VLANS: VLAN ID (1-4094)

8.3.7.2 Root Switch

To establish PVSTP function, a root switch should be chosen first. Each switch has its own bridge ID, and one of the switchs on same LAN is chosen as a root switch by comparing with their bridge IDs. A bridge ID, consisting of the switch priority and the switch MAC address, is associated with each instance. However, you can configure the priority and make it more likely that the switch will be chosen as the root switch. The switch having the lowest priority becomes the root switch for that VLAN.

To configure the switch priority for a VLAN, use the following command.

Command	Mode	Description
spanning-tree vlan *VLANS* **priority** <0-61440>	Bridge	Configures a priority for specified VLAN. VLANS: VLAN ID (1-4094) 0-61440: priority value in increments of 4096 (default: 32768)
no spanning-tree vlan *VLANS* **priority**		Deletes a configured priority for specified VLAN.

8.3.7.3 Path-cost

After deciding Root switch, you need to decide to which route you will forward the packet. To do this, the standard is path-cost. Generally, path-cost depends on transmission speed of LAN interface in switch. In case the route is overload based on Path-cost, it is better to take another route.

By considering the situation, the user can configure Path-cost of Root port in order to designate the route on ones own.

To configure the path-cost value for specified vlan in PVSTP, use the following command.

Command	Mode	Description
spanning-tree vlan *VLANS* **port** *PORTS* **cost** <1-200000000>	Bridge	Configures path-cost to configure route on user's own. VLANS: VLAN ID (1-4094) PORTS: port number
no spanning-tree vlan *VLANS* **port** *PORTS* **cost**		Deleted a configured path-cost.

8.3.7.4 Port Priority

When all conditions of two routes of switch are same, the last standard to decide a route is port-priority. You can configure port priority and select a route manually.

To configure a port priority for specified VLAN, use the following command.

Command	Mode	Description
spanning-tree vlan *VLANS* **port** *PORTS* **port-priority** <0-240>	Bridge	Configures the port priority of specific VLAN. VLANS: VLAN ID (1-4094) 0-240: port priority in increments of 16 (default:128)
no spanning-tree vlan *VLANS* **port** *PORTS* **port-priority**		Deleted the configuration port priority of specifiec VLAN

8.3.7.5 Displaying Configuration

To display the configuration after configuring PVSTP, use the following command.

Command	Mode	Description
show spanning-tree vlan *VLANS*	Enable Global Bridge	Shows all configurations of a specific vlan id: VLANS: VLAN ID (1-4094)
show spanning-tree vlan *VLANS* **port** *PORTS* [**active** [**detail**] | **cost** | **detail** [**active**] | **edgeport** | **inconsistency** | **rootcost** | **state** | **priority**]		Shows information of vlan id for specified port. VLANS: VLAN ID (1-4094)
show spanning-tree vlan *VLANS* **active** [**detail**]	Bridge	Shows information of a specific vlan id on active interface: detail: detailed PVSTP information (as option).
show spanning-tree vlan *VLANS* **blockedport**		Shows information of the blocked ports
show spanning-tree vlan *VLANS* **detail** [**active**]		Shows detailed information of the specific vlan id: VLANS: VLAN ID (1-4094)
show spanning-tree vlan *VLANS* **inconsistentports**		Shows information of root-inconsistency state. VLANS: VLAN ID (1-4094)
show spanning-tree vlan *VLANS* **bridge** [**address** | **detail** | **forward-time** | **hello-time** | **id** | **max-age** | **protocol** | **priority** [**system-id**]]		Shows information of the bridge status and configuration of a specific vlan id VLANS: VLAN ID (1-4094)
show spanning-tree vlan *VLANS* **root** [**address** | **cost** | **detail** | **forward-time** | **hello-time** | **id** | **max-age** | **port** | **priority** [**system-id**]]		Shows the status and configuration for the root bridge of a specifiec vlan id. VLANS: VLAN ID (1-4094)
show spanning-tree vlan *VLANS* **summary** [**totals**]		Shows a summary of a specific vlan id: totals: the total lines of PVSTP

8.3.8 Root Guard

The standard STP does not allow the administrator to enforce the position of the root bridge, as any bridge in the network with lower bridge ID will take the role of the root bridge. Root guard feature is designed to provide a way to enforce the root bridge placement in the network. Even if the administrator sets the root bridge priority to zero in an effort to secure the root bridge position, there is still no guarantee against bridge with priority zero and a lower MAC address.

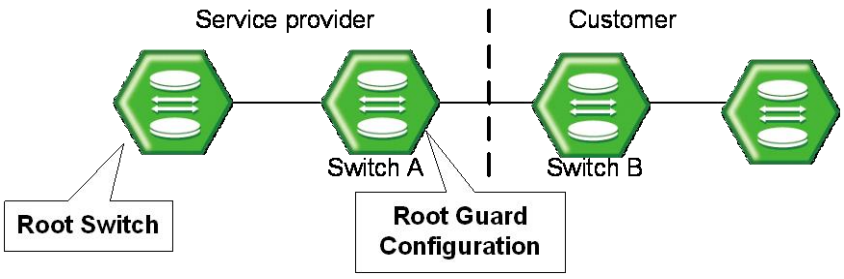


Fig. 8.26 Root Guard

Software-based bridge applications launched on PCs or other switches connected by a customer to a service-provider network can be elected as root switches. If the priority of bridge B is zero or any value lower than that of the root bridge, device B will be elected as a root bridge for this VLAN. As a result, network topology could be changed. This may lead to sub-optimal switching. But, by configuring root guard on switch A, no switches behind the port connecting to switch A can be elected as a root for the service provider's switch network. In which case, switch A will block the port connecting switch B.

To configure Root-Guard, use the following command.

Command	Mode	Description
spanning-tree port *PORTS* **guard root**	Bridge	Configures Root Guard on the network.

To delete a configured Root-Guard of specified port, use the following command.

Command	Mode	Description
spanning-tree port *PORTS* **guard none**	Bridge	Disables Root Guard function.
no spanning-tree port *PORTS* **guard**		Deletes a configured Root Guard, returns to default configurations.

8.3.9 Loop Guard

An STP loop is created when an STP blocking port in an redundant topology erroneously transitions to the forwarding state. This usually happens because one of the ports in a physically redundant topology no longer receives BPDUs. In this case, the designated port transmits BPDUs, and the non-designated port receives BPDUs. As a result, the blocking port from the alternate or backup port eventually becomes designated and moves to forwarding state. This might cause a loop if the reason for not receiving BPDUs has been other than actual failure of a link. If BPDUs are not received on a non-designated port when loop guard is enabled, that port is moved into the STP loop-inconsistent blocking state, instead of the listening / learning / forwarding state. Without the loop guard feature, the port assumes the designated port role. The port moves to the STP forwarding state and creates a loop.

To enable/disable the loop guard on the specified port, use the following command.

Command	Mode	Description
spanning-tree port *PORTS* **guard loop**	Bridge	Enables the loop guard on the ports
spanning-tree port *PORTS* **guard none**		Disables the loop guard on the ports.

To enable/disable the loop guard on all the ports, use the following command.

Command	Mode	Description
spanning-tree loopguard default	Bridge	Enables loop guard function on all the ports.
no spanning-tree loopguard default		Disables loop guard function on all the ports.

8.3.10 Topology Change Detection

The ability to detect topology changes can be enabled or disabled on a per-port. If the TCN guard function is enabled on a port, it detects its STP topology change.

To configure TCN Guard on the ports, use the following command.

Command	Mode	Description
spanning-tree port *PORTS* **tcnguard enable**	Bridge	Enables a guard for STP topology change notification.
spanning-tree port *PORTS* **tcnguard disable**		Disables a guard for STP topology change notification..
no spanning-tree port *PORTS* **tcnguard**		

8.3.11 Restarting Protocol Migration

MSTP protocol has a backward compatibility. MSTP is compatible with STP and RSTP. If some other bridge runs on STP mode and sends the BPDU version of STP or RSTP, MSTP automatically changes to STP mode. But STP mode cannot be changed to MSTP mode automatically. If administrator wants to change network topology to MSTP mode, administrator has to clear the previously detected detected protocol manually.

To prevent this, the OLT provides the **clear spanning-tree detected-protocols** command. If you enable this command, the switch checks STP protocol packet once again. To clear configured Restarting Protocol Migration, use the following command.

Command	Mode	Description
clear spanning-tree detected-protocols	Bridge	Restarts protocol migration function.
clear spanning-tree port *PORTS* **detected-protocols**		Restarts protocol migration function of specified port: PORTS: port number

8.3.12 Loop Back Detection

The problem occurs because the keepalive packet is looped back to the port that sent the keepalive. Keepalives are sent on the switches in order to prevent loops in the network. You see this problem on the device that detects and breaks the loop, but not on the device that causes the loop.

To enable error-disable detection for loop back cause, use the following command.

Command	Mode	Description
errdisable detect cause loopback	Bridge	Enables error-disable detection for loop back cause
no errdisable detect cause loopback		Disables error-disable detection for loop back cause

To display the status of error-disable cause, use the following command.

Command	Mode	Description
show errdisable detect cause	Bridge	Shows status of error-disable causes

To enable/disable the error-disable recovery function for loop back cause, use the following command.

Command	Mode	Description
errdisable recovery cause loopback	Bridge	Enables the recovery function for loop back error-disable cause
no errdisable recovery cause loopback		Disables the recovery function for loop

		back error-disable cause

To specify the time to recover from a specified error-disable cause, use the following command.

Command	Mode	Description
errdisable recovery interval <30-86400>	Bridge	Sets the interval of error-disable recovery: 30-86400: the recovery interval (default: 300 sec)
no errdisable recovery interval		Deleted the con figured time for error-disable recovery and returns to the default setting.

To display information of error-disable recovery function, use the following command.

Command	Mode	Description
show errdisable recovery	Bridge	Shows information of error-disable recovery function.

To enable/disable the debugging function of error-disable status caused by loop back, use the following command.

Command	Mode	Description
debug errdisable loopback enable	Enable	Enables the debugging for loop back error-disable cause.
debug errdisable loopback disable		Disables the debugging for loop back error-disable cause.

8.3.13 BPDU Configuration

BPDU is a transmission message in LAN in order to configure, and maintain the configuration for STP/RSTP/MSTP. Switches that STP is configured exchange their information BPDU to find the best path. MSTP BPDU is a general STP BPDU having additional MST data on its end. MSTP part of BPDU does not rest when it is out of region.

- **Hello Time**
  Hello time is an interval of which a switch transmits BPDU. It can be configured from 1 to 10 seconds. The default is 2 seconds.
- **Max Age**
  Root switch transmits new information every time based on information from other switches. However, if there are many switches on network, it takes lots of time to transmit BPDU. And if network status is changed while transmitting BPDU, this information is useless. To get rid of useless information, max age should be identified each information.
- **Forward Delay**
  Switches find the location of other switches connected to LAN though received BPDU and transmit packets. Since it takes certain time to receive BPDU and find the location before transmitting packet, switches send packet at regular interval. This interval time is named forward delay.

i The configuration for BPDU is applied as selected in force-version. The same commands are used for STP, RSTP, MSTP and PVSTP.

8.3.13.1 Hello Time

Hello time decides an interval time when a switch transmits BPDU. To configure hello time, use the following command.

Command	Mode	Description
spanning-tree mst hello-time <1-10>	Bridge	Configures hello time to transmit the message in MSTP. 1-10: the hello time. (default: 2 sec)
spanning-tree vlan *VLANS* **hello-time** <1-10>		Configures hello time to transmit the message in PVSTP per VLAN. 1-10: the hello time. (default: 2 sec) VLANS: VLAN ID (1-4094)

To delete a configured hello-time, use the following command.

Command	Mode	Description
no spanning-tree mst hello-time	Bridge	Returns to the default hello time value of STP, RSTP and MSTP.
no spanning-tree vlan *VLANS* **hello-time**		Returns to the default hello time value of PVSTP.

8.3.13.2 Forward Delay Time

It is possible to configure forward delay, which means time to take port status from listening to forwarding. To configure forward delay, use the following command.

Command	Mode	Description
spanning-tree mst forward-time <4-30>	Bridge	Sets the forward-delay time for all MST instances: 4-30: forward delay time value (default:15)
spanning-tree vlan *VLANS* **forward-time** <4-30>		Sets the forward-delay time of PVSTP per VLAN: VLANS: VLAN ID (1-4094) 4-30: forward delay time value (default:15)

To delete a configured forward delay time, use the following command.

Command	Mode	Description
no spanning-tree mst forward-time	Bridge	Returns to the default value of MSTP.
no spanning-tree vlan *VLANS* **forward-time**		Returns to the default value of PVSTP per VLAN.

8.3.13.3 Max Age

Maximum aging time is the number of seconds a switch waits without receiving spanning-tree configuration messages before attempting a reconfiguration.

To configure the maximum aging time for deleting useless messages, use the following command.

Command	Mode	Description
spanning-tree mst max-age <6-40>	Bridge	Changes the maximum aging time of route message of MSTP. 6-40: maximum aging time value (default: 20 sec)
spanning-tree vlan *VLANS* **max-age** <6-40>		Changes the maximum aging time of route message of PVSTP per specified VLAN. VLANS: VLAN ID (1-4094) 6-40: maximum aging time value (default: 20 sec)

i We recommend that the maximum aging time is set less than twice of forward delay time and more than twice of hello time.

To delete a configured maximum aging time, use the following command.

Command	Mode	Description
no spanning-tree mst max-age	Bridge	Returns to the default maximum aging time value of MSTP.
no spanning-tree vlan *VLANS* **max-age**		Returns to the default maximum aging time value of PVSTP. VLANS: VLAN ID (1-4094)

8.3.13.4 BPDU Hop Count

In MSTP, it is possible to configure the number of hops in order to prevent BPDU from wandering. BPDU passes the switches as the number of hops by this function.

To configure the number of hops of BPDU in MSTP, use the following command.

Command	Mode	Description
spanning-tree mst max-hops <1-40>	Bridge	Configures the number of hops for BPDU, set the number of possible hops in MSTP region: 1-40: the number of hops for BPDU (default:20)
no spanning-tree mst max-hops		Deletes the number of hops for BPDU in MSTP.

8.3.13.5 BPDU Filtering

BPDU filtering allows you to avoid transmitting on the ports that are connected to an end system. If the BPDU Filter feature is enabled on the port, then incoming BPDUs will be filtered and BPDUs will not be sent out of the port.

To enable or disable the BPDU filtering function on the port, use the following command.

Command	Mode	Description
spanning-tree port *PORTS* **bpdufilter enable**	Bridge	Enables a BPDU filtering fuction on specific port.
spanning-tree port *PORTS* **bpdufilter disable**		Disables a BPDU filtering fuction on specific port.
no spanning-tree port *PORTS* **bpdufilter**		

By default, it is disabled. The BPDU filter-enabled port acts as if STP is disabled on the port. This feature can be used for the ports that are usually connected to an end system or the port that you don't want to receive and send unwanted BPDU packets. Be cautious about using this feature on STP enabled uplink or trunk port. If the port is removed from VLAN membership, correspond BPDU filter will be automatically deleted.

To enable or disable the BPDU filtering function on the edge port, use the following command.

Command	Mode	Description
spanning-tree edgeport bpdufilter default	Bridge	Enables a BPDU filtering function by default on all edge ports.
no spanning-tree edgeport bpdufilter default		Disables a BPDU filtering function by default on all edge ports.

8.3.13.6 BPDU Guard

BPDU guard has been designed to allow network designers to enforce the STP domain borders and keep the active topology predictable. The devices behind the ports with STP enabled are not allowed to influence the STP topology. This is achieved by disabling the port upon receipt of BPDU. This feature prevents Denial of Service (DoS) attack on the network by permanent STP recalculation. That is caused by the temporary introduction and subsequent removal of STP devices with low (zero) bridge priority.

To configure BPDU guard in the switch, perform the following procedure.

Step 1
Configure the specific port as edge-port.

Command	Mode	Description
spanning-tree port *PORTS* **edgeport enable**	Bridge	Configures the port as Edge port.

Step 2
Enable BPDU guard function on edge port or specific port, use the following command.

Command	Mode	Description
spanning-tree edgeport	Bridge	Enables BPDU Guard function on edge ports

bpduguard default		
spanning-tree port *PORTS* **bpduguard enable**		Enables BPDU Guard function on specified port

To disable BPDU guard function on edge port or specific port, use the following command.

Command	Mode	Description
no spanning-tree edgeport bpduguard default	Bridge	Disables BPDU Guard function of edge ports (default)
spanning-tree port *PORTS* **bpduguard disable**		Disables BPDU Guard function of specified port. (default)
no spanning-tree port *PORTS* **bpduguard**		

However, BPDU Guard can be corrupted by unexpected cause. In this case, the edge port is blocked immediately and remains at this state until user recovers it. To prevent this problem, the OLT provides error-disable recovery function for BPDU guard cause. When an edge port is down for BPDU packet which came from other switch, the port is recovered automatically after configured time.

To enable the recovery function for BPDU guard error-disable cause, use the following command.

Command	Mode	Description
errdisable recovery cause bpduguard	Bridge	Enables the recovery function for BPDU guard error-disable cause
no errdisable recovery cause bpduguard		Disables the recovery function for BPDU guard error-disable cause

To display information of error-disable recovery function, use the following command.

Command	Mode	Description
show errdisable recovery	Bridge	Shows information of error-disable recovery function.

8.3.14 Sample Configuration

Backup Route

When you design layer 2 network, you must consider backup route for stable STP network. This is to prevent network corruption when just one additional path exits.

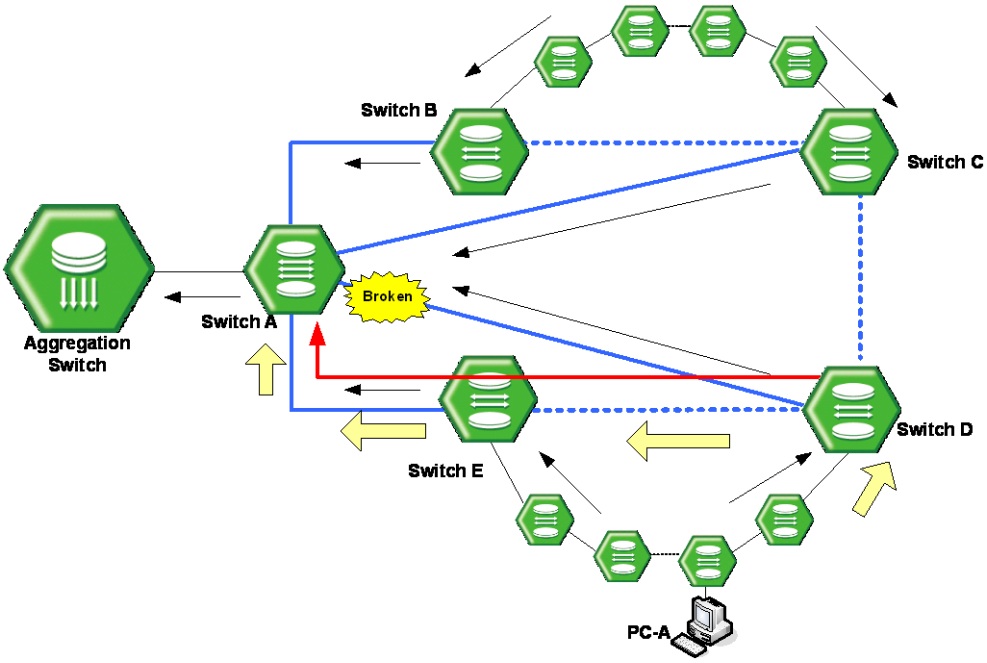


Fig. 8.27 Example of Layer 2 Network Design in RSTP Environment

In ordinary case, data packets go to Root switch A through the blue path. The black arrows describe the routine path to the Aggregation Switch. And the dot lines are in blocking state. But if there is a broken between Switch A and Switch B, the data from PC-A should find another route at Switch D. Switch D can send the data to Switch C and Switch E. Because Switch E has shorter hop count than Switch B, the data may go through the Switch E and A as the red line. And we can assume Switch E is also failed at the same time. In this case, since Switch D can has the other route to Switch C, the network can be stable than just one backup route network.

MSTP Configuration

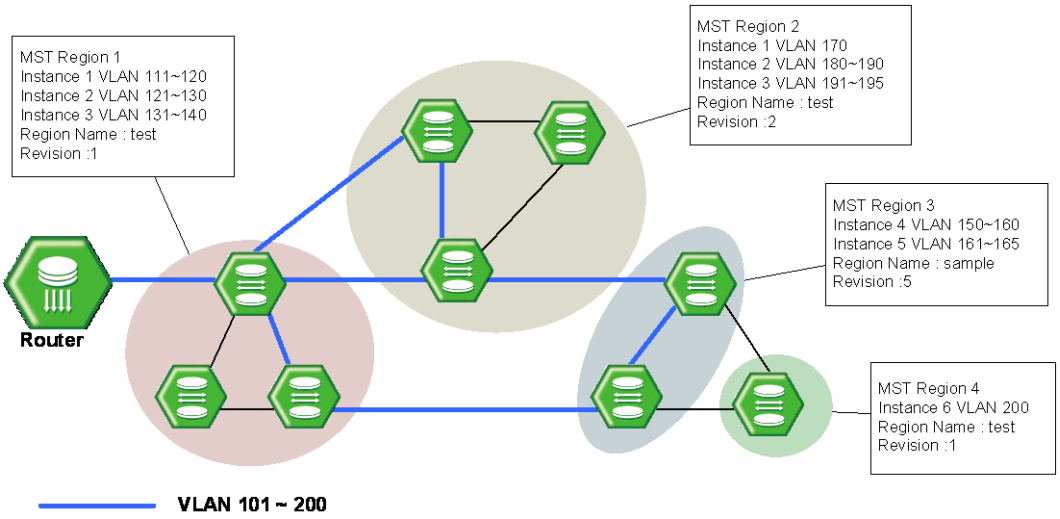


Fig. 8.28 Example of Layer 2 Network Design in MSTP Environment

The following is an example of configuring MSTP in the switch.

```
SWITCH(bridge)# spanning-tree
SWITCH(bridge)# spanning-tree mode mst
SWITCH(bridge)# spanning-tree mst configuration
SWITCH(config-mst)# instance 2 vlan 1-50
SWITCH(config-mst)# name test
SWITCH(config-mst)# revision 1
SWITCH(config-mst)# apply
SWITCH(config-mst)# exit
SWITCH(bridge)# show spanning-tree mst configuration

name                 test
revision             1
instance vlans
-------------------------------------------------------------------
CIST      51-4094
  2       1-50
-------------------------------------------------------------------
SWITCH(bridge)#
```

8.4 Loop Detection

The loop may occur when double paths are used for the link redundancy between switches and one sends unknown unicast or multicast packet that causes endless packet floating on the LAN like loop topology. That superfluous traffic eventually can result in

network fault. It causes superfluous data transmission and network fault.

To prevent this, the OLT provides the loop detecting function. The loop detecting mechanism is as follows:

The switch periodically sends the loop-detecting packet to all the ports with a certain interval, and then if receiving the loop-detecting packet sent before, the switch performs a pre-defined behavior.

To enable/disable the loop detection globally, use the following command.

Command	Mode	Description
loop-detect {**enable** | **disable**}	Bridge	Enables/disables the loop detection globally.

i For the detailed configuration of the loop detection, you need to issuing the **loop-detect enable** command first. If you do not, all the commands concerning the loop detection will show an error message.

To enable/disable the loop detection on a specified port, use the following command.

Command	Mode	Description
loop-detect *PORTS*	Bridge	Enables the loop detection on a specified port.
no loop-detect *PORTS*		Disables the loop detection on a specified port.

To define the behavior on a specified port when a loop is occurred, use the following command.

Command	Mode	Description
loop-detect *PORT* **block**	Bridge	Enables the blocking option. This configures a specified port to automatically change its state to BLOCKED when a loop is detected on it. (default: disable)
loop-detect *PORT* **unblock**		Forces the state of a blocked port to change to NORMAL.
loop-detect *PORT* **timer** <0-86400>		Sets the interval of changing the state of a blocked port to NORMAL. If you set the interval as 0, the state of the blocked port will not be changed automatically. (default: 600 seconds)
no loop-detect *PORT* **block**		Disables the blocking option.

To set the interval of sending the loop-detecting packet, use the following command.

Command	Mode	Description
loop-detect *PORTS* **period** <1-60>	Bridge	Sets the interval of sending the loop-detecting packet. (default: 30 seconds)

You can also configure the source MAC address of the loop-detecting packet. Normally the system's MAC address will be the source MAC address of the loop-detecting packet, but if needed, Locally Administered Address (LAA) can be the address as well.

If the switch is configured to use LAA as the source MAC address of the loop-detecting

packet, the second bit of first byte of the packet will be set to 1. For example, if the switch's MAC address is b8:26:d4:00:00:01, the source MAC address will be changed to ba:26:d4 :00:00:01.

To select the source MAC address type of the loop-detecting packet, use the following command.

Command	Mode	Description
loop-detect srcmac laa	Bridge	Uses LAA as the source MAC address of the loop-detecting packet.
loop-detect srcmac system		Uses the system's MAC address as the source MAC address of the loop-detecting packet. (default)

If you would like to change the source MAC address of the loop-detecting packet, you should disable the loop detection first using the **loop-detect disable** command.

To display a current configuration of the loop detection, use the following command.

Command	Mode	Description
show loop-detect	Enable Global Bridge	Shows the brief information of the loop detection.
show loop-detect {**all** | *PORTS*}		Shows a current configuration of the loop detection per port.

The loop detection cannot operate with LACP.

8.5 Dynamic Host Configuration Protocol (DHCP)

Dynamic Host Configuration Protocol (DHCP) is a TCP/IP standard for simplifying the administrative management of IP address configuration by automating address configuration for network clients. The DHCP standard provides for the use of DHCP servers as a way to manage dynamic allocation of IP addresses and other relevant configuration details to DHCP-enabled clients on the network.

Every device on a TCP/IP network must have a unique IP address in order to access the network and its resources. The IP address (together with its relevant subnet mask) identifies both the host computer and the subnet to which it is attached. When you move a computer to a different subnet, the IP address must be changed. DHCP allows you to dynamically assign an IP address to a client from a DHCP server IP address database on the local network.

The DHCP provides the following benefits:

Saving Cost

Numerous users can access the IP network with a small amount of IP resources in the environment that most users do not have to access the IP network at the same time all day long. This allows the network administrators to save the cost and IP resources.

Efficient IP Management

By deploying DHCP in a network, this entire process is automated and centrally managed. The DHCP server maintains a pool of IP addresses and leases an address to any DHCP-enabled client when it logs on to the network. Because the IP addresses are dynamic (leased) rather than static (permanently assigned), addresses no longer in use are automatically returned to the pool for reallocation.

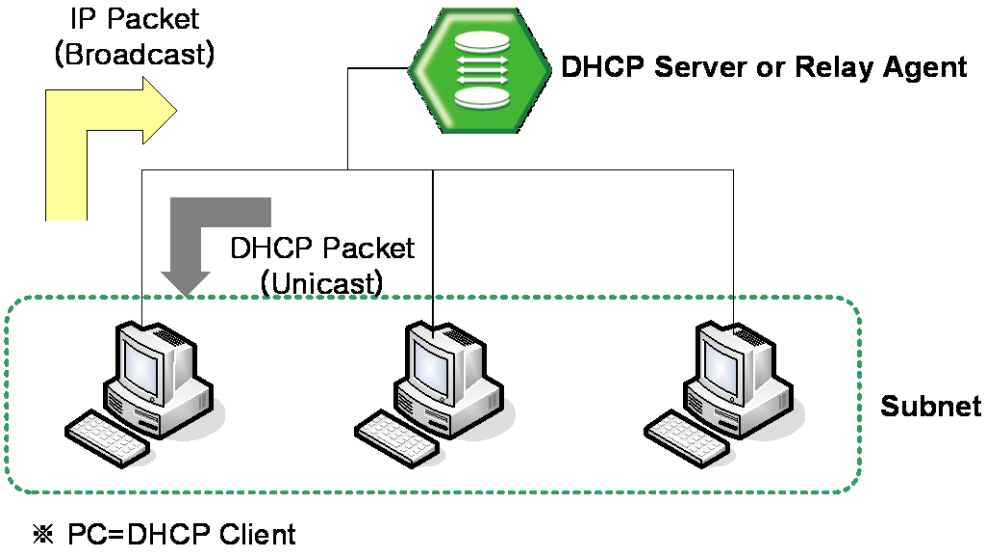


Fig. 8.29 DHCP Service Structure

The OLT flexibly provides the functions as the DHCP server or DHCP relay agent according to your DHCP configuration.

This chapter contains the following sections:

- DHCP Server
- DHCP Address Allocation with Option 82
- DHCP Lease Database
- DHCP Relay Agent
- DHCP Option 82
- DHCP Snooping
- IP Source Guard
- DHCP Client
- DHCP Filtering
- Debugging DHCP

8.5.1 DHCP Server

This section describes the following DHCP server-related features and configurations:

- DHCP Pool Creation
- DHCP Subnet
- Range of IP Address
- Default Gateway
- IP Lease Time
- DNS Server
- Manual Binding
- Domain Name
- DHCP Server Option
- Static Mapping
- Recognition of DHCP Client
- IP Address Validation
- Authorized ARP
- Prohibition of 1:N IP Address Assignment
- Ignoring BOOTP Request
- DHCP Packet Statistics
- Displaying DHCP Pool Configuration

To activate/deactivate the DHCP function in the system, use the following command.

Command	Mode	Description
service dhcp	Global	Activates the DHCP function in the system.
no service dhcp		Deactivates the DHCP function in the system.

i

Before configuring DHCP server or relay, you need to use the **service dhcp** command first to activate the DHCP function in the system.

8.5.1.1 DHCP Pool Creation

The DHCP pool is a group of IP addresses that will be assigned to DHCP clients by DHCP server. You can create various DHCP pools that can be configured with a different network, default gateway and range of IP addresses. This allows the network administrators to effectively handle multiple DHCP environments.

To create a DHCP pool, use the following command.

Command	Mode	Description
ip dhcp pool *POOL*	Global	Creates a DHCP pool and opens *DHCP Pool Configuration* mode.
no ip dhcp pool *POOL*		Deletes a created DHCP pool.

The following is an example of creating the DHCP pool as *sample*.

```
SWITCH(config)# service dhcp
SWITCH(config)# ip dhcp pool sample
SWITCH(config-dhcp[sample])#
```

8.5.1.2 DHCP Subnet

To specify a subnet of the DHCP pool, use the following command.

Command	Mode	Description
network *A.B.C.D/M*	DHCP Pool	Specifies a subnet of the DHCP pool. A.B.C.D/M: network address
no network *A.B.C.D/M*		Deletes a specified subnet.

The following is an example of specifying the subnet as 100.1.1.0/24.

```
SWITCH(config)# service dhcp
SWITCH(config)# ip dhcp pool sample
SWITCH(config-dhcp[sample])# network 100.1.1.0/24
SWITCH(config-dhcp[sample])#
```

i You can also specify several subnets in a single DHCP pool.

8.5.1.3 Range of IP Address

To specify a range of IP addresses that will be assigned to DHCP clients, use the following command.

Command	Mode	Description
range *A.B.C.D A.B.C.D*	DHCP Pool	Specifies a range of IP addresses. A.B.C.D: start/end IP address
no range *A.B.C.D A.B.C.D*		Deletes a specified range of IP addresses.

The following is an example for specifying the range of IP addresses.

```
SWITCH(config)# service dhcp
SWITCH(config)# ip dhcp pool sample
SWITCH(config-dhcp[sample])# network 100.1.1.0/24
SWITCH(config-dhcp[sample])# default-router 100.1.1.254
SWITCH(config-dhcp[sample])# range 100.1.1.1 100.1.1.100
SWITCH(config-dhcp[sample])#
```

i You can also specify several inconsecutive ranges of IP addresses in a single DHCP pool, e.g. 100.1.1.1 to 100.1.1.62 and 100.1.1.129 to 100.1.1.190.

! When specifying a range of IP address, the start IP address must be prior to the end IP address.

8.5.1.4 Default Gateway

To specify a default gateway of the DHCP pool, use the following command.

Command	Mode	Description
default-router *A.B.C.D1* [*A.B.C.D2*] … [*A.B.C.D8*]	DHCP Pool	Specifies a default gateway of the DHCP pool. A.B.C.D: default gateway IP address
no default-router *A.B.C.D1* [*A.B.C.D2*] … [*A.B.C.D8*]		Deletes a specified default gateway.
no default-router all		Deletes all the specified default gateways.

The following is an example of specifying the default gateway 100.1.1.254.

```
SWITCH(config)# service dhcp
SWITCH(config)# ip dhcp pool sample
SWITCH(config-dhcp[sample])# network 100.1.1.0/24
SWITCH(config-dhcp[sample])# default-router 100.1.1.254
SWITCH(config-dhcp[sample])#
```

8.5.1.5 IP Lease Time

Basically, the DHCP server leases an IP address in the DHCP pool to DHCP clients, which will be automatically returned to the DHCP pool when it is no longer in use or expired by IP lease time.

To specify IP lease time, use the following command.

Command	Mode	Description
lease-time default <120-2147483637>	DHCP Pool	Sets default IP lease time in the unit of second. (default: 3600)
lease-time max <120-2147483637>		Sets maximum IP lease time in the unit of second. (default: 3600)
no lease-time {**default** | **max**}		Deletes specified IP lease time.

The following is an example of setting default and maximum IP lease time.

```
SWITCH(config)# service dhcp
SWITCH(config)# ip dhcp pool sample
SWITCH(config-dhcp[sample])# network 100.1.1.0/24
SWITCH(config-dhcp[sample])# default-router 100.1.1.254
SWITCH(config-dhcp[sample])# range 100.1.1.1 100.1.1.100
SWITCH(config-dhcp[sample])# lease-time default 5000
SWITCH(config-dhcp[sample])# lease-time max 10000
SWITCH(config-dhcp[sample])#
```

8.5.1.6 DNS Server

To specify a DNS server to inform DHCP clients, use the following command.

Command	Mode	Description
dns-server *A.B.C.D1* [*A.B.C.D2*] … [*A.B.C.D8*]	DHCP Pool	Specifies a DNS server. Up to 8 DNS servers are possible. A.B.C.D: DNS server IP address
no dns-server *A.B.C.D1* [*A.B.C.D2*] … [*A.B.C.D8*]		Deletes a specified DNS server.
no dns-server all		Deletes all the specified DNS servers.

The following is an example of specifying a DNS server.

```
SWITCH(config)# service dhcp
SWITCH(config)# ip dhcp pool sample
SWITCH(config-dhcp[sample])# network 100.1.1.0/24
SWITCH(config-dhcp[sample])# default-router 100.1.1.254
SWITCH(config-dhcp[sample])# range 100.1.1.1 100.1.1.100
SWITCH(config-dhcp[sample])# lease-time default 5000
SWITCH(config-dhcp[sample])# lease-time max 10000
SWITCH(config-dhcp[sample])# dns-server 200.1.1.1 200.1.1.2 200.1.1.3
SWITCH(config-dhcp[sample])#
```

i If you want to specify a DNS server for all the DHCP pools, use the **dns server** command. For more information, see Section 6.1.8.

8.5.1.7 Manual Binding

To manually assign a static IP address to a DHCP client who has a specified MAC address, use the following command.

Command	Mode	Description
fixed-address *A.B.C.D* *MAC-ADDR*	DHCP Pool	Assigns a static IP address to a DHCP client. A.B.C.D: static IP address MAC-ADDR: MAC address
no fixed-address *A.B.C.D*		Deletes a specified static IP assignment.

8.5.1.8 Domain Name

To set a domain name, use the following command.

Command	Mode	Description
domain-name *DOMAIN*	DHCP Pool	Sets a domain name.
no domain-name		Deletes a specified domain name.

8.5.1.9 DHCP Server Option

The switch operating DHCP server can include DHCP option information in the DHCP communication. Before using this function, a global DHCP option format should be created. For details of setting the DHCP option format, refer to the 8.5.5 DHCP Option.

To specify a DHCP server option, use the following command.

Command	Mode	Description
option code <1-254> **format** *NAME*	DHCP Pool	Specifies a DHCP option format for a DHCP server. code: DHCP option code NAME: DHCP option format name
no option code <1-254> **format**		Removes a specified DHCP option for a DHCP server.

DHCP server may not have any DHCP option that is configured in the DHCP pool mode. Then DHCP server finds the DHCP default option. If it exists, DHCP server sends DHCP clients a DHCP reply packet (Offer/ACK) with the default option information.

To specify a DHCP server default option, use the following command.

Command	Mode	Description
ip dhcp default-option code <1-254> **format** *NAME*	Global	Specifies a DHCP default option format for a DHCP server. code: DHCP option code NAME: DHCP option format name
no ip dhcp default-option code <1-254>		Removes a specified DHCP default option for a DHCP server.

8.5.1.10 Static Mapping

The OLT provides a static mapping function that enables to assign a static IP address without manually specifying static IP assignment by using a DHCP lease database in the DHCP database agent.

To perform a static mapping, use the following command.

Command	Mode	Description
origin file *A.B.C.D FILE*	DHCP Pool	Performs a static mapping. A.B.C.D: DHCP database agent address FILE: file name of DHCP lease database
no origin file		Cancels a static mapping.

i For more information of the file naming of a DHCP lease database, see Section 8.5.3.1.

8.5.1.11 Recognition of DHCP Client

Normally, a DHCP server is supposed to prohibit assigning an IP address when DHCP packets have no client ID (CID). However, some Linux clients may send DHCP discover messages without CID. To solve such a problem, the switch provides the additional option to verify a hardware address (MAC address) instead of CID.

To select a recognition method of DHCP clients, use the following command.

Command	Mode	Description
ip dhcp database-key {**client-id** | **hardware-address**}	Global	Selects a recognition method of DHCP clients

8.5.1.12 IP Address Validation

Before assigning an IP address to a DHCP client, a DHCP server will validate if the IP address is used by another DHCP client with a ping or ARP. If the IP address does not respond to a requested ping or ARP, the DHCP server will realize that the IP address is not used then will assign the IP address to the DHCP client.

To select an IP address validation method, use the following command.

Command	Mode	Description
ip dhcp validate {**arp** | **ping**}	Global	Selects an IP address validation method.

You can also set a validation value of how many responses and how long waiting (timeout) for the responses from an IP address for a requested ping or ARP when a DHCP server validates an IP address.

To set a validation value of how many responses from an IP address for a requested ping or ARP, use the following command.

Command	Mode	Description
ip dhcp {**arp** | **ping**} **packet** <0-20>	Global	Sets a validation value of how many responses. 0-20: response value (default: 2)

To set a validation value of timeout for the responses from an IP address for a requested ping or ARP, use the following command.

Command	Mode	Description
ip dhcp {**arp** | **ping**} **timeout** <100-5000>	Global	Sets a validation value of timeout for the responses in the unit of millisecond. 100-5000: timeout value (default: 500)

8.5.1.13 Authorized ARP

The authorized ARP is to limit the lease of IP addresses to authorized users. This feature

enables a DHCP server to add ARP entries only for the IP addresses currently in lease referring to a DHCP lease table, discarding ARP responses from unauthorized users (e.g. an illegal use of a static IP address).

When this feature is running, dynamic ARP learning on an interface will be disabled, since DHCP is the only authorized component currently allowed to add ARP entries.

The authorized ARP is enabled only in a DHCP server.

To limit the lease of IP addresses to authorized users, use the following command.

Command	Mode	Description
ip dhcp authorized-arp start <120-2147483637> **timeout** <120-2147483637>	Global	Discards an ARP response from unauthorized user. start: starting time (default: 3600 sec) timeout: expire time
ip dhcp authorized-arp <120-2147483637>		Discards an ARP response from unauthorized user. 120-2147483637: expire time
no ip dhcp authorized-arp		Disables the authorized ARP function.

You can verify the valid and invalid list for the authorized ARP. The valid list includes the IP addresses currently in lease, while the invalid list includes the IP addresses that send ARP requests, but not in lease. Both lists include IP addresses of a DHCP pool, but the authorized ARP only allows the ARP response of the IP addresses in the valid list.

To display entries of the valid and invalid lists, use the following command.

Command	Mode	Description
show ip dhcp authorized-arp valid	Enable Global Bridge	Shows entries of the valid list.
show ip dhcp authorized-arp invalid		Shows entries of the invalid list.

To delete entries of the invalid list, use the following command.

Command	Mode	Description
clear ip dhcp authorized-arp invalid	Enable Global Bridge	Deletes entries of the invalid IP addresses.

8.5.1.14 Prohibition of 1:N IP Address Assignment

The DHCP server may assign plural IP addresses to a single DHCP client in case of plural DHCP requests from the DHCP client, which has the same hardware address. Some network devices may need plural IP addresses, but most DHCP clients like personal computers need only a single IP address. In this case, you can configure the OLT to prohibit assigning plural IP addresses to a single DHCP client.

To prohibit assigning plural IP addresses to a DHCP client, use the following command.

Command	Mode	Description
ip dhcp check client-hardware-address	Global	Prohibits assigning plural IP addresses.
no ip dhcp check client-hardware-address		Permits assigning plural IP addresses.

8.5.1.15 Ignoring BOOTP Request

To allow a DHCP server to ignore received bootstrap protocol (BOOTP) request packets, use the following command.

Command	Mode	Description
ip dhcp bootp ignore	Global	Ignores BOOTP request packets.
no ip dhcp bootp ignore		Permits BOOTP request packets.

8.5.1.16 DHCP Packet Statistics

To display DHCP packet statistics of the DHCP server, use the following command.

Command	Mode	Description
show ip dhcp server statistics	Enable Global Bridge	Shows DHCP packet statistics.
clear ip dhcp statistics		Deletes collected DHCP packet statistics.

The following is an example of displaying DHCP packet statistics.

```
SWITCH(config)# show ip dhcp server statistics

 ==========================================
 Message              Recieved/Error(0/0)
 ------------------------------------------
 DHCP DISCOVER                0
 DHCP REQUEST                 0
 DHCP DECLINE                 0
 DHCP RELEASE                 0
 DHCP INFORM                  0

 =========================================
 Message              Sent/Error(0/0)
 -----------------------------------------
 DHCP OFFER                   0
 DHCP ACK                     0
 DHCP NAK                     0

SWITCH(config)#
```

8.5.1.17 Setting DHCP Pool Size

To limit a size of DHCP pool, use the following command.

Command	Mode	Description
ip dhcp max-pool-size <1-12>	Global	Configures a maximum size of DHCP pool.

8.5.1.18 Displaying DHCP Pool Configuration

To display a DHCP pool configuration, use the following command.

Command	Mode	Description
show ip dhcp pool [*POOL*]	Enable Global Bridge	Shows a DHCP pool configuration.
show ip dhcp pool summary [*POOL*]		Shows a summary of a DHCP pool configuration. POOL: pool name

The following is an example of displaying a DHCP pool configuration.

```
SWITCH(config)# show ip dhcp pool summary
[Total -- 1 Pools]
 Total      0                                0.00 of total
 Available  0                                0.00 of total
 Abandon    0                                0.00 of total
 Bound      0                                0.00 of total
 Offered    0                                0.00 of total
 Fixed      0                                0.00 of total

[sample]

 Total      0            0.00% of the pool    0.00 of total
 Available  0            0.00% of the pool    0.00 of total
 Abandon    0            0.00% of the pool    0.00 of total
 Bound      0            0.00% of the pool    0.00 of total
 Offered    0            0.00% of the pool    0.00 of total
 Fixed      0            0.00% of the pool    0.00 of total

SWITCH(config)#
```

8.5.2 DHCP Address Allocation with Option 82

The DHCP server provided by the OLT can assign dynamic IP addresses based on DHCP option 82 information sent by the DHCP relay agent.

The information sent via DHCP option 82 will be used to identify which port the DHCP_REQUEST came in on. The feature introduces a new DHCP class capability, which is a method to group DHCP clients based on some shared characteristics other than the subnet in which the clients reside. The DHCP class can be configured with option 82 information and a range of IP addresses.

8.5.2.1 DHCP Class Capability

To enable the DHCP server to use a DHCP class to assign IP addresses, use the following command.

Command	Mode	Description
ip dhcp use class	Global	Enables the DHCP server to use a DHCP class to assign IP addresses.
no ip dhcp use class		Disables the DHCP server to use a DHCP class.

8.5.2.2 DHCP Class Creation

To create a DHCP class, use the following command.

Command	Mode	Description
ip dhcp class *CLASS*	Global	Creates a DHCP class and opens *DHCP Class Configuration* mode. CLASS: DHCP class name
no ip dhcp class [*CLASS*]		Deletes a created DHCP class.

8.5.2.3 Relay Agent Information Pattern

To specify option 82 information for IP assignment, use the following command.

Command	Mode	Description
relay-information remote-id ip *A.B.C.D* [**circuit-id** {**hex** *HEXSTRING* | **index** <0-65535> | **text** *STRING*}]	DHCP Class	Specifies option 82 information for IP assignment.
relay-information remote-id hex *HEXSTRING* [**circuit-id** {**hex** *HEXSTRING* | **index** <0-65535> | **text** *STRING*}]		
relay-information remote-id text *STRING* [**circuit-id** {**hex** *HEXSTRING* | **index** <0-65535> | **text** *STRING*}]		

To delete specified option 82 information for IP assignment, use the following command.

Command	Mode	Description
no relay-information remote-id ip *A.B.C.D* [**circuit-id** {**hex** *HEXSTRING* | **index** <0-65535> | **text** *STRING*}]	DHCP Class	Deletes specified option 82 information for IP assignment.
no relay-information remote-id hex *HEXSTRING* [**circuit-id** {**hex** *HEXSTRING* | **index** <0-65535> | **text** *STRING*}]		
no relay-information remote-id text *STRING* [**circuit-id** {**hex** *HEXSTRING* | **index** <0-65535> | **text** *STRING*}]		

To delete specified option 82 information for IP assignment, use the following command.

Command	Mode	Description
no relay-information remote-id all	DHCP Class	Deletes all specified option 82 information that contains only a remote ID.
no relay-information all		Deletes all specified option 82 information.

8.5.2.4 Associating DHCP Class

To associate a DHCP class with a current DHCP pool, use the following command.

Command	Mode	Description
class *CLASS*	DHCP Pool	Associates a DHCP class with a DHCP pool and opens *DHCP Pool Class Configuration* mode. CLASS: DHCP class name
no class [*CLASS*]		Releases an associated DHCP class from a current DHCP pool.

8.5.2.5 Range of IP Address for DHCP Class

To specify a range of IP addresses for a DHCP class, use the following command.

Command	Mode	Description
address range *A.B.C.D A.B.C.D*	DHCP Pool Class	Specifies a range of IP addresses. A.B.C.D: start/end IP address
no address range *A.B.C.D A.B.C.D*		Deletes a specified range of IP addresses.

A range of IP addresses specified with the **address range** command is valid only for a current DHCP pool. Even if you associate the DHCP class with another DHCP pool, the specified range of IP addresses will not be applicable.

8.5.3 DHCP Lease Database

8.5.3.1 DHCP Database Agent

The OLT provides a feature that allows to a DHCP server automatically saves a DHCP lease database on a DHCP database agent.

The DHCP database agent should be a TFTP server, which stores a DHCP lease database as numerous files in the form of **leasedb.***MAC-ADDRESS*, e.g. **leasedb.***0A:31:4B:1A:77:6A*. The DHCP lease database contains a leased IP address, hardware address, etc.

To specify a DHCP database agent and enable an automatic DHCP lease database back-up, use the following command.

Command	Mode	Description
ip dhcp database *A.B.C.D INTERVAL*	Global	Specifies a DHCP database agent and back-up interval. A.B.C.D: DHCP database agent address INTERVAL: 120-2147483637 (unit: second)
no ip dhcp database		Deletes a specified DHCP database agent.

i Upon entering the **ip dhcp database** command, the back-up interval will begin.

To display a configuration of the DHCP database agent, use the following command.

Command	Mode	Description
show ip dhcp database	Enable Global Bridge	Shows a configuration of the DHCP database agent.

8.5.3.2 Displaying DHCP Lease Status

To display current DHCP lease status, use the following command.

Command	Mode	Description
show ip dhcp lease {**all** | **bound** | **abandon** | **offer** | **fixed** | **free**} [*POOL*]	Enable Global Bridge	Shows current DHCP lease status. all: all IP addresses bound: assigned IP address abandon: illegally assigned IP address offer: IP address being ready to be assigned fixed: manually assigned IP address free: remaining IP address POOL: pool name
show ip dhcp lease detail [*A.B.C.D*]		

8.5.3.3 Deleting DHCP Lease Database

To delete a DHCP lease database, use the following command.

Command	Mode	Description
clear ip dhcp leasedb *A.B.C.D/M*	Enable Global	Deletes a DHCP lease database a specified subnet.
clear ip dhcp leasedb pool *POOL*		Deletes a DHCP lease database of a specified DHCP pool.
clear ip dhcp leasedb all		Deletes the entire DHCP lease database.

8.5.4 DHCP Relay Agent

A DHCP relay agent is any host that forwards DHCP packets between clients and servers. The DHCP relay agents are used to forward DHCP requests and replies between clients

and servers when they are not on the same physical subnet. The DHCP relay agent forwarding is distinct from the normal forwarding of an IP router, where IP datagrams are switched between networks somewhat transparently.

By contrast, DHCP relay agents receive DHCP messages and then generate a new DHCP message to send out on another interface. The DHCP relay agent sets the gateway address and, if configured, adds the DHCP option 82 information in the packet and forwards it to the DHCP server. The reply from the server is forwarded back to the client after removing the DHCP option 82 information.

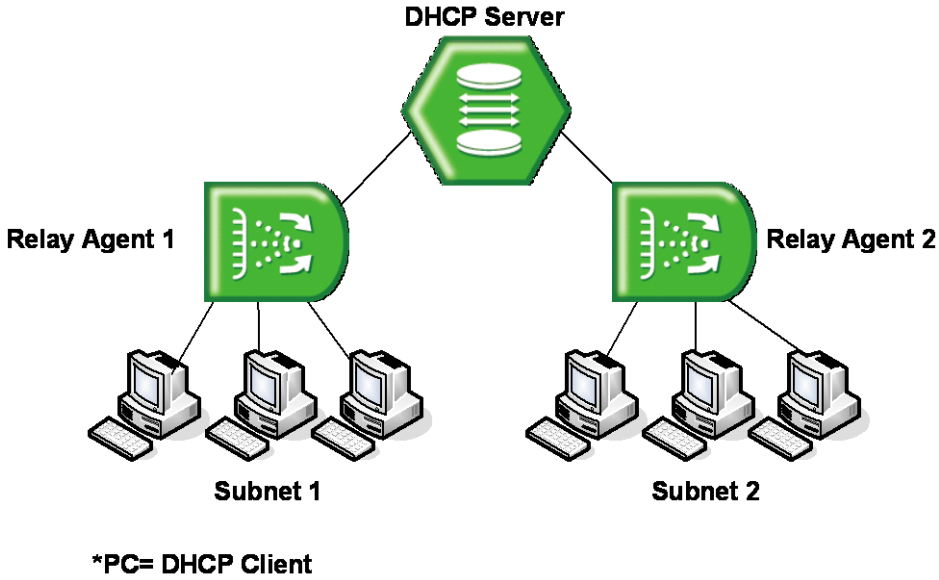


Fig. 8.30 Example of DHCP Relay Agent

To activate/deactivate the DHCP function in the system, use the following command.

Command	Mode	Description
service dhcp	Global	Activates the DHCP function in the system.
no service dhcp		Deactivates the DHCP function in the system.

i Before configuring DHCP server or relay, you need to use the **service dhcp** command first to activate the DHCP function in the system.

8.5.4.1 DHCP Helper Address

A DHCP client sends DHCP_DISCOVER message to a DHCP server. DHCP_DISCOVER message is broadcasted within the network to which it is attached. If the client is on a network that does not have any DHCP server, the broadcast is not forwarded because the switch is configured to not forward broadcast traffic. To solve this problem, you can configure the interface that is receiving the broadcasts to forward certain classes of broadcast to a helper address.

To specify a DHCP helper address, use the following command.

Command	Mode	Description
ip dhcp helper-address *A.B.C.D*	Interface	Specifies a DHCP helper address. More than one address is possible. A.B.C.D: DHCP server address
no ip dhcp helper-address {*A.B.C.D* | **all**}		Deletes a specified packet forwarding address.

i

If a DHCP helper address is specified on an interface, the OLT will enable a DHCP relay agent.

You can also specify an organizationally unique identifier (OUI) when configuring a DHCP helper address. The OUI is a 24-bit number assigned to a company or organization for use in various network hardware products, which is a first 24 bits of a MAC address. If an OUI is specified, a DHCP relay agent will forward DHCP_DISCOVER message to a specific DHCP server according to a specified OUI.

To specify a DHCP helper address with an OUI, use the following command.

Command	Mode	Description
ip dhcp oui *XX:XX:XX* **helper-address** *A.B.C.D*	Interface	Specifies a DHCP helper address with an OUI. More than one address is possible. XX:XX:XX: OUI (first 24 bits of a MAC address in the form of hexadecimal) A.B.C.D: DHCP server address
no ip dhcp oui *XX:XX:XX* [**helper-address** *A.B.C.D*]		Deletes a specified DHCP helper address.

8.5.4.2 Smart Relay Agent Forwarding

Normally, a DHCP relay agent forwards DHCP_DISCOVER message to a DHCP server only with a primary IP address on an interface, even if there is more than one IP address on the interface.

If the smart relay agent forwarding is enabled, a DHCP relay agent will retry sending DHCP_DISCOVER message with a secondary IP address, in case of no response from the DHCP server.

To enable the smart relay agent forwarding, use the following command.

Command	Mode	Description
ip dhcp smart-relay	Global	Enables a smart relay.
no ip dhcp smart-relay		Disables a smart relay.

8.5.4.3 DHCP Server ID Option

In case that more than two DHCP servers are connected to one DHCP relay agent, if the relay agent is supposed to broadcast the DHCP_DISCOVER message sent from a DHCP client to all connected DHCP servers, and then the servers will return DHCP_OFFER

message. The relay agent, however, will forward only one DHCP_OFFER message of the responses from the servers to the DHCP client. The DHCP client will try to respond to the server which sent the DHCP_OFFER with DHCP_REQUEST message, but the relay agent broadcasts it to all the DHCP servers again.

To prevent the unnecessary broadcast like this, you can configure a DHCP relay agent to aware the server ID. This will allow the DHCP relay agent to forward DHCP_REQUEST message to only one DHCP server with the unicast form under the multiple server environment.

To enable/disable a DHCP relay agent to recognize the DHCP server ID option in the forwarded DHCP_REQUEST message, use the following command.

Command	Mode	Description
ip dhcp relay aware-server-id	Global	Enables the system to recognize the DHCP server ID in the DHCP_REQUEST message.
no ip dhcp relay aware-server-id		Disables the DHCP server ID recognition option.

8.5.4.4 DHCP Relay Statistics

To display DHCP relay statistics, use the following command.

Command	Mode	Description
show ip dhcp relay [**statistics all**]	Enable Global Bridge	Shows DHCP relay statistics for all the interfaces.
show ip dhcp relay statistics vlan *VLANS*		Shows DHCP relay statistics for a specified VLAN.

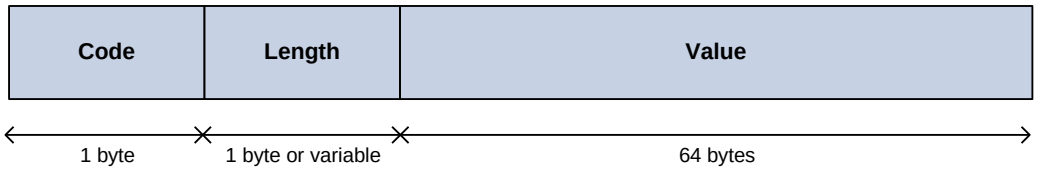
To delete collected DHCP relay statistics, use the following command.

Command	Mode	Description
clear ip dhcp relay statistics	Enable Global Bridge	Deletes collected DHCP relay statistics.

8.5.5 DHCP Option

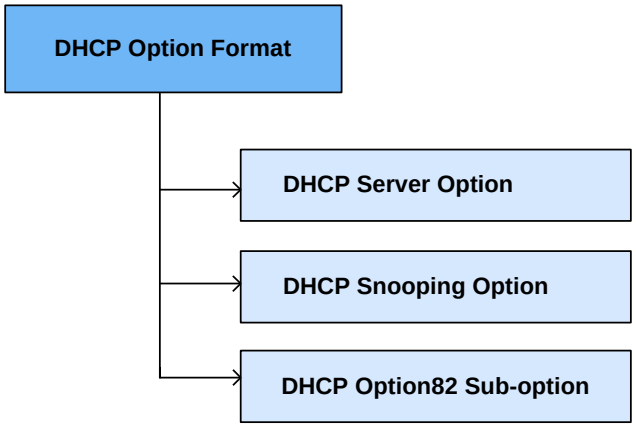
This function enables administrators to define DHCP options that are carried in the DHCP communication between DHCP server and client or relay agent. The following indicates the format of the DHCP options field.

DHCP Option Format



A code identifies each DHCP option. It can be expressed in value 0 to 255 by user configuration and some of them are predefined in the standards. (128 ~ 254 is site specific) A length can be variable according to value or can be fixed. A value contains actual information such an IP address, string, or index, which is inserted into the DHCP packet.

Administrators can configure a DHCP option format in *DHCP Option* mode, which is globally used over the DHCP functions. The DHCP option format can be applied in other DHCP software modules and the following figure indicates it.



8.5.5.1 Entering DHCP Option Mode

To enter the DHCP option mode, use the following command.

Command	Mode	Description
ip dhcp option format *NAME*	Global	Enters the DHCP option mode. NAME: DHCP option format name

8.5.5.2 Configuring DHCP Option Format

To configure a DHCP option format, use the following command.

Command	Mode	Description
attr <1-32> **type** <0-255> **length** {<1-64> | **variable**} **value** {**hex** | **index** | **ip** | **string**} *VALUE*	DHCP Option /Policy	Sets the type, length, and value of an attribute for a DHCP option. attr: They can be made in a DHCP option and are applied in order of attribute value (1-32). type: The type of a value length: The length of a value. It could be a fixed length by user input or a variable length according to the actual value length. 1-64: 1 to 64 bytes fixed length (size) of the value field value: The actual value of an option
attr <1-32> **type** <0-255> **length-hidden** {<1-64> | **variable**} **value** {**hex** | **index** | **ip** | **string**} *VALUE*		
attr <1-32> **length variable value** {**hex** | **index** | **ip** | **string**} *VALUE*		Sets the length and value of an attribute for a DHCP option.
attr <1-32> **length** <1-64> **value** {**hex** | **index** | **ip** | **string**} *VALUE*		
attr <1-32> **length-hidden variable value** {**hex** | **index** | **ip** | **string**} *VALUE*		Sets the value of an attribute for a DHCP option..
attr <1-32> **length-hidden** <1-64> **value** {**hex** | **index** | **ip** | **string**} *VALUE*		
no attr <1-32>	DHCP Option	Deletes the given attribute.

i

The packets can be mapped to the option format string that defined by variable values with special character (%).

%FRAME: frame (chassis) number for receiving DHCP packets
%SLOT: slot number for receiving DHCP packets
%PORT: port number
%IN_IF_IP: input interface IP address
%VID: VLAN ID tagged on packets
%CPU-MAC: system MAC address
%ONU-ID: ONU ID
%ONU_PORT_NUM: ONU's UNI port number
%ONU_SERIAL_NUM: ONU's serial number
%ONU_DESCRIPTION: ONU description written by administrator
%ONU_PORT_DESCRIPTION: ONU port description written by administrator

i

If the variable value of attribute is configured with %ONU-PORT_NUM, a GPON MAC bridge service profile should be used to one single UNI port. If there are more than two UNI ports for one Bridge service profile, DHCP option 82 can not add/classify the ONU UNI port number information into DHCP option field.
The DHCP option format has the following restrictions;
- The length of attribute should be within 64 bytes.
- A hidden-length variable of attribute should be set once in a single attribute.

- The total length of an option format cannot exceed 254 bytes.

8.5.5.3 Deleting DHCP Option Format

To delete a specified DHCP option format, use the following command.

Command	Mode	Description
no ip dhcp option format *NAME*	Global	Deletes the given DHCP option format.

8.5.5.4 Displaying DHCP option

To print a specified DHCP option format, use the following command.

Command	Mode	Description
show ip dhcp option format *NAME* [**port** *PORTS* **vlan** *VLANS*]	Enable Global DHCP Option	Prints the given option format and actual raw data in the packet.

8.5.5.5 Different DHCP option Code Configurations

[DHCP Option 66]

When the DHCP server gives the information of TFTP boot server to DHCP client, DHCP option code is 66. This option is used to identify a TFTP server when the 'sname' field in the DHCP header has been used for DHCP options.

The following is an example of configuring IP address or domain name for TFTP server using DHCP option 66.

```
SWITCH(config)# ip dhcp option format OPTION66_1
SWITCH(dhcp-opt[OPTION66_1])# attr 1 length-hidden variable value ip
10.60.250.16
SWITCH(dhcp-opt[OPTION66_1])# exit
SWITCH(config)# ip dhcp pool test

SWITCH(config-dhcp[test])# option code 66 format OPTION66_1


SWITCH(config)# ip dhcp option format OPTION66_2
SWITCH(dhcp-opt[OPTION66_2])# attr 1 length-hidden variable value
tftp.furukawa.com
SWITCH(dhcp-opt[OPTION66_2])# exit
SWITCH(config)# ip dhcp pool test
SWITCH(config-dhcp[test])# option code 66 format OPTION66_2
```

[DHCP Option 82]

The DHCP option 82 field's circuit-ID/remote-ID can be mapped to the option format defined by variable values with special character (%). The following is an example of configuring the switch running DHCP snooping with option 82.

```
SWITCH(config)# ip dhcp option format circuit
SWITCH(dhcp-opt[circuit])# attr 1 type 1 length variable value string %FRAME
SWITCH(dhcp-opt[circuit])# attr 2 type 2 length variable value string %SLOT
SWITCH(dhcp-opt[circuit])# attr 3 type 3 length variable value string %PORT
SWITCH(dhcp-opt[circuit])# attr 4 type 4 length variable value string %VID
SWITCH(dhcp-opt[circuit])# attr 5 length-hidden variable value string %ONU-ID
SWITCH(dhcp-opt[circuit])# attr 6 length-hidden variable value
string %ONU_PORT_NUM

SWITCH(dhcp-opt[circuit])# exit
SWITCH(config)#
SWITCH(config)# ip dhcp option format remote
SWITCH(dhcp-opt[remote])# attr 1 type 1 length variable value string %CPU-MAC
SWITCH(dhcp-opt[remote])# attr 2 type 2 length variable value string 10.1.1.1
SWITCH(dhcp-opt[remote])# exit
SWITCH(config)#
SWITCH(config)# ip dhcp option82
SWITCH(config-opt82)# system-remote-id option format remote
SWITCH(config-opt82)# system-circuit-id 1-4 option format circuit
SWITCH(config-opt82)# trust default permit
SWITCH(config-opt82)# exit

SWITCH(config)# gpon
SWITCH(gpon)# traffic-profile TEST create
SWITCH(config-traffic-pf[TEST])# mapper 1
SWITCH(config-traffic-pf[TEST]-mapper[1])# gemport count 1
SWITCH(config-traffic-pf[TEST]-mapper[1])# write memory
SWITCH(config-traffic-pf[TEST]-mapper[1])# exit
SWITCH(config-traffic-pf[TEST])# mapper 2
SWITCH(config-traffic-pf[TEST]-mapper[2])# gemport count 1
SWITCH(config-traffic-pf[TEST]-mapper[2])# write memory
SWITCH(config-traffic-pf[TEST]-mapper[2])# exit
SWITCH(config-traffic-pf[TEST])# bridge 1
SWITCH(config-traffic-pf[TEST]-bridge[1])# ani mapper 1
SWITCH(config-traffic-pf[TEST]-bridge[1]-ani[mapper:1])# vlan-filter vid
3500,3510 untagged allow
SWITCH(config-traffic-pf[TEST]-bridge[1]-ani[mapper:1])# write memory
SWITCH(config-traffic-pf[TEST]-bridge[1]-ani[mapper:1])# exit
SWITCH(config-traffic-pf[TEST]-bridge[1])# uni eth 1
SWITCH(config-traffic-pf[TEST]-bridge[1]-uni[eth:1])# multicast-profile
V3510_tag
SWITCH(config-traffic-pf[TEST]-bridge[1]-uni[eth:1])# extended-vlan-tagging-
operation HSI_1
SWITCH(config-traffic-pf[TEST]-bridge[1]-uni[eth:1])# write memory
SWITCH(config-traffic-pf[TEST]-bridge[1]-uni[eth:1])# exit
SWITCH(config-traffic-pf[TEST]-bridge[1])# exit
SWITCH(config-traffic-pf[TEST])# bridge 2
SWITCH(config-traffic-pf[TEST]-bridge[2])# ani mapper 2
SWITCH(config-traffic-pf[TEST]-bridge[2]-ani[mapper:2])# vlan-filter vid
3500,3510 untagged allow
SWITCH(config-traffic-pf[TEST]-bridge[2]-ani[mapper:2])# write memory
SWITCH(config-traffic-pf[TEST]-bridge[2]-ani[mapper:2])# exit
```

```
SWITCH(config-traffic-pf[TEST]-bridge[2])# uni eth 2
SWITCH(config-traffic-pf[TEST]-bridge[2]-uni[eth:2])#         multicast-profile
V3510_tag
SWITCH(config-traffic-pf[TEST]-bridge[2]-uni[eth:2])#    extended-vlan-tagging-
operation HSI_1
SWITCH(config-traffic-pf[TEST]-bridge[2]-uni[eth:2])# write memory
```

8.5.6 DHCP Option 82

In some networks, it is necessary to use additional information to further determine which IP addresses to allocate. By using the DHCP option 82, a DHCP relay agent can include additional information about itself when forwarding client-originated DHCP packets to a DHCP server. The DHCP relay agent will automatically add the circuit ID and the remote ID to the option 82 field in the DHCP packets and forward them to the DHCP server.

The DHCP option 82 resolves the following issues in an environment in which untrusted hosts access the internet via a circuit based public network:

Broadcast Forwarding

The DHCP option 82 allows a DHCP relay agent to reduce unnecessary broadcast flooding by forwarding the normally broadcasted DHCP response only on the circuit indicated in the circuit ID.

DHCP Address Exhaustion

In general, a DHCP server may be extended to maintain a DHCP lease database with an IP address, hardware address and remote ID. The DHCP server should implement policies that restrict the number of IP addresses to be assigned to a single remote ID.

Static Assignment

A DHCP server may use the remote ID to select the IP address to be assigned. It may permit static assignment of IP addresses to particular remote IDs, and disallow an address request from an unauthorized remote ID.

IP Spoofing

A DHCP client may associate the IP address assigned by a DHCP server in a forwarded DHCP_ACK message with the circuit to which it was forwarded. The circuit access device may prevent forwarding of IP packets with source IP addresses, other than, those it has associated with the receiving circuit. This prevents simple IP spoofing attacks on the central LAN, and IP spoofing of other hosts.

MAC Address Spoofing

By associating a MAC address with a remote ID, a DHCP server can prevent offering an IP address to an attacker spoofing the same MAC address on a different remote ID.
Client Identifier Spoofing

By using the agent-supplied remote ID option, the untrusted and as-yet unstandardized client identifier field need not be used by the DHCP server.

Fig. 8.31 shows how the DHCP relay agent with the DHCP option 82 operates.

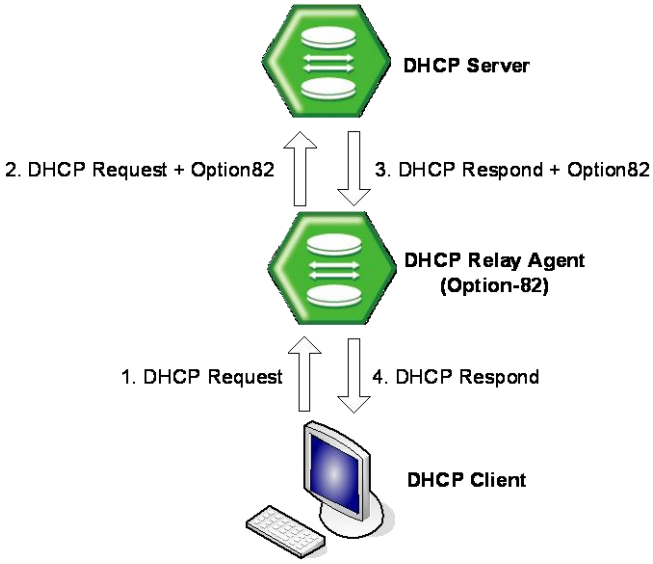


Fig. 8.31 DHCP Option 82 Operation

8.5.6.1 Enabling DHCP Option 82

To enable/disable the DHCP option 82, use the following command.

Command	Mode	Description
ip dhcp option82	Global	Enables the system to add the DHCP option 82 field.
no ip dhcp option82		Disables the system to add the DHCP option 82 field.

8.5.6.2 Option 82 Sub-Option

The DHCP option 82 enables a DHCP relay agent to include information about itself when forwarding client-originated DHCP packets to a DHCP server. The DHCP server can use this information to implement security and IP address assignment policies.

There are 2 sub-options for the DHCP option 82 information as follows:

- **Remote ID**
  This sub-option may be added by DHCP relay agents which terminate switched or permanent circuits and have mechanisms to identify the remote host of the circuit. Note that, the remote ID must be globally unique.
- **Circuit ID**
  This sub-option may be added by DHCP relay agents which terminate switched or permanent circuits. It encodes an agent-local identifier of the circuit from which a DHCP client-to-server packet was received. It is intended for use by DHCP relay agents in forwarding DHCP responses back to the proper circuit.

To specify a remote ID, use the following command.

Command	Mode	Description
system-remote-id hex *HEXSTRING*	Option 82	Specifies a remote ID. (default: system MAC address)
system-remote-id ip *A.B.C.D*		
system-remote-id text *STRING*		
system-remote-id option format *NAME*		

Because the **remote-id** option is applied to the system, the option format of variable values with GPON-related attributes (%ONU_PORT_NUM, %ONU_ID, %ONU_PORT_DESCRIPTION, etc.) SHOULD not be used for the **remote-id** in DHCP option 82 field.

To specify a circuit ID, use the following command.

Command	Mode	Description
system-circuit-id *PORTS* **hex** *HEXSTRING*	Option 82	Specifies a circuit ID. (default: port number)
system-circuit-id *PORTS* **index** <0-65535>		
system-circuit-id *PORTS* **text** *STRING*		
system-circuit-id *PORTS* **option format** *NAME*		
system-circuit-id port-type physical		

To delete a specified remote and circuit ID, use the following command.

Command	Mode	Description
no system-remote-id	Option 82	Deletes a specified remote and circuit ID
no system-remote-id option format		
no system-circuit-id *PORTS* [**option format**]		
no system-circuit-id port-type physical		

8.5.6.3 Option 82 Reforwarding Policy

A DHCP relay agent may receive a DHCP packet from a DHCP server or another DHCP relay agent that already contains relay information. You can specify a DHCP option 82 reforwarding policy to be suitable for the network.

To specify a DHCP option 82 reforwarding policy, use the following command.

Command	Mode	Description
policy {**replace** | **keep**}	Option 82	Specifies a DHCP option 82 reforwarding policy. replace: replaces an existing DHCP option 82 information with a new one. keep: keeps an existing DHCP option 82 information (default). non-option82: DHCP packet option82: DHCP option 82 packet none: no DHCP packet (default)
policy drop {**non-option82** | **option82** | **none**}		

8.5.6.4 Option 82 Trust Policy

Default Trust Policy

To specify the default trust policy for DHCP packets, use the following command.

Command	Mode	Description
trust default {**deny** | **permit**}	Option 82	Specifies the default trust policy for a DHCP packet.

i If you specify the default trust policy as **deny**, the DHCP packet that carries the information you specifies below will be permitted, and vice versa.

Trusted Remote ID

To specify a trusted remote ID, use the following command.

Command	Mode	Description
trust remote-id hex *HEXSTRING*	Option 82	Specifies a trusted remote ID.
trust remote-id ip *A.B.C.D*		
trust remote-id text *STRING*		

To delete a specified trusted remote ID, use the following command.

Command	Mode	Description
no trust remote-id hex *HEXSTRING*	Option 82	Deletes a specified trusted remote ID.
no trust remote-id ip *A.B.C.D*		
no trust remote-id text *STRING*		

Trusted Physical Port

To specify a trusted physical port, use the following command.

Command	Mode	Description
trust port *PORTS* {**normal** | **option82** | **all**}	Option 82	Specifies a trusted physical port. normal: DHCP packet option82: DHCP option 82 packet all: DHCP + option 82 packet
no trust port {**all** | PORTS} {**normal** | **option82** | **all**}		Deletes a specified trusted port.

8.5.7 DHCP Snooping

For enhanced security, the OLT provides the DHCP snooping feature. The DHCP snooping filters untrusted DHCP messages and builds/maintains a DHCP snooping binding table. The untrusted DHCP message is a message received from outside the network, and an untrusted interface is an interface configured to receive DHCP messages

from outside the network.

The DHCP snooping basically permits all the trusted messages received from within the network and filters untrusted messages. In case of untrusted messages, all the binding entries are recorded in a DHCP snooping binding table. This table contains a hardware address, IP address, lease time, VLAN ID, interface, etc.

It also gives you a way to differentiate between untrusted interfaces connected to the end-user and trusted interfaces connected to the DHCP server or another switch.

i The DHCP snooping only filters the DHCP server message such as a DHCP_OFFER or DHCP_ACK, which is received from untrusted interfaces.

8.5.7.1 Enabling DHCP Snooping

To enable the DHCP snooping globally, use the following command

Command	Mode	Description
ip dhcp snooping	Global	Enables the DHCP snooping globally.
no ip dhcp snooping		Disables the DHCP snooping globally. (default)

⚠ Upon enabling the DHCP snooping, the DHCP_OFFER and DHCP_ACK messages from all the ports will be discarded before specifying a trusted port.

To enable the DHCP snooping on a VLAN, use the following command

Command	Mode	Description
ip dhcp snooping vlan *VLANS*	Global	Enables the DHCP snooping on a specified VLAN.
no ip dhcp snooping vlan *VLANS*		Disables the DHCP snooping on a specified VLAN.

⚠ You must enable DHCP snooping globally before enabling DHCP snooping on a VLAN.

8.5.7.2 DHCP Trust State

To define a state of a port as trusted or untrusted, use the following command.

Command	Mode	Description
ip dhcp snooping trust *PORTS*	Global	Defines a state of a specified port as trusted.
no ip dhcp snooping trust *PORTS*		Defines a state of a specified port as untrusted. (default)

8.5.7.3 DHCP Filter on Trust Port

To filter broadcast request packets outgoing from the specified trust port, use the following command.

Command	Mode	Description
ip dhcp snooping trust *PORTS* **filter egress bcast-req**	Global	Filters egress broadcast request packets on the trust port.
no ip dhcp snooping trust *PORTS* **filter egress bcast-req**		Disable filtering egress broadcast request packets on the trust port.

8.5.7.4 DHCP Rate Limit

To set the number of DHCP packets per second (pps) that an interface can receive, use the following command.

Command	Mode	Description
ip dhcp snooping limit-rate *PORTS* <1-255>	Global	Sets a rate limit for DHCP packets. (unit: pps)
no ip dhcp snooping limit-rate *PORTS*		Deletes a rate limit for DHCP packets.

i Normally, the DHCP rate limit is specified to untrusted interfaces and 15 pps is recommended for a proper value. If, however, you want to set a rate limit for trusted interfaces, keep in mind that trusted interfaces aggregate all DHCP traffic in the switch, and you will need to adjust the rate limit to a higher value.

To set the number of DHCP discover/request message per second, use the following command.

Command	Mode	Description
ip dhcp snooping limit-rate { **discover** | **request** } <1-32767>	Global	Receieves the DHCP discover/request message as much as the specified packet per second. 1-32767: packet per second
no ip dhcp snooping limit-rate { **discover** | **request** }		Disables the discover/request message limit function.

i DHCP snooping function should be activated before setting the **ip dhcp snooping limit-rate** { **discover** | **request** } command.

To display the rate limit for DHCP packets, use the following command.

Command	Mode	Description
show ip dhcp snooping limit-rate {**config** | **status**}	Enable Global	Shows the rate limit for DHCP packets. config: user configuration status: current status of DHCP packets limit

8.5.7.5 DHCP Lease Limit

The number of entry registrations in DHCP snooping binding table can be limited. If there are too many DHCP clients on an interface and they request IP address at the same time, it may cause IP pool exhaustion.

To set the number of entry registrations in DHCP snooping binding table, use the following command.

Command	Mode	Description
ip dhcp snooping limit-lease *PORTS* <1-2147483637>	Global	Enables a DHCP lease limit on a specified untrusted port. 1-2147483637: the number of entry registrations
no ip dhcp snooping limit-lease *PORTS*		Deletes a DHCP lease limit.

You can limit the number of entry registrations only for untrusted interfaces, because the DHCP snooping binding table only contains the information for DHCP messages from untrusted interfaces.

To set the number of DHCP discover message per second that an interface can receive just one DHCP discover message, use the following command.

Command	Mode	Description
ip dhcp snooping limit-rate discover	Global	Receieves a single DHCP discover message per second.
no ip dhcp snooping limit-rate discover		Disable the discover message limit function.

DHCP snooping function should be activated before setting the **ip dhcp snooping limit-rate discover** command.

8.5.7.6 Source MAC Address Verification

The OLT can verify that the source MAC address in a DHCP packet that is received on untrusted ports matches the client hardware address in the packet. To enable the source MAC address verification, use the following command.

Command	Mode	Description
ip dhcp snooping verify mac-address	Global	Enables the source MAC address verification.
no ip dhcp snooping verify mac-address		Disables the source MAC address verification.

8.5.7.7 Static DHCP Snooping Binding

The DHCP snooping binding table contains a hardware address, IP address, lease time, VLAN ID, and port information that correspond to the untrusted interfaces of the system. To manually specify a DHCP snooping binding entry, use the following command.

Command	Mode	Description
ip dhcp snooping binding <1-4094> *PORT A.B.C.D MAC-ADDR* <120-2147483637>	Global	Configures binding on DHCP snooping table. 1-4094: VLAN ID PORT: port number A.B.C.D: IP address MAC-ADDR: MAC address 120-2147483637: lease time (unit: second)
clear ip dhcp snooping binding *PORT* {*A.B.C.D* | **all**}		Deletes a specified static DHCP snooping binding. all: all DHCP snooping bindings

8.5.7.8 DHCP Snooping Database Agent

When the DHCP snooping is enabled, the system uses the DHCP snooping binding database to store information about untrusted interfaces. Each database entry (binding) has an IP address, associated MAC address, lease time, interface to which the binding applies and VLAN to which the interface belongs.

You can save the current binding entries in a file at a remote location (TFTP server). Upon reloading, the switch can read the file to build the DHCP snooping database for the binding. The system keeps the current file by writing to the file as the database changes.

To specify a TFTP server and interval to back up the DHCP snooping database, use the following command.

Command	Mode	Description
ip dhcp snooping database *A.B.C.D INTERVAL*	Global	Specifies a TFTP server to save the backup file of DHCP snooping database. Sets the interval of how often the DHCP snooping binding DB will be backed up. A.B.C.D: TFTP server address INTERVAL: 120-2147483637 (unit: second)
no ip dhcp snooping database		Deletes the configured TFTP server address and interval for DHCP snooping DB backup.

To restore the DHCP snooping binding entries from a TFTP server, use the following command.

Command	Mode	Description
ip dhcp snooping database renew *A.B.C.D*	Global	Reads the current DHCP snooping database file from a TFTP server. A.B.C.D: TFTP server address
ip dhcp snooping database renew auto {**on** | **off**}		Enables/disables the system to be automatically restored the DHCP snooping DB file from the TFTP server after a restart or reload of the switch.

ip dhcp snooping database renew auto retry <1-50>		Specifies the maximum number of retry attempts to automatically restore the DHCP snooping DB file from the TFTP server.

i The file of DHCP snooping database entries is stored in a remote location accessible through TFTP.

8.5.7.9 ARP Inspection Start Time

This function sets the time before ARP inspection starts to run. Before setting this, ARP inspection should be turned on. ARP inspection checks validity of incoming ARP packets by using DHCP snooping binding table and denies the ARP packets if they are not identified in the table.

However, the OLT may be rebooted with any reason, then DHCP snooping binding table entries, which are dynamically learned from DHCP packets back and forth the OLT, would be lost. Thus, ARP inspection should be delayed to start during some time so that DHCP snooping table can build entries. If no time given, ARP inspection sees empty snooping table and drop every ARP packet.

To specify the ARP inspection delay time, use the following command.

Command	Mode	Description
ip dhcp snooping arp-inspection start <1-2147483637>	Global	Configures the ARP inspection delay time. If reboot, ARP inspection resumes after the time you configure. 1-2147483637: delay time (unit: second)
no ip dhcp snooping arp-inspection start		Delete the configured ARP inspection delay time.

8.5.7.10 DHCP Snooping with Option82

In case of L2 environment, when forwarding DHCP messages to a DHCP server, a DHCP switch can insert or remove DHCP option82 data on the DHCP messages from the clients.

In case of a switch is enabled with DHCP snooping, it floods DHCP packets with DHCP option82 field when the DHCP option82 is enabled. This allows an enhanced security and efficient IP assignment in the Layer 2 environment with a DHCP option82 field.

i If DHCP snooping is enabled in the system of OLT, DHCP packets includes DHCP option82 field by default.

To enable/disable the switch which is enabled by DHCP snooping to insert or remove DHCP option82 field, use the following command.

Command	Mode	Description
ip dhcp snooping information option	Global	Enables the switch to insert DHCP option 82 field in forwarded DHCP packets to the DHCP server.
no ip dhcp snooping information option		Disables the switch not to insert DHCP option 82 field in forwarded DHCP packets to the DHCP server

8.5.7.11 DHCP Snooping Option

DHCP snooping switch may receive DHCP messages (Discover/Request) with various different options from clients, which cause DHCP server hard to manage client's informtion in the perspective of data consistency. That's why this function is necessay.

The switch operating DHCP snooping can modify or attach an option field of the DHCP messages (Discover/Request) with a defined snooping option and can forward them to DHCP server. The snooping option can be applied on a port basis or on entire ports. Before using this function, a global DHCP option format should be created. For details of setting the DHCP option format, refer to the 8.5.5 DHCP Option.

To set a DHCP snooping option for a specifc port, use the following command.

Command	Mode	Description
ip dhcp snooping port *PORTS* **opt-code** <1-254> **format** *NAME*	Global	Specifies a snooping option format on a port. opt-code: DHCP option code NAME: DHCP option format name
ip dhcp snooping port *PORTS* **opt-code** <1-254> **policy** {**keep** | **replace**}		Configures a policy against DHCP option belonging to a DHCP message (default: replace) keep: forwards a DHCP message to DHCP server without any modification. replace: deletes the DHCP message's option and adds the snooping option if both of them are same. However, if they are different each other, **replace** option just adds the snooping option.
no ip dhcp snooping port PORTS opt-code <1-254>		Removes the DHCP snooping option for a given port.

In case there is not a DHCP snooping option for a specific port, DHCP snooping switch finds the snooping default option. If it exists, DHCP snooping switch sends a DHCP server DHCP messages (Discover/Request) by replacing their options with the snooping default option.

To specify a DHCP server default option, use the following command.

Command	Mode	Description
ip dhcp snooping default-option code <1-254> **format** *NAME*	Global	Specifies a snooping default option format for a switch. NAME: DHCP option format name
ip dhcp snooping default-option code <1-254> **policy** <**keep** | **replace**>		Configures a policy against DHCP option belonging to a DHCP message (default: replace) keep: forwards a DHCP message to DHCP server without any modification. replace: deletes the DHCP message's option and adds the snooping default option if both of them are same. However, if they are different each other, **replace** option just adds the snooping default option.
no ip dhcp snooping default-option code <1-254>		Removes the DHCP snooping default option for a given port.

8.5.7.12 Displaying DHCP Snooping Configuration

To display DHCP snooping table, use the following command.

Command	Mode	Description
show ip dhcp snooping	Enable Global	Shows a DHCP snooping configuration.
show ip dhcp snooping binding [**port** *PORTS*]		Shows DHCP snooping binding entries. PORTS: port number to use
show ip dhcp snooping binding vlan *VLANS*		Shows DHCP snooping binding vlan. VLANS: vlan id to use
show ip dhcp snooping lease-time		Shows DHCP snooping lease time.
show ip dhcp snooping statistics [**port** *PORTS*]		Shows DHCP snooping statistics.

To clear DHCP snooping statistics of the DHCP server, use the following command.

Command	Mode	Description
clear ip dhcp snooping statistics [**port** *PORTS*]	Enable Global	Clears DHCP snooping statistics.

8.5.8 IP Source Guard

IP source guard is similar to DHCP snooping. This function is used on DHCP snooping untrusted Layer 2 port. Basically, except for DHCP packets that are allowed by DHCP snooping process, all IP traffic comes into a port is blocked. If an authorized IP address from the DHCP server is assigned to a DHCP client, or if a static IP source binding is configured, the IP source guard restricts the IP traffic of client to those source IP addresses configured in the binding; any IP traffic with a source IP address other than that in the IP source binding will be filtered out. This filtering limits a host's ability to attack

the network by claiming a neighbor host's IP address.

IP source guard supports the Layer 2 port only, including both access and trunk. For each untrusted Layer 2 port, there are two levels of IP traffic security filtering:

- **Source IP Address Filter**
  IP traffic is filtered based on its source IP address. Only IP traffic with a source IP address that matches the IP source binding entry is permitted. An IP source address filter is changed when a new IP source entry binding is created or deleted on the port, which will be recalculated and reapplied in the hardware to reflect the IP source binding change. By default, if the IP filter is enabled without any IP source binding on the port, a default policy that denies all IP traffic is applied to the port. Similarly, when the IP filter is disabled, any IP source filter policy will be removed from the interface.
- **Source IP and MAC Address Filter**
  IP traffic is filtered based on its source IP address as well as its MAC address; only IP traffic with source IP and MAC addresses matching the IP source binding entry are permitted. When IP source guard is enabled in IP and MAC filtering mode, the DHCP snooping option 82 must be enabled to ensure that the DHCP protocol works properly. Without option 82 data, the switch cannot locate the client host port to forward the DHCP server reply. Instead, the DHCP server reply is dropped, and the client cannot obtain an IP address.

8.5.8.1 Enabling IP Source Guard

After configuring DHCP snooping, configure the IP source guard using the provided command. When IP source guard is enabled with this option, IP traffic is filtered based on the source IP address. The switch forwards IP traffic when the source IP address matches an entry in the DHCP snooping binding database or a binding in the IP source binding table.

To enable IP source guard, DHCP snooping needs to be enabled.

To enable IP source guard with a source IP address filtering on a port, use the following command.

Command	Mode	Description
ip dhcp verify source *PORTS*	Global	Enables IP source guard with a source IP address filtering on a port.
no ip dhcp verify source *PORTS*		Disables IP source guard.

To enable IP source guard with a source IP address and MAC address filtering on a port, use the following command.

Command	Mode	Description
ip dhcp verify source port-security *PORTS*	Global	Enables IP source guard with a source IP address and MAC address filtering on a port.
no ip dhcp verify source port-security *PORTS*		Disables IP source guard.

Note that the IP source guard is only enabled on DHCP snooping untrusted Layer 2 port! If you try to enable this function on a trusted port, the error message will be shown up.

You cannot configure IP source guard with the **ip dhcp verify source** and **ip dhcp verify source port-security** commands together.

8.5.8.2 Static IP Source Binding

The IP source binding table has bindings that are learned by DHCP snooping or manually specified with the **ip dhcp verify source binding** command. The switch uses the IP source binding table only when IP source guard is enabled.

To specify a static IP source binding entry, use the following command.

Command	Mode	Description
ip dhcp verify source binding <1-4094> *PORT A.B.C.D MAC-ADDR*	Global	Specifies a static IP source binding entry. 1-4094: VLAN ID PORT: port number A.B.C.D: IP address MAC-ADDR: MAC address
no ip dhcp verify source binding {*A.B.C.D* | **all**}		Deletes a specified static IP source binding.

8.5.8.3 Displaying IP Source Guard Configuration

To display IP source binding table, use the following command.

Command	Mode	Description
show ip dhcp verify source binding	Enable Global	Shows IP source binding entries.

8.5.9 DHCP Client

An interface of the OLT can be configured as a DHCP client, which can obtain an IP address from a DHCP server. The configurable DHCP client functionality allows a DHCP client to use a user-specified client ID, class ID or suggested lease time when requesting an IP address from a DHCP server. Once configured as a DHCP client, the OLT cannot be configured as a DHCP server or relay agent.

8.5.9.1 Enabling DHCP Client

To configure an interface as a DHCP client, use the following command.

Command	Mode	Description
ip address dhcp	Interface	Enables a DHCP client on an interface.
no ip address dhcp		Disables a DHCP client.

8.5.9.2 DHCP Client ID

To specify a client ID, use the following command.

Command	Mode	Description
ip dhcp client client-id hex *HEXSTRING*	Interface	Specifies a client ID.
ip dhcp client client-id text *STRING*		
no ip dhcp client client-id		Deletes a specified client ID.

8.5.9.3 DHCP Class ID

To specify a class ID, use the following command.

Command	Mode	Description
ip dhcp client class-id hex *HEXSTRING*	Interface	Specifies a class ID. (default: system MAC address)
ip dhcp client class-id text *STRING*		
no ip dhcp client class-id		Deletes a specified class ID.

8.5.9.4 Host Name

To specify a host name, use the following command.

Command	Mode	Description
ip dhcp client host-name *NAME*	Interface	Specifies a host name.
no ip dhcp client host-name		Deletes a specified host name.

8.5.9.5 IP Lease Time

To specify IP lease time that is requested to a DHCP server, use the following command.

Command	Mode	Description
ip dhcp client lease-time <120-2147483637>	Interface	Specifies IP lease time in the unit of second (default: 3600).
no ip dhcp client lease-time		Deletes a specified IP lease time.

8.5.9.6 Requesting Option

To configure a DHCP client to request an option from a DHCP server, use the following command.

Command	Mode	Description
ip dhcp client request {**domain-name** | **dns**}	Interface	Configures a DHCP client to request a specified option.

To configure a DHCP client not to request an option, use the following command.

Command	Mode	Description
no ip dhcp client request {**domain-name** | **dns**}	Interface	Configures a DHCP client not to request a specified option.

8.5.9.7 Forcing Release or Renewal of DHCP Lease

The OLT supports two independent operation: immediate release a DHCP lease for a DHCP client and force DHCP renewal of a lease for a DHCP client.

To force a release or renewal of a DHCP release for a DHCP client, use the following command.

Command	Mode	Description
release dhcp *INTERFACE*	Enable	Forces a release of a DHCP lease.
renew dhcp *INTERFACE*		Forces a renewal of a DHCP lease.

8.5.9.8 Displaying DHCP Client Configuration

To display a DHCP client configuration, use the following command.

Command	Mode	Description
show ip dhcp client [*INTERFACE*]	Enable Global Interface	Shows a configuration of DHCP client.

8.5.10 DHCP Filtering

8.5.10.1 DHCP Packet Filtering

For the OLT, it is possible to block the specific client with MAC address. If the MAC address blocked by administrator requests an IP address, the server does not assign IP. This function is to strength the security of DHCP server.

The following is the function of blocking to assign IP address on a port.

Command	Mode	Description
ip dhcp filter-port *PORTS*	Global	Configures a port in order not to assign IP.
no ip dhcp filter-port *PORTS*		Disables DHCP packet filtering.

The following is to designate MAC address which IP address is not assigned.

Command	Mode	Description
ip dhcp filter-address *MAC-ADDR*	Global	Blocks a MAC address in case of requesting IP address. MAC-ADDR: MAC address
no ip dhcp filter-address *MAC-ADDR*		Disables DHCP MAC filtering.

8.5.10.2 DHCP Server Packet Filtering

Dynamic Host Configuration Protocol (DHCP) makes DHCP server assign IP address to DHCP clients automatically and manage the IP address. Most ISP operators provide the service as such a way. At this time, if a DHCP client connects with the equipment that can be the other DHCP server such as Internet access gateway router, communication failure might be occurred.

DHCP filtering helps to operate DHCP service by blocking DHCP request which enters through subscriber's port and goes out into uplink port or the other subscriber's port and DHCP reply which enters to the subscriber's port.

In the Fig. 8.32, server A has the IP area from 192.168.10.1 to 192.168.10.10. Suppose a user connects with client 3 that can be DHCP server to A in order to share IP address from 10.1.1.1 to 10.1.1.10.

Here, if client 1 and client 2 are not blocked from client 3 of DHCP server, client 1 and client 2 will request and receive IP from client 3 so that communication blockage will be occurred. Therefore, the filtering function should be configured between client 1 and client 3, client 2 and client 3 in order to make client 1 and client 2 receive IP without difficulty from DHCP server A.

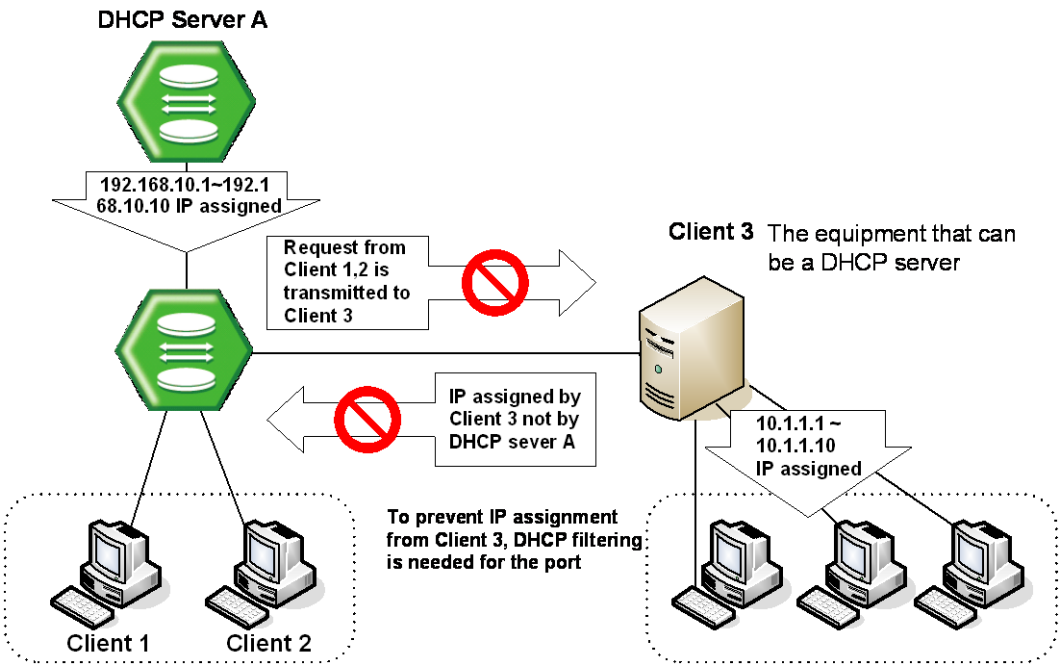


Fig. 8.32 DHCP Server Packet Filtering

To enable the DHCP server packet filtering, use the following command.

Command	Mode	Description
dhcp-server-filter *PORTS*	Bridge	Enables the DHCP server packet filtering.
no dhcp-server-filter *PORTS*		Disables the DHCP server packet filtering.

To display a status of the DHCP server packet filtering, use the following command.

Command	Mode	Description
show dhcp-server-filter	Enable Global Bridge	Show a status of the DHCP server packet filtering.

8.5.11 Debugging DHCP

To enable/disable a DHCP debugging, use the following command.

Command	Mode	Description
debug dhcp {filter | lease | packet | service | all}	Enable	Enables a DHCP debugging.
no debug dhcp {filter | lease | packet | service | all}		Disables a DHCP debugging.

To display the debugging information, use the following command.

Command	Mode	Description
show debugging dhcp	Enable Global	Shows the debugging information of DHCP.

8.6 Dynamic Host Configuration Protocol (DHCP) for IPv6

Dynamic Host Configuration Protocol (DHCP) for IPv6 provides a device with addresses assigned by a DHCP server and other configuration information, which are carried in options. DHCPv6 offers the capability of automatic allocation of reusable network addresses.

The basic DHCPv6 client, server and relay agent concept is similar to DHCP for IPv4. An advantage of DHCPv6 for dynamic address assignment is that it is capable of providing additional information to the nodes. DHCPv6 provides DNS information and uses a 16-bit option space.

DHCPv6 can record addresses assigned to hosts and assign addresses to specific hosts, thus facilitating network management. And it assigns prefixes to devices, thus facilitating automatic configuration and management of the entire network.

A node may autoconfigure addresses based on router advertisement (RA) under IPv6 environment.

DHCP Unique Identifier (DUID)

Using a DHCP unique identifier (DUID), each DHCP for IPv6 client and server is identified. A DUID is used to identify the device when exchanging DHCPv6 messages. The DUID is designed to be unique around all DHCPv6 clients and servers, and it is stable for any specific client or server. A DUID can be no longer than 128 octets. There are three types of DUIDs.

- **DUID-LLT (Link-layer address plus time)**
  Link-layer address of any one network interface that is connected to the DHCP device at the time that the DUID is generated.
- **DUID-EN (Enterprise number)**
  It consists of the vendor's registered private enterprise number as maintained by IA_NA followed by a unique identifier assigned by the vendor.
- **DUID-LL (Link-layer address)**
  It consists of the link-layer address of any one network interface that is permanently connected to the client or server device.

An Identity Association (IA) is a construct through which a server and a client can identify, group, and manage a set of related IPv6 addresses. Each IA consists of an Identity Association Identifier (IAID) and associated configuration information. A client should associate at least one IA with each of its network interfaces for which it is to request the assignment of IPv6 addresses from a DHCP server. There are three main IPv6 prefix types: IA_PD, IA_NA, and IA_TA. Each Identity Association for Temporary Address (IA_TA) option contains at most one temporary address for each of the prefixes on the link to which the client is attached. The clients ask for temporary addresses and servers assign them. An Identity Association for Non-temporary Address (IA_NA) carries assigned addresses that are not temporary addresses. An Identity Association for Prefix Delegation (IA_PD) is a collection of prefixes assigned to the requesting router. Each IA_PD has an associated IAID.

DHCPv6 Address Assignment Mechanism

DHCP for IPv6 can provide stateful address configuration or stateless configuration settings to IPv6 hosts. IPv6 hosts use several methods to configure addresses:

- **Stateful Mechanism**
  It obtains interface address and configuration information from DHCP server. A site requires tighter control over exact address assignment.
- **Stateless Mechanism**
  It allows a host to generate its own address using a combination information advertisement by routers. A site is not concerned with the exact address hosts use.

DHCPv6 Message Types

There are 13 DHCP message types. The following table summarizes the DHCP message types.

DHCPv6 Message	Value	Description
Solicit	1	Sent by clients to locate DHCPv6 servers.
Advertise	2	Sent by server as a response to Solicit message received from a client to indicate that it is available for DHCP service.
Request	3	Sent by clients to request configuration parameters, including IP address or delegated prefixes, from a specific server.
Confirm	4	Sent by clients to verify that their address and configuration parameters are still valid.
Renew	5	Sent by clients to renew their configuration parameters with their original DHCP server when their lease is about to expire.
Rebind	6	Sent by client to extend the lifetime of their address and renew their configuration parameters with any DHCP server when their lease is about to expire
Reply	7	Sent by DHCP servers responding to Request, Confirm, Renew, Rebind, Release, and Decline messages.
Release	8	Sent by clients to release their IP address
Decline	9	Sent by clients to indicate that one or more addresses assigned to them are already in use on the link.
Reconfigure	10	Sent by DHCP servers to inform clients that the server has new or updated configuration information. The clients then must initiate a request in order to obtain the updated information.
Information-request	11	Sent by clients to request configuration parameters without the assignment of any IP addresses to the client.
Relay-forward	12	Sent by DHCP relays to forward client messages to servers. The relay encapsulates the client message in an option in the relay-forward message.
Relay-reply	13	Sent by DHCP servers to send messages to clients through a relay. The client message is encapsulated as an option in the relay-reply message. The relay decapsulates the message and forwards it to the client.

Tab. 8.4 DHCPv6 Message Types

- Message types from client to server
  - Solicit, Request, Confirm, Renew, Rebind, Release, Decline, Information-request
- Message types from server to client
  - Advertise, Replay, Reconfigure
- Message type from relay to relay/server
  - Relay-forward
- Message type from relay/server to relay
  - Relay-reply

- **DHCPv6 Client-Server Message**

DHCP servers communicate with DHCP clients by a series of DHCP messages. The Msg. Type field (1-byte) indicates the type of DHCPv6 message. The Transaction ID field (3-byte) is determined by a client and used to group the messages of a DHCPv6 message exchange together. Following the Transaction-ID field, DHCPv6 options are used to indicate client and server identification, addresses, and other configuration settings. For the list of defined DHCPv6 options, see RFC 3315. DHCPv6 options are formatted with the type-length-value (TLV) format.

The following figure shows the structure of DHCPv6 messages sent between client and server.

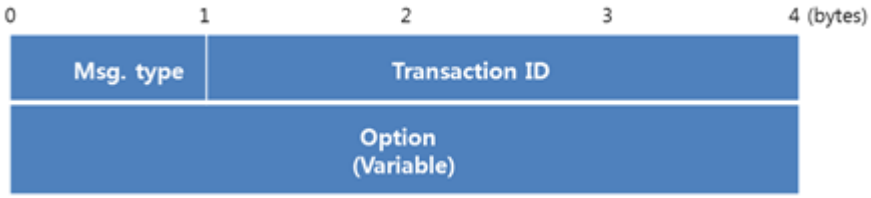


Fig. 8.33 Basic DHCPv6 Message Format

- **DHCPv6 Relay agent-Server Message**

DHCP relay agent is a node that acts as an intermediary to deliver DHCP messages between clients and servers, and is on the same link as the client. If there is a relay agent between the client and the server, the relay agent sends the server Relay-Forward messages containing the encapsulated Solicit and Request messages from the client. The server sends the relay agent Relay-Reply messages containing the encapsulated Advertise and Reply messages for the client.

There is a separate message structure for the messages exchanged between relay agents and servers to record additional information.

The following figure shows the structure of these kinds of messages.

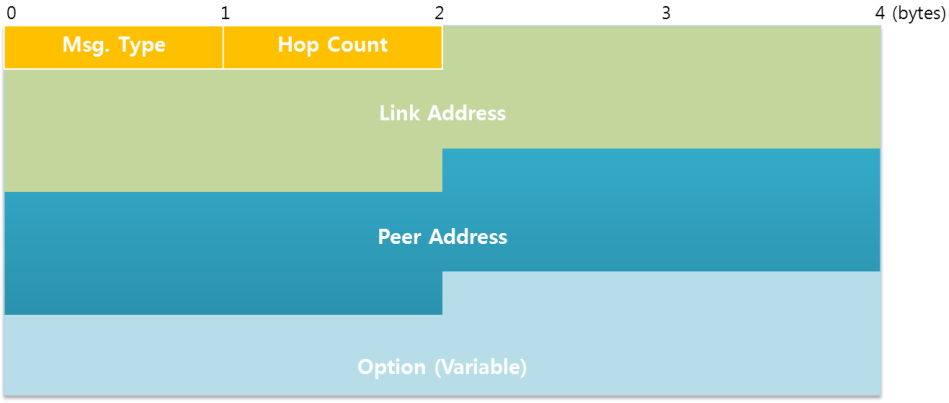


Fig. 8.34 General Shared Relay Message Format

The Hop Count field (1-byte) indicates the number of relay agents that have received the message. A receiving relay agent can discard the message if it exceeds a configured maximum hop count. The Link Address field (16-byte) contains a non-link-local address that is assigned to an interface connected to the subnet on which the client is located. From the Link Address field, the server can determine the correct address scope from which to assign an address. The Peer Address field (16-byte) contains the IPv6 address of the client that originally sent the message or the previous relay agent that relayed the message. The Relay Message option provides an encapsulation of the messages being exchanged between the client and the server.

Prefix Delegation for DHCPv6

This prefix delegation mechanism is appropriate for use by an ISP to delegate a prefix to a subscriber, where the delegated prefix would possibly be subnetted and assigned to the links within the subscriber's network. Prefix delegation with DHCP is independent of address assignment with DHCP. A requesting router can use DHCP for just prefix delegation or for prefix delegation along with address assignment and other configuration information.

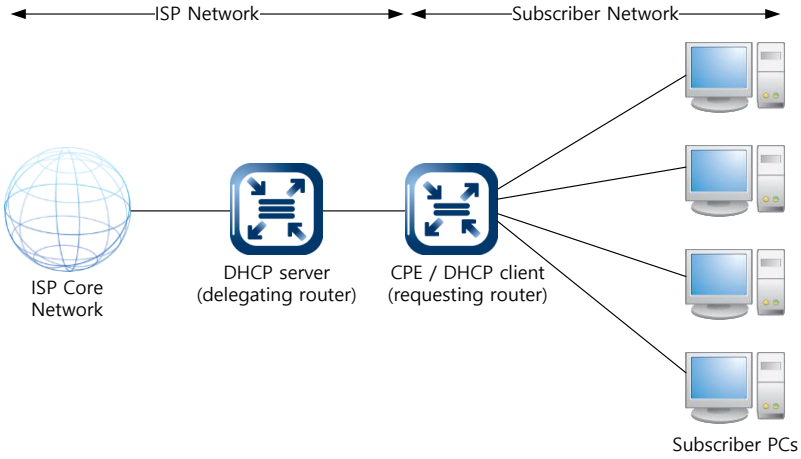


Fig. 8.35 An Example of Prefix Delegation

The delegating router acts as a DHCP server, and is responding to the prefix request. It is configured with a set of prefixes to be used for assignment to customers at the time of each customer's first connection to the ISP service. The prefix delegation process begins when the requesting router requests configuration information through DHCPv6. The DHCP messages from the requesting router (DHCP client) are received by the delegating router in the aggregation device. When the delegating router receives the request, it selects an available prefix or prefixes for delegation to the requesting router. The delegating router then returns the prefix or prefixes to the requesting router. The requesting router subnets the delegated prefix and assigns the longer prefixes to links in the subscriber's network. The requesting router subnets a single delegated /48 prefix into /64 prefixes and assigns one /64 prefix to each of the links in the subscriber network.

The prefix delegation options can be used in conjunction with other DHCP options carrying other configuration information to the requesting router. The requesting router provides DHCP service to hosts attached to the internal network. For example, the requesting router may obtain the addresses of DNS and NTP servers from the ISP delegating router, and then pass that configuration information on to the subscriber hosts through a DHCP server in the requesting router.

DHCPv6 Basic Operation

DHCPv6 clients and servers exchange DHCP messages using UDP port. DHCPv6 clients listen for DHCP messages on UDP port 546. DHCPv6 servers and relay agents listen for DHCPv6 messages on UDP port 547. The client can obtain server or relay agent's address using All-DHCP-Server and All-DHCP-Agent address.

	Port	Port #	Description
Client	UDP	546	Clients listen for DHCP messages on UDP port 546.
Server	UDP	547	Server and relay agents listen for DHCP messages on UDP port 547.

Tab. 8.5 DHCPv6 UDP port

There are no broadcast addresses defined for IPv6. Therefore, the use of the limited broadcast address for some DHCPv4 messages has been replaced with the use of the site-scoped multicast address (FF05::1:3) and link-scoped multicast address (FF02::1:2) for DHCPv6.

DHCPv6 Multicast Address		Description
All_DHCP_Servers (Site-local scope)	FF05::1:3	A site-scoped multicast address used by a relay agent or client to communicate with servers, either because the relay agent wants to send messages to all servers or because it does not know the unicast addresses of the servers. All DHCP servers within a site are members of this multicast group.
All_DHCP_Relay_Agents _and_Servers (Link-local scope)	FF02::1:2	A link-scoped multicast address used by a client to communicate with neighboring (i.e., on-link) relay agents and servers. All servers and relay agents are members of this multicast group.

Tab. 8.6 DHCPv6 Address

There is the four-message exchange handshake for a single interface with one IA_NA and one address for this IA_NA.

To obtain an IP address, the DHCP client daemon (dhcpcd6) sends a Solicit message to the link-scoped address (FF02::1:2), which is received by the server and processed. If a free address is available for that client, an Advertise message is created and sent back to the client. This message contains an IP address and other options that are appropriate for that client. The client receives the server DHCP Advertise message and stores it while waiting for other advertisements. When the client has chosen the best advertisement, it sends a DHCP Request to the link-scoped address (FF02::1:2) specifying which server advertisement it wants.

All configured DHCP servers receive the Request message. Each monitors to see if it is the requested server. The server does not process any packet with a server DUID that does not match its own. The requested server marks the address as assigned and returns a DHCP Reply, at which time, the transaction is complete. The client has an address for the period of time (valid-lifetime) designated by the server.

When the preferred-lifetime expires for the address, the client sends the server a Renew message to extend the lease time. If the server is willing to renew the address, it sends a DHCP Reply message. If the client does not get a response from the server that owns its current address, it multicasts a DHCP Rebind message if, for example, the server has been moved from one network to another. If the client has not renewed its address after the valid-lifetime, the address is removed from the interface and the process starts over. This cycle prevents multiple clients on a network from being assigned the same address.

8.6.1 DHCPv6 Server

8.6.1.1 Creating DHCPv6 address Pool

The DHCP pool is a group of IP addresses that will be assigned to DHCP clients by DHCP server. You can create various DHCP pools that can be configured with a different network, default gateway and range of IP addresses. This allows the network administrators to effectively handle multiple DHCP environments. To create a DHCPv6 pool, use the following command.

Command	Mode	Description
ipv6 dhcp pool *POOL*	Global	Creates a DHCPv6 pool and opens *DHCPv6 Pool Configuration* mode.
no ipv6 dhcp pool *POOL*		Removes the specified DHCPv6 pool.

The following is an example of creating the DHCPv6 pool as *sample*.

```
SWITCH(config)# ipv6 dhcp pool sample
SWITCH(config-dhcp6[sample])#
```

To display a DHCPv6 pool configuration, use the following command.

Command	Mode	Description
show ipv6 dhcp pool [*POOL*]	Enable Global Bridge	Shows the DHCPv6 address pool information POOL: DHCPv6 pool name

8.6.1.2 Domain Name

To set a domain name, use the following command.

Command	Mode	Description
domain-name *DOMAIN*	DHCPv6 Pool	Sets a domain name. DOMAIN: a domain name
no domain-name		Deletes the configured domain name.

8.6.1.3 DNS Server

The DNS server option is used to inform clients of DNS server addresses. The address of the DNS server should be statically configured in the DHCPv6 server configuration.

To specify a DNS server to inform DHCP clients, use the following command.

Command	Mode	Description
dns-server *X:X::X:X*	DHCPv6 Pool	Specifies a DNS server. X:X::X:X: DNS server IPv6 address
no dns-server *X:X::X:X*		Deletes a specified DNS server.

8.6.1.4 Range of IPv6 Address

To specify a range of IP addresses that will be assigned to DHCP clients, use the following command.

Command	Mode	Description
range *X:X::X:X X:X::X:X* [{**second** <60-315360000> <60-315360000> | **minute** <1-5256000> <1-5256000>}]	DHCPv6 Pool	Specifies a range of IPv6 addresses. X:X::X:X : start/end IPv6 address 60-315360000: valid life time (unit: second, default: 2592000) 60-315360000: preferred life time (unit: second, default: 604800) 1-5256000: valid life time (unit: minute, default: 43200) 1-5256000: preferred life time (unit: minute, default: 10080)
no range *X:X::X:X X:X::X:X*		Deletes the specified range of IP addresses.

8.6.1.5 DHCPv6 Options

DHCPv6 can be used in two ways. The first way of using DHCPv6 is to grant clients addresses from a pool while also using DHCPv6 to push configuration options. This is called stateful configuration. The other option is to use DHCPv6 combined with SLAAC for addressing, while using DHCPv6 for configuration options. This is called stateless configuration. DHCP for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients. To configure the NIS server DHCPv6 option, use the following command.

Command	Mode	Description
nis domain-name *DOMAIN*	DHCPv6 Pool	Sets a domain name of a NIS server. DOMAIN: a domain name of the NIS server for client to use
nis address X:X::X:X		Specifies the NIS server address to be sent to the client. X:X::X:X: NIS server IPv6 address
no nis domain-name		Removes the NIS domain name.
no nis address X:X::X:X		Removes the NIS server address.

To configure the NIS+ server DHCPv6 option, use the following command.

Command	Mode	Description
nisp domain-name *DOMAIN*	DHCPv6 Pool	Sets a domain name of a NIS+ server. DOMAIN: a domain name of the NIS+ server for client to use
nisp address X:X::X:X		Specifies the NIS+ server address to be sent to the client.
no nisp domain-name		Removes the NIS+ domain name.
no nisp address X:X::X:X		Removes the NIS+ server address.

To configure the SIP server DHCPv6 option, use the following command.

Command	Mode	Description
sip domain-name *DOMAIN*	DHCPv6 Pool	Sets a domain name of a SIP server. DOMAIN: a domain name of the SIP server for client to use
sip address X:X::X:X		Specifies the SIP server address to be sent to the client.
no sip domain-name		Removes the SIP domain name.
no sip address X:X::X:X		Removes the SIP server address.

8.6.1.6 Enabling DHCPv6 Server on Interface

After a DHCPv6 address pool is created, you need to apply/enable the specified pool to an interface. To configure DHCPv6 server functionality on an interface, use the following command.

Command	Mode	Description
ipv6 dhcp server *POOL* [**rapid-commit**] [**preference** <0-255>]	Interface	Enables DHCPv6 server functionality on an interface. POOL: DHCPv6 pool name containing stateless and/or prefix delegation parameters rapid-commit: an option that allows for an abbreviated exchange between the client and server 0-255: value used by clients to determine preference between multiple DHCPv6 servers
no ipv6 dhcp server		Disables the DHCPv6 server functionality.

8.6.1.7 Displaying DHCPv6 Information

To display a DHCPv6 pool configuration, use the following command.

Command	Mode	Description
show ipv6 dhcp pool [*POOL*]	Enable Global	Shows the DHCPv6 address pool information POOL: DHCPv6 pool name

A DHCPv6 Unique Identifier (DUID) is used to identify the device when exchanging DHCPv6 messages. To display the DUID of the local device, use the following command.

Command	Mode	Description
show ipv6 dhcp	Enable Global	Shows this device's DUID.

To display the DHCPv6 interface configuration, use the following command.

Command	Mode	Description
show ipv6 dhcp interface	Enable Global	Shows the DHCPv6 information for all relevant interfaces or the specified interface.

To display information about user-defined local IPv6 address pools, use the following command.

Command	Mode	Description
show ipv6 local pool [*PREFIX-POOL*]	Enable Global	Shows information about any defined IPv6 address local pools.

To display DHCP binding information from the DHCPv6 server binding table, use the following command.

Command	Mode	Description
show ipv6 dhcp binding	Enable Global	Shows all automatic client bindings for the specific IP address from the DHCPv6 server binding table.

To delete/reset the configured bindings of DHCPv6 server, use the following command.

Command	Mode	Description
clear ipv6 dhcp binding	Enable Global	Clears an automatic address binding from the DHCP server database.

8.6.2 DHCPv6 Snooping

For enhanced security, the OLT provides the DHCP snooping feature. The DHCP snooping filters untrusted DHCP messages and maintains a DHCP snooping binding table. An untrusted message is a message received from outside the network, and an untrusted interface is an interface configured to receive DHCP messages from outside the network.

The DHCP snooping basically permits all the trusted messages received from within the network and filters untrusted messages. In case of untrusted messages, all the binding entries are recorded in a DHCP snooping binding table. This table contains a hardware address, IP address, lease time, VLAN ID, interface, etc. It also gives you a way to differentiate between untrusted interfaces connected to the end-user and trusted interfaces connected to the DHCP server or another switch.

8.6.2.1 Enabling DHCPv6 Snooping

DHCPv6 snooping should be enabled to allow clients to obtain IPv6 addresses from an authorized DHCPv6 server. To enable the DHCPv6 snooping on the system, use the following command

Command	Mode	Description
ipv6 dhcp snooping	Global	Enables the DHCPv6 snooping on the system.
no ipv6 dhcp snooping		Disables the DHCPv6 snooping on the system. (default)

To enable the DHCPv6 snooping on a VLAN, use the following command

Command	Mode	Description
ipv6 dhcp snooping vlan *VLANS*	Global	Enables the DHCPv6 snooping on a specific VLAN.
no ipv6 dhcp snooping vlan *VLANS*		Disables the DHCPv6 snooping on a specific VLAN.

You must enable DHCPv6 snooping on the system before enabling DHCPv6 snooping on a VLAN.

8.6.2.2 DHCPv6 Snooping Port State

To define a state of a port as trusted or untrusted, use the following command.

Command	Mode	Description
ipv6 dhcp snooping trust *PORTS*	Global	Configures the specified port as a DHCPv6 snooping trusted port.
no ipv6 dhcp snooping trust *PORTS*		Configures the specified port as a DHCPv6 snooping untrusted port.

8.6.2.3 DHCP Rate Limit

To set the number of DHCPv6 packet per second (pps) that an interface can receive, use the following command.

Command	Mode	Description
ipv6 dhcp snooping limit-rate *PORTS* <1-255>	Global	Sets a rate limit for DHCPv6 packets. (unit: pps)
no ipv6 dhcp snooping limit-rate *PORTS*		Deletes a rate limit for DHCPv6 packets.

Normally, the DHCP rate limit is specified to untrusted interfaces and 15 pps is recommended for a proper value. However, if you want to set a rate limit for trusted interfaces, keep in mind that trusted interfaces aggregate all DHCP traffic in the switch, and you will need to adjust the rate limit to a higher value.

8.6.2.4 DHCP Lease Limit

The number of entry registration in DHCP snooping binding table can be limited. If there are too many DHCP clients on an interface and they request IP address at the same time, it may cause IP pool exhaustion.

To set the number of entry registration in DHCP snooping binding table, use the following command.

Command	Mode	Description
ipv6 dhcp snooping limit-lease *PORTS* <1-2147483637>	Global	Enables a DHCP lease limit on a specified untrusted port. 1-2147483637: the number of entry registration
no ipv6 dhcp snooping limit-lease *PORTS*		Deletes a DHCP lease limit.

You can limit the number of entry registration only for untrusted interfaces, because the DHCP snooping binding table only contains the information for DHCP messages from

untrusted interfaces.

8.6.2.5 Specifying DHCPv6 Snooping Binding Entry

The DHCPv6 snooping binding table contains a hardware address, IPv6 address, lease time, VLAN ID, and port information that correspond to the valid interfaces of the system.

To manually add DHCPv6 snooping binding entry, use the following command.

Command	Mode	Description
ipv6 dhcp snooping binding <1-4094> *PORT X:X::X:X MAC-ADDR* <120-2147483637>	Global	Adds the static entry to the DHCPv6 snooping binding table. 1-4094: VLAN ID PORT: port number X:X::X:X: IPv6 address MAC-ADDR: DHCPv6 client's MAC address 120-2147483637: Expiry time (unit: second)

To remove the configured entry from DHCPv6 snooping binding table, use the following command.

Command	Mode	Description
clear ipv6 dhcp snooping binding *PORT* {*X:X::X:X* | **all**}	Global	Removes the static entry from the DHCPv6 snooping table. PORT: port number X:X::X:X: IPv6 address

8.6.2.6 DHCP Snooping Option

DHCP snooping-enabled switch may receive DHCP messages with various different options from clients, which cause DHCP server hard to manage client's information in the perspective of data consistency. That's why this function is necessary.

The switch operating DHCP snooping can modify or attach an option field of the DHCP messages with the defined snooping option and can forward them to DHCP server. The snooping option can be applied on a port basis or on entire ports.

Before using this function, a global DHCPv6 option format should be created and configured. For details of setting the DHCP option format, refer to the 8.6.4 DHCPv6 Option.

To enter the DHCPv6 option mode, use the following command.

Command	Mode	Description
ipv6 dhcp option format *NAME*	Global	Enters the DHCPv6 option mode to configure the DHCPv6 option format. NAME: DHCPv6 option format name
no ipv6 dhcp option format *NAME*		Deletes the given DHCPv6 option format.

To set a DHCP snooping option for a specific port, use the following command.

Command	Mode	Description
ipv6 dhcp snooping port *PORTS* **opt-code** <1-254> **format** *NAME*	Global	Specifies a snooping option format on a port. opt-code: DHCPv6 option code NAME: DHCPv6 option format name
ipv6 dhcp snooping port *PORTS* **opt-code** <1-254> **policy** {**keep** | **replace**}		Configures a policy against DHCP option belonging to a DHCP message (default: replace) keep: forwards a DHCP message to DHCP server without any modification. replace: deletes the DHCP message's option and adds the snooping option if both of them are same. However, if they are different each other, **replace** option just adds the snooping option.
no ip dhcp snooping port *PORTS* **opt-code** <1-254>		Removes the DHCP snooping option for a given port.

In case there is not a DHCP snooping option for a specific port, DHCP snooping switch finds the snooping default option. If it exists, DHCP snooping switch sends a DHCP server DHCP messages by replacing their options with the snooping default option.

To specify a DHCP server default option, use the following command.

Command	Mode	Description
ipv6 dhcp snooping default-option code <1-254> **format** *NAME*	Global	Specifies a snooping default option format for a switch. NAME: DHCPv6 option format name
ipv6 dhcp snooping default-option code <1-254> **policy** <**keep** | **replace**>		Configures a policy against DHCP option belonging to a DHCP message (default: replace) keep: forwards a DHCP message to DHCP server without any modification. replace: deletes the DHCP message's option and adds the snooping default option if both of them are same. However, if they are different each other, **replace** option just adds the snooping default option.
no ipv6 dhcp snooping default-option code <1-254>		Removes the DHCP snooping default option for a given port.

8.6.2.7 Displaying DHCPv6 Snooping Configuration

To display DHCPv6 snooping table, use the following command.

Command	Mode	Description
show ipv6 dhcp snooping	Enable Global	Shows a DHCPv6 snooping configuration.
show ipv6 dhcp snooping binding		Shows DHCP snooping binding entries for IPv6.

8.6.3 DHCPv6 Relay Agent

8.6.3.1 DHCPv6 Relay Agent Destination

To specify a destination address to which client messages are forwarded and enable DHCP for IPv6 relay service on the interface, use the following command.

Command	Mode	Description
ipv6 dhcp relay destination *X:X::X:X* [*INTERFACE*]	Interface	Specifies relay destination address on an interface. X:X::X:X: IPv6 destination address for DHCPv6 packet forwarding INTERFACE: interface name
no ipv6 dhcp relay destination {**all** | *X:X::X:X* [*INTERFACE*] }		Deletes the specified relay destination address.

8.6.3.2 DHCP Relay Agent Option

The switch operating DHCP server can include DHCP option information in the DHCP communication. Before using this function, a global DHCP option format should be created. For details of setting the DHCPv6 option format, refer to the 8.6.4 DHCPv6 Option.

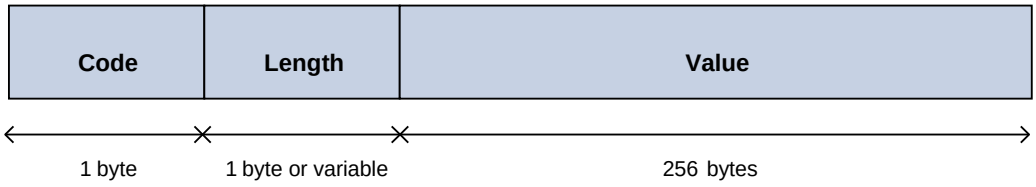
To specify a DHCPv6 server option, use the following command.

Command	Mode	Description
ipv6 dhcp relay option code <1-254> **format** *NAME*	Interface	Specifies a DHCPv6 option format for a DHCP server. code: DHCP option code NAME: DHCPv6 option format name
no ipv6 dhcp relay option code <1-254> **format**		Removes a specified DHCPv6 option for a DHCP server.

8.6.4 DHCPv6 Option

This function enables administrators to define DHCP options that are carried in the DHCP communication between DHCP server and client or relay agent. The following indicates the format of the DHCP options field.

DHCP Option Format



A code identifies each DHCP option. It can be expressed in value 0 to 255 by user configuration and some of them are predefined in the standards. (128 ~ 254 is site

specific) A length can be variable according to value or can be fixed. A value contains actual information such an IPv6 address, string, or index, which is inserted into the DHCP packet.

Administrators can configure a DHCPv6 option format in *DHCPv6 Option* mode, which is globally used over the DHCP functions.

8.6.4.1 Entering DHCPv6 Option Mode

To enter the DHCPv6 option mode, use the following command.

Command	Mode	Description
ipv6 dhcp option format *NAME*	Global	Enters the DHCPv6 option mode. NAME: DHCPv6 option format name

8.6.4.2 Configuring DHCPv6 Option Format

To configure a DHCPv6 option format, use the following command.

Command	Mode	Description
attr <1-32> **type** <0-255> **length** {<1-256> | **variable**} **value** {**hex** | **index** | **ipv6** | **if_ipv6** | **string**} *VALUE*	DHCPv6 Option	Sets the type, length, and value of an attribute for a DHCPv6 option. attr: They can be made in a DHCPv6 option and are applied in order of attribute value (1-32). type: The type of a value length: The length of a value. It could be a fixed length by user input or a variable length according to the actual value length. value: The actual value of an option
attr <1-32> **type** <0-255> **length-hidden** {<1-256> | **variable**} **value** {**hex** | **index** | **ipv6** | **if_ipv6** | **string**} *VALUE*		
attr <1-32> **length variable value** {**hex** | **index** | **ipv6** | **if_ipv6** | **string**} *VALUE*		Sets the length and value of an attribute for a DHCPv6 option.
attr <1-32> **length** <1-256> **value** {**hex** | **index** | **ipv6** | **if_ipv6** | **string**} *VALUE*		
attr <1-32> **length-hidden variable value** {**hex** | **index** | **ipv6** | **if_ipv6** | **string**} *VALUE*		Sets the value of an attribute for a DHCPv6 option.
attr <1-32> **length-hidden** <1-256> **value** {**hex** | **index** | **ipv6** | **if_ipv6** | **string**} *VALUE*		
no attr <1-32>		Deletes the given attribute.

i

The packets can be mapped to the option format string that defined by variable values with special character (%).

%DEVICE-NAME: device name
%VENDOR-NAME: vendor name
%MODEL-NAME: product model name

%FIRMWARE-VERSION: firmware version
%PORT-NUM: input port number
%IN_IF_IPv6: input interface IPv6 address
%ONT-SERIAL: ONT serial number

8.6.4.3 Deleting DHCPv6 Option Format

To delete a specified DHCPv6 option format, use the following command.

Command	Mode	Description
no ipv6 dhcp option format *NAME*	Global	Deletes the given DHCPv6 option format.

8.6.4.4 Displaying DHCPv6 option

To print a specified DHCPv6 option format, use the following command.

Command	Mode	Description
show ipv6 dhcp option format *NAME*	Enable Global DHCPv6 Option	Shows the information of a given DHCPv6 option format.

8.6.5 Debugging DHCPv6

To enable/disable a DHCPv6 debugging, use the following command.

Command	Mode	Description
debug ipv6 dhcp [**detail**]	Enable	Enables DHCPv6 debugging.
no debug ipv6 dhcp [**detail**]		Disables DHCPv6 debugging.

To display the debugging information, use the following command.

Command	Mode	Description
show debugging ipv6 dhcp	Enable Global Bridge	Shows the debugging information of DHCP.

8.7 Virtual Router Redundancy Protocol (VRRP)

Virtual router redundancy protocol (VRRP) is configuring Virtual router (VRRP Group) consisted of VRRP routers to prevent network failure caused by one dedicated router. You can configure maximum 255 VRRP routers in VRRP group of OLT. First of all, decide which router plays a roll as Master Virtual Router. The other routers will be Backup Virtual Routers. After you give priority to these backup routers, the router serves for Master Virtual Router when there are some problems in Master Virtual router. When you configure VRRP, configure all routers in VRRP with unified Group Id and assign unified Associated IP to them. After that, decide Master Virtual Router and Backup Virtual Router. A router that has the highest priority is supposed to be Master and Backup Virtual Routers also get orders depending on priority.

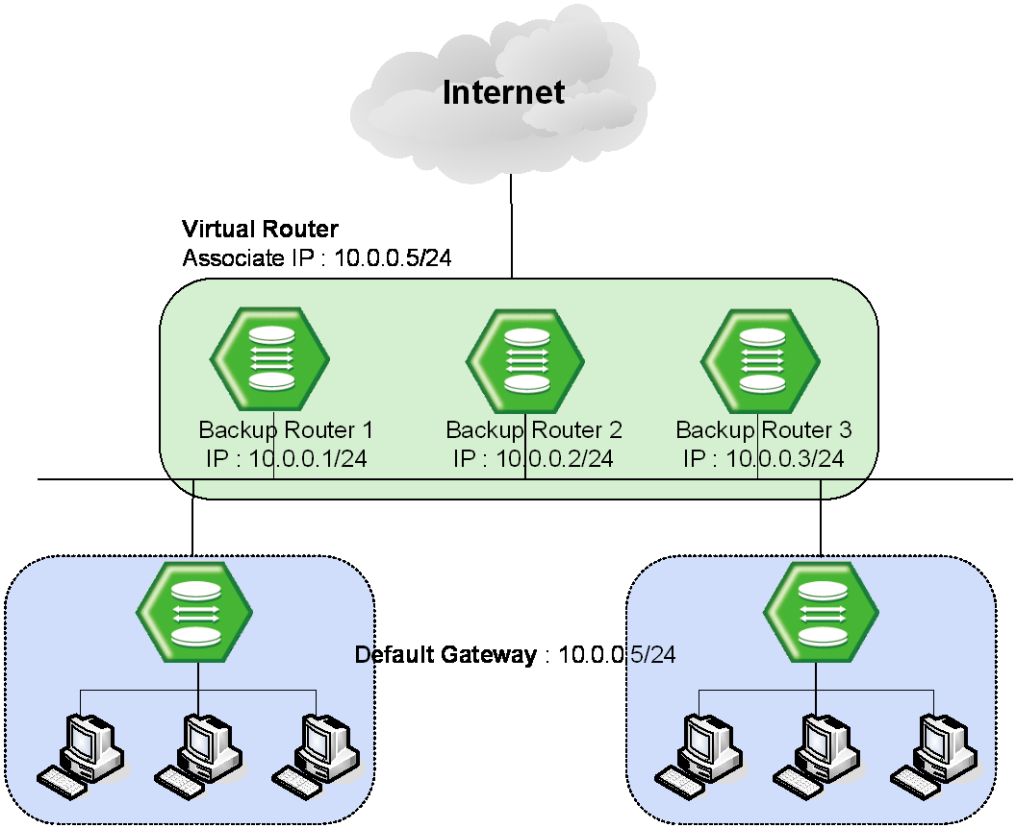


Fig. 8.36 VRRP Operation

In case routers have same priorities, then a router, which has higher IP address, gets the precedence. Fig. 8.36 shows an example of configuring three routers which have IP addresses, 10.0.0.1/24, 10.0.0.2/24 and 10.0.0.3/24 for each one as Virtual router by Associated IP, 10.0.0.5/24. If these three routers have same Priority, a router, which has the highest IP, address, 10.0.0.3/24 is decided to be Master Router. Also, switches and PCs connected to the Virtual Router are to have IP address of Virtual Router, 10.0.0.5/24 as default gateway.

8.7.1 Configuring VRRP

To configure the OLT as device in Virtual Router, use the following command on *Global Configuration* mode. Then you can configure VRRP by opening *VRRP Configuration* mode.

Command	Mode	Description
router vrrp *INTERFACE GROUP-ID*	Global	Configures Virtual Router (VRRP Group). GROUP-ID: 1-255

To delete the VRRP configuration, use the following command.

Command	Mode	Description
no router vrrp {<1-255> | **all**}	Global	Configures Virtual Router (VRRP Group). 1-255: VRRP virtual server ID

8.7.1.1 Associated IP Address

After configuring a virtual router, you need to assign an associated IP address to the virtual router. Assign unified IP address to routers in one group.

To assign an associate IP address to routers to a virtual router or delete a configured associate IP address, use the following command.

Command	Mode	Description
associate *A.B.C.D*	VRRP	Assigns an associated IP address to a virtual router. A.B.C.D: virtual router IP address
no associate {*A.B.C.D* | **all**}		Deletes an assigned associated IP address from a virtual router.

8.7.1.2 Access to Associated IP Address

If you configure the function of accessing Associated IP address, you can access to Associated IP address by the commands such as ping.

To configure the function of accessing Associated IP address, use the following command.

Command	Mode	Description
vip-access	VRRP	Enables the function of accessing associated IP address.
no vip-access		Disables the function of accessing associated IP address.

8.7.1.3 Master Router and Backup Router

The OLT can be configured as Master Router and Backup Router by comparing Priority and IP address of devices in Virtual Router. First of all, it compares Priority. A device, which has higher Priority, is to be higher precedence. And when devices have same Priority, then it compares IP address. A device, which has higher IP address, is to be

higher precedence. If a problem occurs on Master Router and there are more than two routers, one of them is selected as new Master Router according to their precedence.

To configure Priority of Virtual Router or delete the configuration, use the following commands.

Command	Mode	Description
vr-priority <1-254>	VRRP	Configures Priority of Virtual Router.
no vr-priority		Deletes configured Priority of Virtual Router.

i Priority of Virtual Backup Router can be configured from 1 to 254.

To set VRRP advertisement timers or delete the configuration, use the following command.

Command	Mode	Description
vr-timers advertisement <1-10>	VRRP	Sets VRRP timers. 1-10: advertisement time in the unit of second
no vr-timers advertisement		Clears a configured VRRP time.

The following is an example of configuring Master Router and Backup Router by comparing their Priorities: Virtual Routers, Layer 3 SWITCH 1 – 101 and Layer 3 SWITCH 2 – 102. Then, regardless of IP addresses, one that has higher Priority, Layer 3 SWITCH 2 becomes Master Router.

<Layer 3 SWITCH1: IP Address - 10.0.0.1/24>

```
SWTICH1(config)# router vrrp default 1
SWITCH1(config-router)# associate 10.0.0.5
SWITCH1(config-router)# vr-priority 101
SWITCH1(config-router)# exit
SWITCH1(config)# show vrrp

default - virtual router 1
---------------------------------------------
state                        backup
virtual mac address            00:00:5E:00:01:01
advertisement interval          1 sec
preemption                    enabled
priority                      101
master down interval            3.624 sec
 [1] associate address : 10.0.0.5
```

<Layer 3 SWITCH 2: IP Address - 10.0.0.2/24>

```
SWTICH2(config)# router vrrp default 1
SWITCH2(config-router)# associate 10.0.0.5
SWITCH1(config-router)# vr-priority 102
SWITCH2(config-router)# exit
SWITCH2(config)# show vrrp

default - virtual router 1
---------------------------------------------
state                        master
virtual mac address            00:00:5E:00:01:01
advertisement interval          1 sec
preemption                    enabled
priority                      102
master down interval            3.620 sec
 [1] associate address : 10.0.0.5
```

SWITCH 2 with higher priority is configured as Master.

By default, Priority of the OLT is configured as “100”. Therefore, unless you configure specific Priority, this switch becomes Master Router because a device, which has lower IP address, has higher precedence.

Also, when there are more than two Backup Routers, IP addresses are compared to decide order. The following is an example of configuring Master Router and Backup Router by comparing IP addresses: Virtual Routers, Layer 3 SWITCH 1 – 10.0.0.1 and Layer 3 SWITCH 2 – 10.0.0.2.

<Layer 3 SWITCH1: IP address - 10.0.0.1/24>

```
SWTICH1(config)# router vrrp default 1
SWITCH1(config-router)# associate 10.0.0.5
SWITCH1(config-router)# exit
SWITCH1(config)# show vrrp

default - virtual router 1
---------------------------------------------
state                          master
virtual mac address              00:00:5E:00:01:01
advertisement interval            1 sec
preemption                      enabled
priority                        100
master down interval              3.624 sec
 [1] associate address : 10.0.0.5
```

<Layer 3 SWITCH 2: IP Address - 10.0.0.2/24>

```
SWTICH2(config)# router vrrp default 1
SWITCH2(config-router)# associate 10.0.0.5
SWITCH2(config-router)# exit
SWITCH2(config)# show vrrp

default - virtual router 1
---------------------------------------------
state                          backup
virtual mac address              00:00:5E:00:01:01
advertisement interval            1 sec
preemption                      enabled
priority                        100
master down interval              3.620 sec
 [1] associate address : 10.0.0.5
```

In case of same priorities, SWITCH 1 with higher IP address is configured as Master.

8.7.1.4 VRRP Track Function

When the link connected to Master Router of VRRP is off as below, if link of Master Router is not recognized, the users on the interface are not able to communicate because the interface is not able to access to Master Router.

In the condition that Link to VRRP's master router is down as the figure shown below, or the link of Master Router cannot be recognized, the communication would be impossible.

For the OLT, you can configure Master Router to be changed by giving lower Priority to Master Router when the link of Master Router is disconnected. This function is VRRP Track.

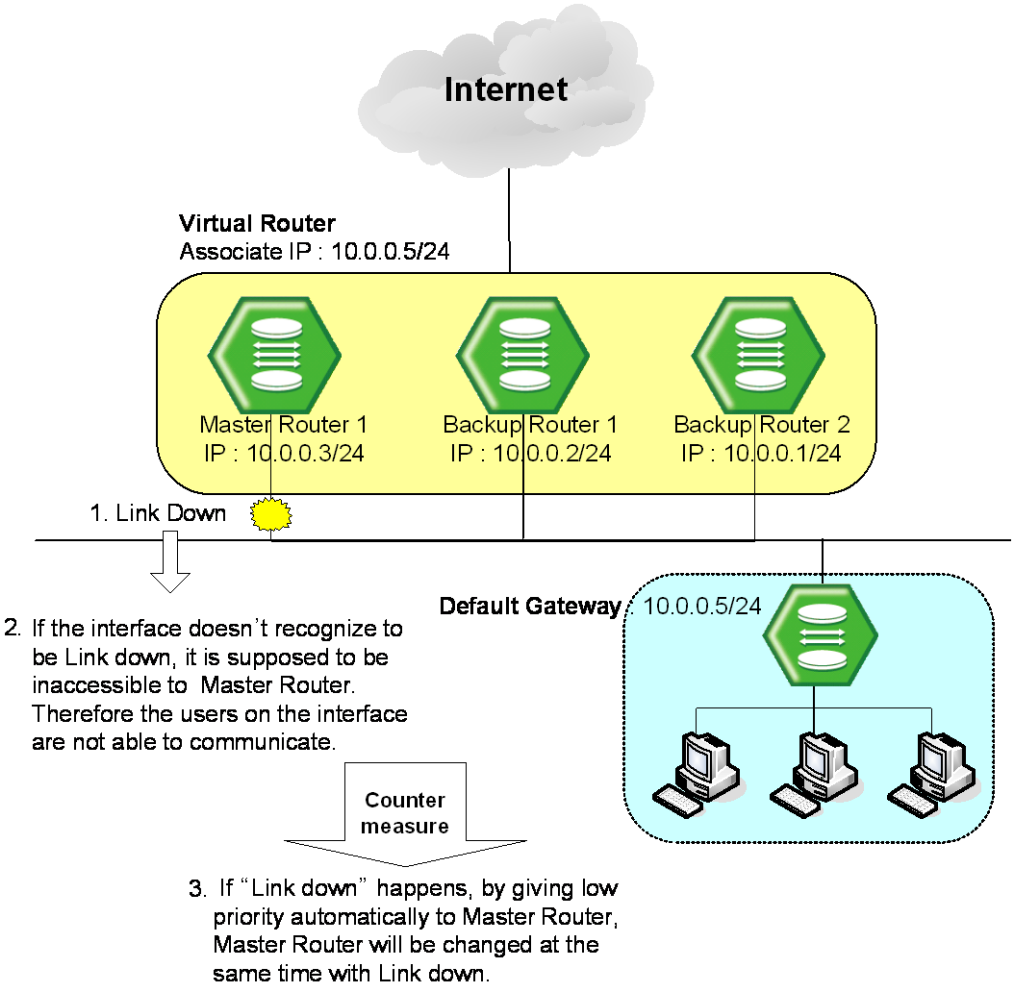


Fig. 8.37 VRRP Track

To configure VRRP Track, use the following command.

Command	Mode	Description
track interface *INTERFACE* **priority** <1-254>	VRRP	Enables the interface tracking and decreases the VRRP priority as the track results.

To release VRRP Track configuration, use the following command.

Command	Mode	Description
no track interface *INTERFACE*	VRRP	Disables the interface tracking and deletes a specified priority.

8.7.1.5 Authentication Password

If anyone knows Group ID and Associated IP address, he can configure another device as a Virtual Router. To prevent this, user needs to configure a password, named authentication password that can be used only in Virtual Router user configured.

To configure an authentication password for security of Virtual Router, use the following command on VRRP configuration mode.

Command	Mode	Description
authentication clear_text *PASSWORD*	VRRP	Configures an authentication password.
no authentication		Deletes a configured authentication password.

i Authentication password can be configured with maximum 7 digits.

The following is an example of configuring Authentication password in Virtual Router as network and showing it.

```
SWITCH(config-vrrp)# authentication clear_text network
SWITCH(config-vrrp)# show running-config
Building configuration...
(Omitted)
vrrp default 1
 authentication clear_text network
 associate 10.0.0.5
no snmp
SWITCH(config-vrrp)#
```

8.7.1.6 Preempt

Preempt is a function that an added device with the highest Priority user gave is automatically configured as Master Router without rebooting or specific configuration.

To configure Preempt, use the following command.

Command	Mode	Description
preempt	VRRP	Enables Preempt. (default: enable)
preempt delay <1-3600>		Specifies the number of seconds the router delays before issuing an advertisement claiming virtual IP address ownership to be the master router.

To disable Preempt and return to as default setting of delay time, use the following command.

Command	Mode	Description
no preempt	VRRP	Deletes the former configuration of Preempt to enable it.
no preempt delay		Returns to the default setting.

8.7.2 VRRP Monitoring and Management

You can view all kinds of statistics and database recorded in IP routing table. The information can be used to enhance system utility and solve problem in case of trouble. You can check network connection and data routes through the transmission.

8.7.2.1 Displaying VRRP Protocol Information

To display a configuration of VRRP, use the following command.

Command	Mode	Description
show vrrp	Enable Global VRRP	Shows current configuration of VRRP. VRID: VRRP virtual server id (1-255)
show vrrp vrid {*VRID* | **all**}		
show vrrp interface {*INTERFACE* | **all**}		Shows current configuration of specified interface VRRP or all interfaces.
show ipv6 vrrp	Enable Global Bridge	Shows current configuration of IPv6 VRRP.

8.7.2.2 VRRP Statistics

To display the VRRP statistics that packets have been sent and received, use the following command.

Command	Mode	Description
show vrrp stat	Enable Global Bridge VRRP	Shows statistics of packets in Virtual Router Group.

To clear the VRRP statistics information, use the following command.

Command	Mode	Description
clear vrrp stat	Enable Global Bridge VRRP	Clears statistics of packets in Virtual Router Group.

8.7.2.3 VRRP Debug

To enable VRRP debugging, use the following command.

Command	Mode	Description
debug vrrp [**all**]	Enable	Enables VRRP debugging. all: all VRRP debugging
debug vrrp nsm [**interface** | **bfd**]		Enables VRRP debugging. nsm: NSM notifications debugging interface: interface information bfd: BFD detection
debug vrrp packet [**send** | **recv** | **detail**]		Enables VRRPv2 packets debugging. packet: VRRPv2 packets send: outgoing packets recv: incoming packets detail: detail information
debug vrrp sm [**events** | **status** | **timers**]		Enables VRRP state machine debugging. sm: state machine events: SM events status: SM status timers: SM timers

To disable VRRP debugging, use the following command.

Command	Mode	Description
no debug vrrp [**all**]	Enable	Disables VRRP debugging.
no debug vrrp nsm [**interface** | **bfd**]		
no debug vrrp packet [**send** | **recv** | **detail**]		
no debug vrrp sm [**events** | **status** | **timers**]		

To display the debugging information, use the following command.

Command	Mode	Description
show debugging vrrp	Enable Global VRRP	Shows the debugging information of VRRP.

8.8 Rate Limit

User can customize port bandwidth according to user's environment. By this configuration, you can prevent a certain port to monopolize whole bandwidth so that all ports can use bandwidth equally. Egress and ingress can be configured both to be same and to be different.

The OLT can apply the rate limit with 64 Kbps unit for GE port, and support ingress policing and egress shaping.

To set a rate limit for ports, use the following command.

Command	Mode	Description
rate-limit port *PORTS* **rate** *RATE* {**egress** | **ingress dot3x**}	Bridge	Sets a rate limit for ports. If you input egress or ingress, you can configure outgoing packet or incoming packet. The unit is 64 Kbps.
no rate-limit port *PORTS* {**egress** | **ingress dot3x**}		Clears a specified rate limit for port.

For the ingress rate limit, the flow control should be enabled on a specified port! For more information of the flow control, see Section 5.1.5.

To display a configured rate limit, use the following command.

Command	Mode	Description
show rate-limit	Enable Global Bridge	Shows a configured rate limit.

8.9 Flood Guard

Flood guard limits number of packets, how many packets can be transmitted, in configured bandwidth, whereas Rate limit controls packets through configuring width of bandwidth, which packets pass through. This function prevents receiving packets more than configured amount without enlarging bandwidth.

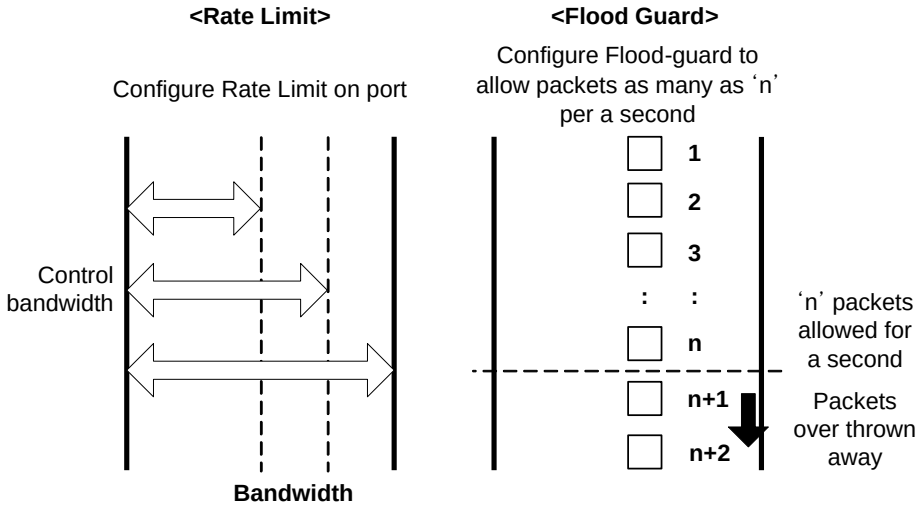


Fig. 8.38 Rate Limit and Flood Guard

8.9.1 MAC Flood Guard

MAC flood guard controls the number of incoming packets per second, which have the same MAC address. Using this function, you can protect malicious attacks such as Denial of Service (DoS) from unauthorized user.

To configure the MAC flood guard, use the following command.

Command	Mode	Description
mac-flood-guard *PORTS* <1-6000>	Bridge	Enables the MAC flood guard on a port by specifying the number of incoming packets with the same MAC address per second. PORTS: port number 1-6000: the number of packets per second
no mac-flood-guard [*PORTS*]		Disables the MAC flood guard.

To display the configured MAC flood guard, use the following command.

Command	Mode	Description
show mac-flood-guard	Enable Global Bridge	Shows the configured MAC flood guard.
show mac-flood-guard macs		Shows the MAC addresses blocked by the MAC flood guard.

Occasionally, unknown unicast or multicast traffic is flooded to a switch port because a MAC address has timed out or has not been learned by the switch.

To disable the flooding of multicast and unicast packets to an interface, use the following command.

Command	Mode	Description
port flood-block *PORTS* **bcast**	Bridge	Blocks Broadcast forwarding to the port.
port flood-block *PORTS* **dlf**		Blocks DLF forwarding to the port.

To flood the multicast and unicast packets to an interface, use the following command.

Command	Mode	Description
no port flood-block *PORTS* **bcast**	Bridge	Floods Broadcast forwarding to the port.
no port flood-block *PORTS* **dlf**		Floods DLF forwarding to the port.

To display the configured flood blocking, use the following command.

Command	Mode	Description
show port flood-block	Enable Bridge	Shows the configured flood blocking.

8.9.2 CPU Flood Guard

CPU flood guard controls the number of broadcast and multicast packets per second, which is coming to CPU to prevent CPU overload. If the number of those packets exceeds the threshold, the system generates an SNMP trap.

To enable/disable the CPU flood guard, use the following command.

Command	Mode	Description
cpu-flood-guard {**enable** | **disable**}	Bridge	Enables/disables the CPU flood guard.

To specify the number of broadcast and multicast packets per second, which is coming to CPU, use the following command.

Command	Mode	Description
cpu-flood-guard *PORTS* <1-6000>	Bridge	Specifies the number of broadcast and multicast packets toward CPU per second. PORTS: port number 1-6000: the number of packets per second
no cpu-flood-guard [*PORTS*]		Deletes a specified number of packets.

You can also enable the blocking option. When the blocking option for CPU flood guard is running, if the number of incoming broadcast and multicast packets per second exceeds a configured value, the port will discard those packets during a specified time.

To enable the blocking option, use the following command.

Command	Mode	Description
cpu-flood-guard *PORTS* **timer** <10-3600>	Bridge	Enables the blocking option. PORTS: port number 10-3600: blocking time (unit: second)
cpu-flood-guard *PORTS* **unblock**		Forces the state of a blocked port to change to NORMAL.

To display the configured CPU flood guard, use the following command.

Command	Mode	Description
show cpu-flood-guard	Enable Global Bridge	Shows the configured CPU flood guard.

8.9.3 System Flood Guard

A packet flooding occurs unexpectedly when a large number of broadcast or multicast packets are received on a port, which may cause unnecessary network congestion. OLT provides the system flood guard function that controls traffic for a port by given threshold. If the number of incoming packets exceeds the threshold, the system generates a syslog message/SNMP trap or discards those packets.

To enable/disable the system flood guard, use the following command.

Command	Mode	Description
system-flood-guard {**enable** | **disable**}	Bridge	Enables/disables the system flood guard.

To specify the number of packets per second according to the type of packets, which is transmitted to a specific port, use the following command.

Command	Mode	Description
system-flood-guard *PORTS* { **multicast**| **broadcast** | **both**} <1-2147483647> **block**	Bridge	Specifies the number of incoming packets to a port per second according to the packets' type. Discards the packets which exceeds given threshold. PORTS: port number 1-2147483647: the number of packets per 1 second
no system-flood-guard [*PORTS*]		Deletes a specified number of packets.

To generate the trap message when the number of incoming packets is less than a configured value, use the following command.

Command	Mode	Description
system-flood-guard *PORTS* { **multicast**| **broadcast** | **both**} <1-2147483647> **unblock**	Bridge	Enables the system to display a trap message when the number of incoming packets per second is less than the threshold. PORTS: port number

		1-2147483647: the number of packets per 1 second

You can also enable the blocking option. When the blocking option for system flood guard is running, if the number of incoming packets per second exceeds a configured value, the port will discard those packets during a specified time.

To set an expire time for blocked port, use the following command.

Command	Mode	Description
system-flood-guard *PORTS* **timer** <10-3600>	Bridge	Enables the blocking option. 10-3600: blocking time (default:60, unit: second)

To disable the blocking option for the blocked port to permit the packet transmission, use the following command.

Command	Mode	Description
system-flood-guard *PORTS* **unblock**	Bridge	Disables the blocking option.

To display the configured system flood guard, use the following command.

Command	Mode	Description
show system-flood-guard	Enable Global Bridge	Shows the configured system flood guard.

i BPDU is still transmitted even if the specific port is blocked by system flood guard.

8.9.4 Invalid Traffic Guard

A packet storm may occur unexpectly if a large number of invalid packets are received on a port. It can cause the network to slow down or to time out. The OLT provides the traffic guard function that controls the port's traffic by threshold value. The threshold (%) rate is based on the number of packets per second (pps). Basically, a maximum pps is usually calculated when all Ethernet frames are of 64-bytes in length, or the minimum size frame. Because of the Inter-Packet Gap (12 bytes) and preamble (8 bytes), the minimum packet size becomes 84 bytes.

The following table shows the performance numbers in packets per second (pps) for 100M, 1G and 10G Ethernet port.

Port Speed	Bytes/second	PPS for 64-byte	PPS for 1518-byte
100M Port	12,500,000	148,809	8,234
1G Port	125,000,000	1,488,095	82,345

10G Port	1,250,000,000	14,880,952	823,451

The invalid traffic guard function is configured with the threshold rate (%) that is based on pps of the maximum Ethernet port's bandwidth.

	Frame size for PPS calculation	Packet Type which are counted	Threshold Rate (%) based on PPS
Attack-guard	64-byte	Multicast, Unicast, Broadcast	1G port: 100% (=1,488,095 pps) 10G port: 100% (=14,880,952 pps) Default: High-80%, Low-20%
Error-guard	64-byte	Error packets	1G port: 100% (=1,488,095 pps) 10G port: 100% (=14,880,952 pps) Default: 1%

i To generate a SNMP trap of invalid traffic guard (attack/error), SNMP trap mode should be "alarm-report" mode.

8.9.4.1 Attack Guard

A packet storm may unexpectedly occur if a large number of broadcast, unicast, or multicast packets are received on a port. Forwarding these packets can cause the network to slow down or to time out. The OLT provides the attack guard function that controls traffic for a specified port by threshold value. The threshold (%) rate of attack guard is based on the number of packets per second (pps) that is calculated by 64-byte frame size. If the number of incoming packets exceeds a given threshold, the system can shut down the port or generate SNMP trap messages for warning when attack guard function is enabled on this port. If the threshold (%) comes down to a given low threshold, it generates traps. You can specify the packet type, a high threshold value and a low threshold for a port.

To enable/disable the attack guard function, use the following command.

Command	Mode	Description
attack-guard {**broadcast** | **multicast** | **unicast**} <0-100> <0-100> [*PORTS*]	Bridge	Enables the attack guard function according to its packet type and sets the threshold. PORTS: port number 0-100: high rate threshold percent (default: 80%) 0-100: low rate threshold percent (default: 20%)
no attack-guard {**broadcast** | **multicast** | **unicast**} [*PORTS*]		Disable the attack guard function.

i If the high threshold is set to 85% for 1G Ethernet port, the OLT monitors the number of configured packet type. The number of those packets exceeds 1,264,880 pps (=14,880,95 * 0.85), the shutdown/trap action will be performed.

To determine the policy to take action when the incoming broadcast/multicast/unicast

packets exceed the configured threshold, use the following command.

Command	Mode	Description
attack-guard action shutdown [*PORTS*]	Bridge	Shuts down the port if the amount of traffic exceeds a high threshold.
attack-guard action trap [*PORTS*]		Generates a trap message when the amount of traffic exceeds a high threshold.
no attack-guard action {**shutdown** | **trap** } [*PORTS*]		Disables the shutdown action or trap action on a port when the attack guard function is enabled.

To display the attack guard configuration, use the following command.

Command	Mode	Description
show attack-guard	Enable Global Bridge	Displays the attack guard configuration.

8.9.4.2 Error Guard

A packet storm may unexpectedly occur if a large number of error packets (CRC, FCS, alignment and bad symbols) are received on a port. These packets can cause unexpected errors of the whole network environment connected to the switch as well as one single switch.

The OLT provides error guard function that controls incoming error packets through the port using the threshold. The threshold rate (%) is based on pps of 64-byte frame size calculation within the maximum port bandwidth. If the number of incoming packets per second exceeds the given threshold, the system shuts down the port or generates trap messages for warning when the error guard function is enabled on this port.

To enable/disable the error guard function, use the following command.

Command	Mode	Description
error-guard <0-100> [*PORTS*]	Bridge	Enables the error guard function and sets its threshold. PORTS: port number 0-100: high rate threshold percent (default: 1%)
no error-guard [*PORTS*]		Disables the error guard function.

i The threshold (%) rate of Error Guard is based on 64-byte frame size calculation. If the high threshold is set to 5% for 10G Ethernet port, the OLT monitors the error packet count. The number of those packets exceeds 744,048 pps (=14,880,952 * 0.05), the shutdown/trap action will be performed.

To determine the policy to take action when the incoming error packets exceed the configured threshold, use the following command.

Command	Mode	Description

error-guard action shutdown [*PORTS*]	Bridge	Performs port blocking if the amount of error packets exceeds a high threshold.
error-guard action trap [*PORTS*]		Generates a trap message when the amount of error packets exceeds a high threshold.
no error-guard action {**shutdown** | **trap** } [*PORTS*]		Deletes the policy to take action when the incoming error packets exceed the configured threshold.

To display the error guard configuration, use the following command.

Command	Mode	Description
show error-guard	Enable Global Bridge	Displays the error guard configuration.

8.10 PPS Control

A packet storm occurs unexpectedly when a large number of broadcast, unicast, or multicast packets are received on a port, which may cause unnecessary network congestion. The OLT provides the PPS control function that controls traffic for a port by given threshold. If the number of incoming packets exceeds the threshold, the system generates a syslog message and SNMP trap.

To set the threshold for PPS control, use the following command.

Command	Mode	Description
pps-control port *PORTS THRESHOLD* {**5** | **60** | **600**}	Global	Sets the threshold for PPS control. PORTS: port number THRESHOLD: number of packets per second (pps) 5 | 60 | 600: time interval (unit: second)
no pps-control port *PORTS*		Deletes the configured threshold for PPS control.

When the blocking option for PPS control is running, if the number of incoming packets exceeds a configured threshold, the traffic is discarded during specified time.

To enable the blocking option, use the following command.

Command	Mode	Description
pps-control port *PORTS* **block timer** <10-3600>	Global	Enables the blocking option. PORTS: port number 10-3600: blocking time (unit: second)
no pps-control port *PORTS* **block**		Disables the blocking option.

To display current incoming packet statistics and configurations for PPS control, use the following command.

Command	Mode	Description
show pps-control port [*PORTS*]	Enable Global Bridge	Shows current incoming packet statistics and configurations for PPS control.

8.11 Storm Control

The OLT provides a storm control feature for mass broadcast, multicast, and destination lookup failure (DLF). Generally, wrong network configuration, hardware malfunction, virus and so on cause these kinds of mass packets. Packet storm occupies most of the bandwidth of the network, and that causes the network to become very unstable.

To enable/disable the storm control, use the following command.

Command	Mode	Description
storm-control {**broadcast** | **multicast** | **dlf**} *RATE* [*PORTS*]	Bridge	Enables broadcast, multicast or DLF storm control respectively in a port with a user defined rate. RATE: unit: Packet/s, range: FE(0-262142), GE(0-2097150)
no storm-control {**broadcast** | **multicast** | **dlf**} [*PORTS*]		Disables broadcast, multicast or DLF storm control respectively.

i By default, DLF storm control is enabled and multicast storm control is disabled.

To display a configuration of the storm control, use the following command.

Command	Mode	Description
show storm-control	Bridge	Displays a configuration of the storm control.

8.12 Jumbo Frame Capacity

The packet range that can be capable to accept is from 64 bytes to 1518 bytes. Therefore, packets not between these ranges will not be taken. However, the OLT can accept jumbo frame larger than 1518 bytes through user's configuration.

To enable/disable the jumbo frame capacity, use the following command.

Command	Mode	Description
jumbo-frame *PORTS* <1518-12288>	Bridge	Configures to accept jumbo frame between specified ranges. (default: 1518)
no jumbo-frame *PORTS*		Disables configuration to accept jumbo frame on specified port.

To display the configuration of jumbo frame, use the following command.

Command	Mode	Description
show jumbo-frame	Enable Global Bridge	Shows a configuration of jumbo frame.

8.13 Configuring PPPoE Tag Option Format

PPP over Ethernet (PPPoE) provides the ability to connect a network of hosts over a simple bridging access device to a remote Access Concentrator (AC). By using PPPoE with vendor tag, switch in the host network can include the additional information about itself before sending PPPoE packets to the AC.

8.13.1 PPPoE Vendor Tag Option

8.13.1.1 Entering PPPoE Vendor Tag Option Mode

To enter the PPPoE vendor tag option mode, use the following command.

Command	Mode	Description
pppoe tag-format *NAME*	Global	Enters the PPPoE vendor tag option mode. NAME: PPPoE vendor tag option format name

8.13.1.2 Configuring PPPoE Vendor Tag Option Format

To configure a PPPoE vendor tag option format, use the following command.

Command	Mode	Description
attr <1-32> **type** <0-255> **length** <1-128> | **variable**} **value** {**hex** | **index** | **ip** | **string** | **tag-format**} *VALUE*	PPPoE Option	Sets the type, length, and value of an attribute for a PPPoE Vendor Tag option. attr: They can be made in a PPPoE vendor tag option and are applied in order of attribute value (1-32). type: The type of a value length: The length (size) of a value field. It could be a fixed length by user input or a variable length according to the actual value length. 1-128: 1 to 128 bytes fixed length (size) of the value field value: The actual value of an option.
attr <1-32> **type** <0-255> **length-hidden** <1-128> **value** {**hex** | **index** | **ip** | **string** | **tag-format** } *VALUE*		
attr <1-32> **length variable value** {**hex** | **index** | **ip** | **string** | **tag-format** } *VALUE*		Sets the length and value of an attribute for a PPPoE Vendor Tag option.
attr <1-32> **length** <1-128> **value** {**hex** | **index** | **ip** | **string** | **tag-format** } *VALUE*		
attr <1-32> **length-hidden variable value** {**hex** | **index** | **ip** | **string** | **tag-format** } *VALUE*		Sets the value of an attribute for a PPPoE vendor tag option.
attr <1-32> **length-hidden** <1-128> **value** {**hex** | **index** | **ip** | **string** | **tag-format** } *VALUE*		
no attr <1-32>		Deletes the given attribute.

i The packets can be mapped to the option format string that defined by variable values

with special character (%).

%FRAME: frame (chassis) number for receiving PPPoE packets
%SLOT: slot number for receiving PPPoE packets
%PORT: port number for receiving PPPoE packets
%VID: VLAN ID tagged on packets
%IN VID: inner VLAN ID
%BANDWIDTH: bandwidth
%MGMT IP: MGMT interface's IP address
%HOST NAME: host name
%IN_IF_IP: input interface IP address
%REAL_PORT: port number (slot#/port#)
%CPU-MAC: system MAC address
%ONU-ID: ONU ID
%ONU_PORT_NUM: ONU's UNI port number
%ONU_DESCRIPTION: ONU description written by administrator
%ONU_PORT_DESCRIPTION: ONU port description written by administrator
%ONU_SERIAL_NUM: ONU's serial number
%BLANK: blank

8.13.1.3 Deleting PPPoE Vendor Tag Option Format

To delete the given PPPoE vendor tag option format, use the following command.

Command	Mode	Description
no pppoe tag-format *NAME*	Global	Deletes the given PPPoE vendor tag option format.

8.13.1.4 Displaying PPPoE Vendor Tag option

To display the specified PPPoE vendor tag option format, use the following command.

Command	Mode	Description
show pppoe tag-format *NAME* [**port** *PORT* **vlan** *VLANS*]	Enable Global PPPoE Option	Shows information about the PPPoE vendor tag format. NAME: PPPoE vendor tag format name

8.13.2 PPPoE Vendor Tag Filtering

8.13.2.1 PPPoE Snooping Mode

To enable/disable PPPoE snooping, use the following command.

Command	Mode	Description
pppoe snooping	Global	Enables PPPoE snooping function.
no pppoe snooping		Disables PPPoE snooping function.

8.13.2.2 Configuring PPPoE Vendor Tag Filtering

The PPPoE filter will decide the way that PPPoE packet is forwarded. Each filter has a unique filter ID. This ID is also used as a priority. The filter having the highest priority will be chosen. The filter can be applied for all ports in switch or some specific ports, all VLANs or some specific VLAN IDs, and chose action drop or permit.

To create a PPPoE packet filter and define the filter, use the following command.

Command	Mode	Description
flt-id <1-16> **port** {**any** | *PORTS*} **vid** {**any** | *VLANS*} **action** {**drop** | **permit**}	PPPoE Snooping	Creates a PPPoE filter ID and selects a port number, VLAN ID and filter action policy (drop/permit). 1-16: PPPoE filter ID
no flt-id <1-16>		Removes the configured PPPoE filter ID.

PPPoE tag operation is the action applied on the PPPoE tag field of the permitted PPPoE packet. The tag operation has lower priority than filter action and can select one action from remove, keep, add, update and replace.

To set the tag operation which will be applied to the PPPoE vendor tag field of the permitted PPPoE packets, use the following command.

Command	Mode	Description
tag-opr-id <1-16> **type** *CODE* **port** {**any** | *PORTS*} **vid** {**any** | *VLANS*} **action** {**remove** | **keep** | **add** | **update** | **replace**} **format** *NAME*	PPPoE Snooping	Specifies a PPPoE tag operation on a port and VLAN. 1-16: tag operation ID CODE: PPPoE Vendor tag type code (e.g. 0x0105 for Vendor-specific) remove: Remove the vendor tag from the PPPoE packets. keep: Keep the vendor tag in the PPPoE packets. add: Add the vendor tag the PPPoE packet if it is not existed. update: Update or add the vendor tag to PPPoE packet regardless of the existence of the tag. replace: Replace the vendor tag if it exist. NAME: PPPoE vendor tag format name
no tag-opr-id <1-16>		Removes the PPPoE tag operation.

8.13.3 PPPoE Debug

To enable debugging of all PPPoE or a specific feature of PPPoE, use the following command.

Command	Mode	Description
debug pppoe { **all** | **func** | **pkt** }	Enable	Enables PPPoE debugging. all: all PPPoE features func: PPPoE function pkt: PPPoE packet
no debug pppoe { **all** | **func** |		Disables PPPoE debugging.

pkt }		

To display the debugging status of PPPoE, use the following command.

Command	Mode	Description
show debugging pppoe	Enable Global	Shows the debugging status of PPPoE.

8.14 Bandwidth

Routing protocol uses bandwidth information to measure routing distance value. To configure bandwidth of interface, use the following command.

Command	Mode	Description
bandwidth *BANDWIDTH*	Interface	Configures bandwidth of interface. BANDWIDTH: 1-10000000 (unit: kbit)
no bandwidth *BANDWIDTH*		Deletes configured bandwidth of interface.

i This bandwidth is valid only for forwarding routing information and it does not concern any physical bandwidth.

8.15 Maximum Transmission Unit (MTU)

MTU is the largest packet size that can be sent over a network. You can set a maximum transmission unit (MTU) with below command.

Command	Mode	Description
mtu <68-12270>	Interface	Sets a MTU size.
no mtu		Returns to the default MTU size.

8.16 Blocking Packet Forwarding

RFC 2644 recommends that system blocks broadcast packet of same network bandwidth with interface of equipment, namely direct broadcast packet. Hereby, OLT is supposed to block direct broadcast packet by default setting. However, you can enable or disable it in OLT.

To block direct broadcast packet, use the following command.

Command	Mode	Description
no ip forward direct-broadcast	Global	Enables blocking Direct broadcast packet. (Default)
ip forward direct-broadcast		Disables blocking Direct broadcast packet.

To block the destination lookup failure (DLF) packets, use the following command.

Command	Mode	Description
no ip forward dlf	Global	Enables blocking DLF packets. (default)
ip forward dlf		Disables blocking DLF packets.

9 IP Multicast

IP communication provides three types of packet transmission: unicast, broadcast and multicast. Unicast is the communication for a single source host to a single destination host. This is still the most common transmission form in the IP network. Broadcast is the communication for a single source host to all destination hosts on a network segment. This transmission is also widely used especially by network protocols, but it sometimes may not be efficient for those hosts in the subnet who are not participating in the broadcast. Multicast is the communication for a single or many source hosts to a specific group of destination hosts, which is interested in the information from the sources. This type of packet transmission can be deployed for a number of applications with more efficient utilization of the network infrastructure.

The point of implementing multicast is how to deliver source traffic to specific destinations without any burden on the sources or receivers using the minimized network bandwidth. The solution is to create a group of hosts with addressing the group, and to let the network determine how to replicate the source traffic to the receivers. The traffic will then be addressed to the multicast address and replicated to the multiple receivers by network devices. Standard multicast protocols such as IGMP and PIM provides most of these capabilities.

IP multicast features on the OLT consist of the group membership management, Layer 2 multicast forwarding, and Layer 3 multicast routing, which allow network administrators to successfully achieve the effective and flexible multicast deployment.

Fig. 9.1 shows an example of the IP multicast network. In this case, the OLT is configured only with IGMP snooping (L2 multicast forwarding feature) in the Layer 2 network.

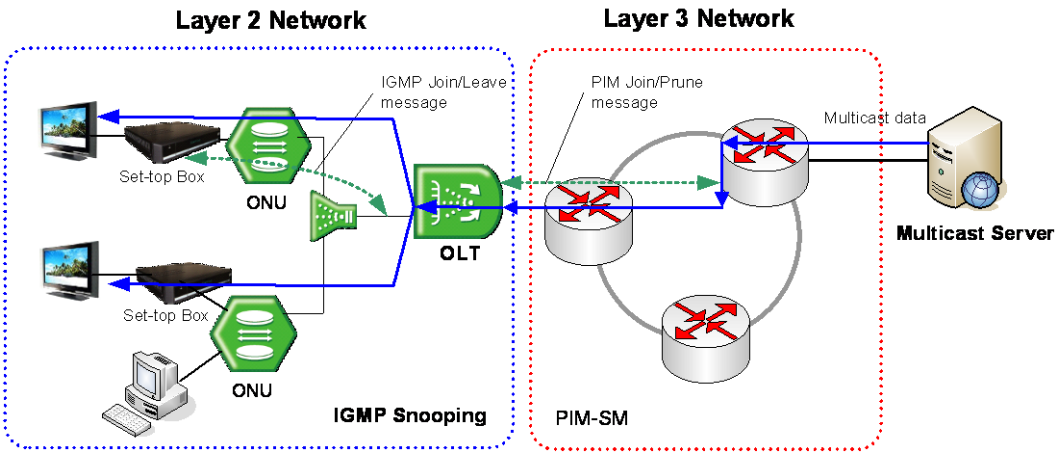


Fig. 9.1 The OLT with IGMP Snooping

IP Multicast to Ethernet/FDDI MAC Address Mapping

All IP multicast frames use MAC layer addresses beginning with the 24-bit prefix of 0x0100.5Exx.xxxx. With only half of these MAC addresses available for use by IP Multicast, 23 bits of MAC address space are available for mapping L3 IP multicast addresses into L2 MAC addresses.

As there are 28 bits (32 – 4 Class D prefix) of unique address space for an IP multicast address and only 23 bits are mapped into the MAC address, there are 5 bits of overlap (28 – 23). These 5 bits represent 25 = 32 addresses. Therefore, there is a 32:1 overlap of IP addresses to MAC addresses – 32 IP multicast addresses are mapped to the same MAC multicast address. As an example, below lists all the IP multicast addresses that are mapped to the same MAC multicast address of 0x0100.5E01.0101.

224.1.1.1	225.1.1.1	226.1.1.1	227.1.1.1	228.1.1.1
229.1.1.1	230.1.1.1	231.1.1.1	232.1.1.1	233.1.1.1
234.1.1.1	235.1.1.1	236.1.1.1	237.1.1.1	238.1.1.1
239.1.1.1	224.129.1.1	225.129.1.1	226.129.1.1	227.129.1.1
228.129.1.1	229.129.1.1	230.129.1.1	231.129.1.1	232.129.1.1
233.129.1.1	234.129.1.1	235.129.1.1	236.129.1.1	237.129.1.1
238.129.1.1	239.129.1.1			

i

The 32:1 address mapping ambiguity can lead to over subscription problem at hosts. You must consider it when you allocate IP multicast addresses for network applications to prevent unexpected behavior.

9.1 Multicast Group Membership

The most important implementation of the multicast is the group membership management. The multicast group membership allows a router to know which host is interested in receiving the traffic from a certain multicast group and to forward the multicast traffic corresponding to the group to that host. Even if there is more than one host interested in the group, the router forwards only one copy of the traffic stream to minimize the use of network bandwidth.

Internet Group Management Protocol (IGMP) is a protocol used by routers and hosts to manage the multicast group membership. Using IGMP, hosts express an interest in a certain multicast group, and routers maintain the multicast group membership database by collecting the interests from the hosts.

The OLT supports IGMP version 1, 2, and 3 each defined in RFC 1112, 2236, and 3376.

9.1.1 IGMP Basic

Internet Group Management Protocol (IGMP) manages the host membership in multicast groups. The hosts inform a neighboring multicast router that they are interested in receiving the traffic from a certain multicast group by sending the membership report (join a group). The router then forwards the multicast traffic corresponding to the report to the hosts.

A multicast router called as a querier is responsible for keeping track of the membership state of the multicast groups by sending periodic general query messages to current interested hosts. If there are no responses to the query from the hosts for a given time (leave a group), the router then stops forwarding the traffic. During the above transaction between hosts and routers, they are using IGMP messages to report or query the group membership.

IGMP has three versions that are supported by hosts and routers. The followings are the simple definitions of each version:

- **IGMP Version 1**
  The basic query-response mechanism for the group membership management is introduced. Routers, however, should use the timeout-based mechanism to discover members with no longer interests in the groups since there is no leave process.
- **IGMP Version 2**
  IGMP messages such as leave group and specific-group query are added for the explicit leave process. This process greatly reduces the leave latency compared to IGMP version 1. Unwanted and unnecessary traffic can be constrained much faster.
- **IGMP Version 3**
  The source filtering is supported. That is, hosts now can join a group with specifying including/excluding a set of sources, allowing supporting the source-specific multicast (SSM). It also increases the multicast address capability, and enhances the security from unknown multicast sources.

9.1.1.1 IGMP Version

By default, the OLT runs IGMP version 3. To change the IGMP protocol version on a current interface, use the following command.

Command	Mode	Description
ip igmp version <1-3>	Interface	Sets an IGMP version on a current interface. 1-3: IGMP version (default: 3)
no ip igmp version		Sets to the default setting.

i Routers running different versions of IGMP negotiate the lowest common version of IGMP that is supported by hosts on their subnet and operate in that version.

9.1.1.2 Querier's Robustness Variable

You can statically configure the Querier's Robustness Variable (QRV) field in the membership query message for IGMP version 2 and 3. The QRV allows tuning for the expected packet loss on a network. If a network is expected to be lossy, the QRV value may be increased. When receiving the query message that contains a certain QRV value from a querier, a host returns the report message as many as the specified QRV value.

To configure the QRV value on an interface, use the following command.

Command	Mode	Description
ip igmp robustness-variable <2-7>	Interface	Configures the Querier's Robustness Variable (QRV) value on an interface. (default: 2)
no ip igmp robustness-variable		Deletes a specified QRV value.

9.1.1.3 Clearing IGMP Entry

To clear IGMP entries, use the following command.

Command	Mode	Description
clear ip igmp	Enable Global	Deletes all IGMP entries.
clear ip igmp interface *INTERFACE*		Deletes the IGMP entries learned from a specified interface. INTERFACE: interface name
clear ip igmp group {***** | *A.B.C.D* [*INTERFACE*]}		Deletes IGMP entries in a specified IGMP group. *: all IGMP group A.B.C.D: IGMP group address

To clear IGMP statistics on an interface, use the following command.

Command	Mode	Description
ip igmp clear-statistics	Interface	Deletes the IGMP statistics

9.1.1.4 IGMP Debug

To enable debugging of all IGMP or a specific feature of IGMP, use the following command.

Command	Mode	Description
debug igmp {**all** | **decode** | **encode** | **events** | **fsm** | **snooping tcn** | **tib**}	Enable	Enables IGMP debugging. all: all IGMP decode: IGMP decoding encode: IGMP encoding events: IGMP events fsm: IGMP Finite State Machine (FSM) snooping tcn: snooping Topology Change Notification (TCN) tib: IGMP Tree Information Base (TIB)
no debug igmp {**all** | **decode** | **encode** | **events** | **fsm** | **snooping tcn** | **tib**}		Disables IGMP debugging.

i Tree Information Base (TIB) is the collection of state at a router that has been created by receiving IGMP messages from local hosts.

To display the debugging information, use the following command.

Command	Mode	Description
show debugging igmp	Enable	Shows the debugging information of IGMP.

9.1.2 IGMP Version 2

In IGMP version 2, the new extensions such as the leave process, election of an IGMP querier, and membership report suppression are added. New IGMP messages, the leave group and group-specific query can be used by hosts to explicitly leave groups, resulting in great reduction of the leave latency.

IGMPv2 Messages

There are three types of IGMPv2 messages of concern to the host-router interaction as shown below:

- **Membership query**
  A multicast router determines if any hosts are listening to a group by sending membership queries. The membership queries have two subtypes.
  – **General query**: This is used to determine if any hosts are listening to any group.
  – **Group-specific query**: This is used to determine if any hosts are listening to a particular group.

- **Version 2 membership report**
  This is used by hosts to join a group (unsolicited) or to respond to membership queries (solicited).
- **Leave group**
  This is used to explicitly leave a group.

IGMPv2 Operation

An IGMP querier is the only router that sends membership query messages for a network segment. In IGMP version 2, the querier is a router with the lowest IP address on the subnet. If the router hears no queries during the timeout period, it becomes the querier.

A host joins multicast groups by sending unsolicited membership report messages indicating its wish to receive multicast traffic for those groups (indicating that the host wants to become a member of the groups).

The querier sends general query messages periodically to discover which multicast groups have members on the attached networks of the router. The messages are addressed to the all-hosts multicast group, which has the address of 224.0.0.1 with a time-to-live (TTL) value of 1. If hosts do not respond to the received query messages for the maximum response time advertised in the messages, a multicast router discovers that no local hosts are members of a multicast group, and then stops forwarding multicast traffic onto the local network from the source for the group.

When hosts respond to membership queries from an IGMP querier, membership reports from the hosts other than the first one are suppressed to avoid increasing the unnecessary traffic. For an IGMP querier, it is sufficient to know that there is at least one interested member for a group on the network segment.

When a host is not interested in receiving the multicast traffic for a particular group any more, it can explicitly leave the group by sending leave group messages. Upon receiving a leave message, a querier then sends out a group-specific query message to determine if there is still any host interested in receiving the traffic. If there is no reply, the querier stops forwarding the multicast traffic.

9.1.2.1 IGMP Static Join

When there are no more group members on a network segment or a host cannot report its group membership using IGMP, multicast traffic is no longer transmitted to the network segment. However, you may want to pull down multicast traffic to a network segment to reduce the time from when an IGMP join request is made to when the requested stream begins arriving at a host, which is called the zapping time.

The IGMP static join feature has been developed to reduce the zapping time by statically creating a virtual host that behaves like a real on a port, even if there is no group member in the group where the port belongs. As a result, a multicast router realizes there is still group member, allowing multicast traffic to be permanently reachable on the group.

To configure the IGMP static join, use the following command.

Command	Mode	Description
ip igmp static-group *A.B.C.D* **vlan** *VLAN* **port** *PORT* [**reporter** *A.B.C.D*]	Global	Configures the IGMP static join. A.B.C.D: IGMP group address VLANS: VLAN ID (1-4094) reporter: host address
no ip igmp static-group		Deletes the configured IGMP static join. *: all addresses
no ip igmp static-group {*A.B.C.D* | **vlan** *VLAN*}		
no ip igmp static-group *A.B.C.D* **vlan** *VLAN* [**port** *PORT*]		
no ip igmp static-group *A.B.C.D* **vlan** *VLAN* **port** *PORT* **reporter** {*A.B.C.D* | *}		

To configure the IGMP static join for a range of IGMP groups on a specific interface, use the following command.

Command	Mode	Description
ip igmp static-group *A.B.C.D*	Interface	Configures the IGMP static join. A.B.C.D: multicast group address
ip igmp static-group range *A.B.C.D A.B.C.D*		Configures the IGMP static join for a range of multicast group addresses. A.B.C.D: start/end multicast group address to be joined
no ip igmp static-group *A.B.C.D*		Deletes the configured IGMP static join on this interface.
no ip igmp static-group range *A.B.C.D A.B.C.D*		

To configure the IGMP static join for a range of IGMP groups by access lists, use the following command.

Command	Mode	Description
ip igmp static-group list {<1-99> | <1300-1999> | WORD} **vlan** *VLAN* **port** *PORT* [**reporter** *A.B.C.D*]	Global	Configures the IGMP static join for a range of IGMP groups by access lists. 1-99: IP standard access list 1300-1999: IP standard access list (extended range) WORD: access list name VLANS: VLAN ID (1-4094) reporter: host address
no ip igmp static-group list {<1-99> | <1300-1999> | WORD}		Deletes the configured IGMP static join for a range of IGMP groups. *: all addresses
no ip igmp static-group list {<1-99> | <1300-1999> | WORD} **vlan** *VLAN* [**port** *PORT*]		
no ip igmp static-group list {<1-99> | <1300-1999> | WORD} **vlan** *VLAN* **port** *PORT* **reporter** {*A.B.C.D* | *}		

To display the IGMP static join group list, use the following command.

Command	Mode	Description
show ip igmp static-group	Enable Global Bridge	Shows the IGMP static join group list. 1-99: IP standard access list 1300-1999: IP standard access list (extended range) WORD: access list name VLANS: VLAN ID (1-4094)
show ip igmp static-group list		
show ip igmp static-group list {<1-99> | <1300-1999> | WORD} [**vlan** *VLAN*]		

i

If you do not specify the **reporter** option, the IP address configured on the VLAN is used as the source address of the membership report by default. If no IP address is configured on the VLAN, 0.0.0.0 is then used.

This feature only supports an IGMPv2 host; it does not support IGMPv3 host.

9.1.2.2 IGMP Access Control

Multicast routers send membership query messages to determine which multicast groups have members in the attached local networks of the router. If hosts respond to the queries, the routers then forward all packets addressed to the multicast group to these group members. You can restrict hosts on a network to join multicast groups on the specified access list.

To control an access to multicast groups on an interface, use the following command.

Command	Mode	Description
ip igmp access-group {<1-99> | *WORD*}	Interface	Enables an IGMP access control on an interface. 1-99: IP standard access list WORD: access list name
no ip igmp access-group		Disables a configured IGMP access control.

9.1.2.3 IGMP Querier Configuration

An IGMP querier is the only router that sends membership query messages for a network segment. In IGMP version 2, the querier is a router with the lowest IP address on the subnet. If the router hears no queries for the timeout period, it becomes the querier.

IGMP Query Interval

The querier (a multicast router) sends general query messages periodically to discover which multicast groups have members on the attached networks of the router.

To specify an interval to send general query messages, use the following command.

Command	Mode	Description
ip igmp query-interval <1-18000>	Interface	Specifies a general query interval. 1-18000: query interval (default: 125 seconds)
no ip igmp query-interval		Deletes a specified general query interval.

IGMP Startup Query Interval

The OLT needs to acquire information of its multicast members for the updated membership when it becomes the querier on the specified IGMP interface. For the updated membership, OLT sends general query messages as a querier. You can specify the interval to send this query messages as many as the configured QRV value.

To specify the interval to send general query messages, use the following command.

Command	Mode	Description
ip igmp startup-query-interval <1-18000>	Interface	Specifies a startup query interval. 1-18000: startup query interval (default: 32 seconds)
no ip igmp startup-query-interval		Deletes a specified startup query interval.

IGMP Query Response Time

In IGMP version 2 and 3, membership query messages include the maximum query response time field. This field specifies the maximum time allowed before sending a responding report. The maximum query response time allows a router to quickly detect that there are no more directly connected group members on a network segment.

To specify a maximum query response time advertised in membership query messages, use the following command.

Command	Mode	Description
ip igmp query-max-response-time <1-25>	Interface	Specifies a maximum query response time. 1-25: maximum response time (default: 10 seconds)
no ip igmp query-max-response-time		Deletes a specified maximum query response time.

IGMP Querier Timeout

There should be a single querier on a network segment to prevent duplicating multicast traffic for connected hosts. When there are several routers, if the router has the lowest IP address or if the router hears no queries during the timeout period, it becomes the querier.

To specify a timeout period before a router takes over as a querier for the interface after the previous querier has stopped querying, use the following command.

Command	Mode	Description
ip igmp querier-timeout <60-300>	Interface	Specifies an IGMP queier timeout period. 60-300: timeout period (default: 255 seconds)
no ip igmp querier-timeout		Deletes a specified IGMP queier timeout period.

IGMP Last Member Query Count and Interval

When a host is not interested in receiving the multicast traffic for a particular group any more, it can explicitly leave the group by sending leave group messages.

Upon receiving a leave message, a querier then sends out a group-specific (IGMPv2) or group-source-specific query (IGMPv3) message to determine if there is still any host interested in receiving the traffic. If there is no reply, the querier stops forwarding the multicast traffic. However, IGMP messages may get lost for various reasons, so you can specify the number of sending query messages and its interval.

To specify the number of sending group-specific or group-source-specific query messages, use the following command.

Command	Mode	Description
ip igmp last-member-query-count <2-7>	Interface	Specifies a last member query count. 2-7: last member query count value (default: 2)
no ip igmp last-member-query-count		Deletes a specified last member query count.

To specify the interval to send group-specific or group-source-specific query messages, use the following command.

Command	Mode	Description
ip igmp last-member-query-interval <1000-25500>	Interface	Specifies a last member query interval. 1000-25500: last member query interval (default: 1000 milliseconds)
no ip igmp last-member-query-interval		Deletes a specified last member query interval.

IGMP Unsolicited Report Interval

When one of its hosts joins a multicast address group to which none of its other hosts belong, sends unsolicited group membership reports to that group. You can specify the interval to send this unsolicited report messages as many as the configured QRV value.

To specify the interval to send unsolicited report messages, use the following command.

Command	Mode	Description
ip igmp unsolicited-report-interval <1-18000>	Interface	Specifies an unsolicited report interval. 1-18000: unsolicited report interval (default: 10 seconds)
no ip igmp unsolicited-report-interval		Deletes a specified unsolicited report interval.

9.1.2.4 IGMP Immediate Leave

Normally, a querier sends a group-specific or group-source-specific query message upon receipt of a leave message from a host. If you want to set a leave latency as 0 (zero), you can omit the querying procedure. When the querying procedure is omitted, the router immediately removes the interface from the IGMP cache for that group, and informs the multicast routing protocols.

To enable the immediate leave feature on a current interface, use the following command.

Command	Mode	Description
ip igmp immediate-leave group-list {<1-99> | <1300-1999> | *WORD*}	Interface	Enables the IGMP immediate leave. 1-99: IP standard access list 1300-1999: IP standard access list (extended range) WORD: access list name
no ip igmp immediate-leave		Disables the IGMP immediate leave.

Use this command only on IGMPv2 and IGMPv3 interfaces to which one IGMP host is connected. If there is more than one IGMP host connected to a network segment through the same interface, and a certain host sends a leave group message, the router will remove all hosts on the interface from the multicast group. The router will lose contact with the hosts that should remain in the multicast group until they send join requests in response to the router's next general query.

9.1.3 IGMP Version 3

IGMP version 3 provides support for the source filtering, which is to receive multicast traffic for a group from specific source addresses, or from except specific source addresses, allowing the Source-Specific Multicast (SSM) model.

The source filtering is implemented by the major revision of the membership report. IGMPv3 membership reports contain two types of the record: current-state and state-change. Each record specifies the information of the filter mode and source list. The report can contain multiple group records, allowing reporting of full current state using fewer packets.

The OLT runs IGMPv3 by default, and there are no additional IGMPv3 parameters you need to configure. IGMPv3 snooping features are provided.

IGMPv3 Messages

There are two types of IGMPv3 messages of concern to the host-router interaction as shown below:

- **Membership query**
  A multicast router determines if any hosts are listening to a group by sending membership queries. There are three variants of the membership queries.
  – **General query**: This is used to determine if any hosts are listening to any group.
  – **Group-specific query**: This is used to determine if any hosts are listening to a particular group.
  – **Group-source-specific query**: This is used to determine if any hosts are listening to a particular group and source.

- **Version 3 membership report**
  This is used by hosts to report the current multicast reception state, or changes in the multicast reception state, of their interfaces. IGMPv3 membership reports contain a group record that is a block of fields containing information of the host's membership in a single multicast group on the interface from which the report is sent. A single re-

port may also contain multiple group records. Each group record has one of the following information:

– **Current-state**: This indicates the current filter mode including/excluding the specified multicast address.
– **Filter-mode-change**: This indicates a change from the current filter mode to the other mode.
– **Source-list-change**: This indicates a change allowing/blocking a list of the multicast sources specified in the record.

IGMPv3 Operation

Basically, IGMPv3 has the same join/leave (allow/block in the IGMPv3 terminology) and query-response mechanism as IGMPv2's. Due to the major revision of the membership report, however, leave group messages are not used for the explicit leave process any longer. In IGMPv3 concept, membership reports with state-change records are used to allow or block multicast sources, and those with current-state records are used to respond to membership queries. Membership report suppression feature has been removed for multicast routers to keep track of membership state per host.

9.1.4 Displaying IGMP Information

To display current IGMP groups and relevant information, use the following command.

Command	Mode	Description
show ip igmp groups [**detail**]	Enable Global Bridge	Shows the multicast groups with receivers directly connected to the router and learned through IGMP. A.B.C.D: IGMP group address INTERFACE: interface name
show ip igmp groups *A.B.C.D* [**detail**]		
show ip igmp groups *INTERFACE* [**detail**]		
show ip igmp groups *INTERFACE A.B.C.D* [**detail**]		
show ip igmp groups [*INTERFACE*] **summary**		
show ip igmp interface		Shows multicast-related information on an interface.
show ip igmp interface *INTERFACE*		

9.2 Multicast Functions

The OLT provides various multicast functions including Layer 2 multicast forwarding, which allow you to achieve the fully effective and flexible multicast deployment.

9.2.1 Multicast Forwarding Database

Internally, the OLT forwards the multicast traffic referred to the multicast forwarding database (McFDB). The McFDB maintains multicast forwarding entries collected from multicast protocols and features, such as PIM, IGMP, etc.

The McFDB has the same behavior as the Layer 2 FDB. When certain multicast traffic comes to a port, the switch looks for the forwarding information (the forwarding entry) for the traffic in the McFDB. If the McFDB has the information for the traffic, the switch forwards it to the proper ports. If the McFDB does not have the information for the traffic, the switch learns the information on the McFDB, and then floods it to all ports. If the information is not referred to forward another multicast traffic during the given aging time, it is aged out from the McFDB.

9.2.1.1 Blocking Unknown Multicast Traffic

When certain multicast traffic comes to a port and the McFDB has no forwarding information for the traffic, the multicast traffic is flooded to all ports by default. You can configure the switch not to flood unknown multicast traffic.

To configure the switch to discard unknown multicast traffic, use the following command.

Command	Mode	Description
ip unknown-multicast [**port** *PORTS*] **block**	Global	Configures the switch to discard unknown multicast traffic. PORTS: port number
ipv6 unknown-multicast [**port** *PORTS*] **block**		
no ip unknown-multicast [**port** *PORTS*] **block**		Configures the switch to flood unknown multicast traffic. (default)
no ipv6 unknown-multicast [**port** *PORTS*] **block**		

This command should not be used for the ports to which a multicast router is attached!

9.2.1.2 Forwarding Entry Aging

To specify the aging time for forwarding entries on the McFDB, use the following command.

Command	Mode	Description
ip mcfdb aging-time <10-10000000>	Global	Specifies the aging time for forwarding entries on the McFDB. 10-10000000: aging time (default: 300)

no ip mcfdb aging-time		Deletes the specified aging time for forwarding entries.

To specify the maximum number of forwarding entries on the McFDB, use the following command.

Command	Mode	Description
ip mcfdb aging-limit <256-65535>	Global	Specifies the maximum number of forwarding entries on the McFDB. 256-65535: number of entries (default: 5000)
no ip mcfdb aging-limit		Deletes the specified maximum number of forwarding entries.

9.2.1.3 Displaying McFDB Information

To display McFDB information, use the following command.

Command	Mode	Description
show ip mcfdb	Enable Global Bridge	Shows the current aging time and maximum number of forwarding entries.
show ip mcfdb aging-entry [**vlan** *VLAN* | **group** *A.B.C.D*] [**mac-based** | **detail**]		Shows the current forwarding entries. VLAN: VLAN ID (1-4094) A.B.C.D: ipv4 multicast group address X:X::X:X: ipv6 multicast group address mac-based: lists entries on a MAC address basis

To clear multicast forwarding entries, use the following command.

Command	Mode	Description
clear ip mcfdb [* | **vlan** *VLAN*]	Enable Global	Clears multicast forwarding entries. *: all forwarding entries VLAN: VLAN ID (1-4094)
clear ip mcfdb vlan *VLAN* **group** *A.B.C.D* **source** *A.B.C.D*		Clears a specified forwarding entry. group A.B.C.D: multicast group address source A.B.C.D: multicast source address

9.2.2 IGMP Snooping Basic

Layer 2 switches normally flood multicast traffic within the broadcast domain, since it has no entry in the Layer 2 forwarding table for the destination address. Multicast addresses never appear as source addresses, therefore the switch cannot dynamically learn multicast addresses. This multicast flooding causes unnecessary bandwidth usage and discarding unwanted frames on those nodes which did not want to receive the multicast transmission. To avoid such flooding, IGMP snooping feature has been developed.

The purpose of IGMP snooping is to constrain the flooding of multicast traffic at Layer 2. IGMP snooping, as implied by the name, allows a switch to snoop the IGMP transaction between hosts and routers, and maintains the multicast forwarding table which contains the information acquired by the snooping. When the switch receives a join request from a

host for a particular multicast group, the switch then adds a port number connected to the host and a destination multicast group to the forwarding table entry; when the switch receives a leave message from a host, it removes the entry from the table.

By maintaining this multicast forwarding table, the OLT dynamically forward multicast traffic only to those interfaces that want to receive it as nominal unicast forwarding does.

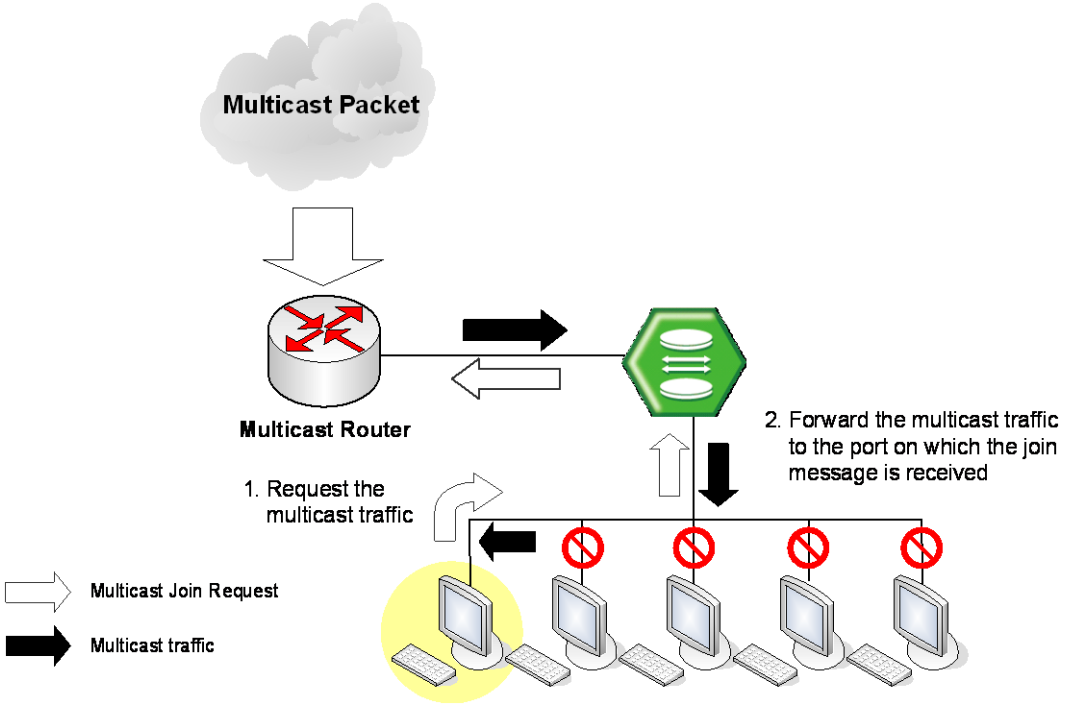


Fig. 9.2 IGMP Snooping

9.2.2.1 Enabling IGMP Snooping

You can enable IGMP snooping globally or on each VLAN respectively. By default, IGMP snooping is globally disabled.

To enable IGMP snooping, use the following command.

Command	Mode	Description
ip igmp snooping	Global	Enables IGMP snooping globally.
ip igmp snooping vlan *VLANS*		Enables IGMP snooping on a VLAN. VLANS: VLAN ID (1-4094)

To disable IGMP snooping, use the following command.

Command	Mode	Description
no ip igmp snooping	Global	Disables IGMP snooping globally.
no ip igmp snooping vlan *VLANS*		Disables IGMP snooping on a VLAN. VLANS: VLAN ID (1-4094)

9.2.2.2 IGMP Snooping Version

The membership reports sent to the multicast router are sent based on the IGMP snooping version of the interface. If you statically specify the version on a certain interface, the reports are always sent out only with the specified version. If you do not statically specify the version, and a version 1 query is received on the interface, the interface dynamically sends out a version 1 report. If no version 1 query is received on the interface for the version 1 router present timeout period (400 seconds), the interface version goes back to its default value (3).

To specify the static IGMP snooping version, use the following command.

Command	Mode	Description
ip igmp snooping version <1-3>	Global	Configures the IGMP snooping version globally. 1-3: IGMP snooping version (default: 3)
ip igmp snooping vlan *VLANS* **version** <1-3>		Configures the IGMP snooping version on a VLAN interface. VLANS: VLAN ID (1-4094)

To delete the specified static IGMP snooping version, use the following command.

Command	Mode	Description
no ip igmp snooping version	Global	Deletes the specified IGMP snooping version.
no ip igmp snooping vlan *VLANS* **version**		

i Dynamic IGMPv3 snooping is configured by default.

9.2.2.3 IGMP Snooping Robustness Value

The robustness variable allows tuning for the expected packet loss on a network. If a network is expected to be lossy, the robustness variable may be increased. When receiving the query message that contains a certain robustness variable from an IGMP snooping querier, a host returns the report message as many as the specified robustness variable.

To configure the robustness variable, use the following command.

Command	Mode	Description
ip igmp snooping robustness-variable <1-7>	Global	Configures the robustness variable. (default: 2)
ip igmp snooping vlan *VLANS* **robustness-variable** <1-7>		Configures the robustness variable on a VLAN. VLANS: VLAN ID (1-4094)

To delete a specified robustness variable, use the following command.

Command	Mode	Description
no ip igmp snooping	Global	Deletes a specified robustness variable.

robustness-variable		
no ip igmp snooping vlan *VLANS* **robustness-variable**		

9.2.3 IGMPv2 Snooping

9.2.3.1 IGMP Snooping Querier Configuration

IGMP snooping querier should be used to support IGMP snooping in a VLAN where PIM and IGMP are not configured.

When the IGMP snooping querier is enabled, the IGMP snooping querier sends out periodic general queries that trigger membership report messages from a host that wants to receive multicast traffic. The IGMP snooping querier listens to these membership reports to establish appropriate forwarding.

Enabling IGMP Snooping Querier

To enable the IGMP snooping querier, use the following command.

Command	Mode	Description
ip igmp snooping querier [**address** *A.B.C.D*]	Global	Enables the IGMP snooping querier globally. A.B.C.D: source address of IGMP snooping query
ip igmp snooping vlan *VLANS* **querier** [**address** *A.B.C.D*]		Enables the IGMP snooping querier on a VLAN. VLANS: VLAN ID (1-4094)

To disable the IGMP snooping querier, use the following command.

Command	Mode	Description
no ip igmp snooping querier [**address**]	Global	Disables the IGMP snooping querier. address: source address of IGMP snooping query
no ip igmp snooping vlan *VLANS* **querier** [**address**]		

i

If you do not specify a source address of an IGMP snooping query, the IP address configured on the VLAN is used as the source address by default. If no IP address is configured on the VLAN, 0.0.0.0 is then used.

IGMP Snooping Query Interval

An IGMP snooping querier periodically sends general query messages to trigger membership report messages from a host that wants to receive IP multicast traffic.

To specify an interval to send general query messages, use the following command.

Command	Mode	Description

ip igmp snooping querier query-interval <1-1800>	Global	Specifies an IGMP snooping query interval in the unit of second. 1-1800: query interval (default: 125)
ip igmp snooping vlan *VLANS* **querier query-interval** <1-1800>		Specifies an IGMP snooping query interval on a VLAN. VLANS: VLAN ID (1-4094)

To delete a specified interval to send general query messages, use the following command.

Command	Mode	Description
no ip igmp snooping querier query-interval	Global	Disables a specified IGMP snooping query interval.
no ip igmp snooping vlan *VLANS* **querier query-interval**		

IGMP Snooping Query Response Time

Membership query messages include the maximum query response time field. This field specifies the maximum time allowed before sending a responding report. The maximum query response time allows a router to quickly detect that there are no more hosts interested in receiving multicast traffic.

To specify a maximum query response time advertised in general query messages, use the following command.

Command	Mode	Description
ip igmp snooping querier max-response-time <1-25>	Global	Specifies a maximum query response time. 1-25: maximum response time (default: 10 seconds)
ip igmp snooping vlan *VLANS* **querier max-response-time** <1-25>		Specifies a maximum query response time. VLANS: VLAN ID (1-4094)

To delete a specified maximum query response time, use the following command.

Command	Mode	Description
no ip igmp snooping querier max-response-time	Global	Deletes a specified maximum query response time.
no ip igmp snooping vlan *VLANS* **querier max-response-time**		

Displaying IGMP Snooping Querier Information

To display IGMP querier information and configured parameters, use the following command.

Command	Mode	Description
show ip igmp snooping [**vlan** *VLANS*] **querier** [**detail**]	Enable Global Bridge	Shows IGMP querier information and configured parameters.

9.2.3.2 IGMP Snooping Last Member Query Interval

Upon receiving a leave message, a switch with IGMP snooping then sends out a group-specific (IGMPv2) or group-source-specific query (IGMPv3) message to determine if there is still any host interested in receiving the traffic. If there is no reply, the switch stops forwarding the multicast traffic. However, IGMP messages may get lost for various reasons, so you can specify an interval to send query messages.

To specify an interval to send group-specific or group-source-specific query messages, use the following command.

Command	Mode	Description
ip igmp snooping last-member-query-interval <100-10000>	Global	Specifies a last member query interval. 100-10000: last member query interval (default: 1000 milliseconds)
ip igmp snooping vlan *VLANS* **last-member-query-interval** <100-10000>		Specifies a last member query interval. VLANS: VLAN ID (1-4094)

To delete a specified an interval to send group-specific or group-source-specific query messages, use the following command.

Command	Mode	Description
no ip igmp snooping last-member-query-interval	Global	Deletes a specified last member query interval.
no ip igmp snooping vlan *VLANS* **last-member-query-interval**		

9.2.3.3 IGMP Snooping Immediate Leave

Normally, an IGMP snooping querier sends a group-specific or group-source-specific query message upon receipt of a leave message from a host. If you want to set a leave latency as 0 (zero), you can omit the querying procedure. When the querying procedure is omitted, the switch immediately removes the entry from the forwarding table for that VLAN, and informs the multicast router.

To enable the IGMP snooping immediate leave, use the following command.

Command	Mode	Description
ip igmp snooping immediate-leave	Global	Enables the IGMP snooping immediate leave globally.
ip igmp snooping port *PORTS*		Enables the IGMP snooping immediate leave on a port.

immediate-leave		PORTS: port number
ip igmp snooping vlan *VLANS* **immediate-leave**		Enables the IGMP snooping immediate leave on a VLAN. VLANS: VLAN ID (1-4094)

To disable the IGMP snooping immediate leave, use the following command.

Command	Mode	Description
no ip igmp snooping immediate-leave	Global	Disables the IGMP snooping immediate leave.
no ip igmp snooping port *PORTS* **immediate-leave**		
no ip igmp snooping vlan *VLANS* **immediate-leave**		

Use this command with the explicit host tracking feature (see Section 9.2.3.6). If you don't, when there is more than one IGMP host belonging to a VLAN, and a certain host sends a leave group message, the switch will remove all host entries on the forwarding table from the VLAN. The switch will lose contact with the hosts that should remain in the forwarding table until they send join requests in response to the switch's next general query message.

9.2.3.4 IGMP Snooping Report Suppression

If an IGMP querier sends general query messages, and hosts are still interested in the multicast traffic, the hosts should return membership report messages. For a multicast router, however, it is sufficient to know that there is at least one interested member for a group on the network segment. Responding a membership report per each of group members may unnecessarily increase the traffic on the network; only one report per group is enough.

When the IGMP snooping report suppression is enabled, a switch suppresses membership reports from hosts other than the first one, allowing the switch to forward only one membership report in response to a general query from a multicast router.

To enable the IGMP snooping report suppression, use the following command.

Command	Mode	Description
ip igmp snooping report-suppression	Global	Enables the IGMP snooping report suppression globally.
ip igmp snooping vlan *VLANS* **report-suppression**		Enables the IGMP snooping report suppression on a VLAN. VLANS: VLAN ID (1-4094)

To disable the IGMP snooping report suppression, use the following command.

Command	Mode	Description
no ip igmp snooping report-	Global	Disables the IGMP snooping report suppression.

suppression		
no ip igmp snooping vlan *VLANS* **report-suppression**		

The IGMP snooping report suppression is supported only IGMPv1 and IGMPv2 reports. In case of an IGMPv3 report, a single membership report can contain the information for all the groups which a host is interested in. Thus, there is no need for the report suppression since the number of reports would be generally equal to the number of hosts only.

9.2.3.5 IGMP Snooping S-Query Report Agency

If IGMP snooping switch receives IGMP group-specific query messages from the multicast router, it just floods them into all of its ports. The hosts received the group-specific queries send the report messages according to their IGMP membership status. However, OLT is enabled as IGMP snooping S-Query report agency, the group-specific queries are not sent downstream. When the switch receives a group-specific query, the switch terminates the query and sends an IGMP report if there is a receiver for the group.

To enable IGMP snooping S-Query Report Agency, use the following command.

Command	Mode	Description
ip igmp snooping s-query-report agency	Global	Enables IGMP snooping s-query-report agency.

To disable IGMP snooping S-Query Report Agency, use the following command.

Command	Mode	Description
no ip igmp snooping s-query-report agency	Global	Disables IGMP snooping s-query-report agency.

9.2.3.6 Explicit Host Tracking

Explicit host tracking is one of the important IGMP snooping features. It has the ability to build the explicit tracking database by collecting the host information via the membership reports sent by hosts. This database is used for the immediate leave for IGMPv2 hosts, the immediate block for IGMPv3 hosts, and IGMP statistics collection.

To enable explicit host tracking, use the following command.

Command	Mode	Description
ip igmp snooping explicit-tracking	Global	Enables explicit host tracking globally.
ip igmp snooping vlan *VLANS* **explicit-tracking**		Enables explicit host tracking on a VLAN. VLANS: VLAN ID (1-4094)

To disable explicit host tracking, use the following command.

Command	Mode	Description
no ip igmp snooping explicit-tracking	Global	Disables explicit host tracking globally.
no ip igmp snooping vlan *VLANS* **explicit-tracking**		Disables explicit host tracking on a VLAN. VLANS: VLAN ID (1-4094)

You can also restrict the number of hosts on a port for the switch performance and enhanced security.

To specify the maximum number of hosts on a port, use the following command.

Command	Mode	Description
ip igmp snooping explicit-tracking max-hosts port *PORTS* **count** <1-65535>	Global	Specifies the maximum number of hosts on a port. PORTS: port number 1-65535: maximum number of hosts (default: 1024)
no ip igmp snooping explicit-tracking max-hosts port *PORTS*		Deletes the specified maximum number of hosts

To enable IGMP group-specific queries Suppression, use the following command.

Command	Mode	Description
ip igmp snooping explicit-tracking s-query-suppression	Global	Enables IGMP group-specific queries suppression. It does not send a group specific query to member host after one sends a leave message on a VLAN.

To disable IGMP group-specific queries suppression, use the following command.

Command	Mode	Description
no ip igmp snooping explicit-tracking s-query-suppression	Global	Disables IGMP group-specific queries suppression. It sends a group specific query to hosts after one sends a leave message on a VLAN. (default)

To display the explicit tracking information, use the following command.

Command	Mode	Description
show ip igmp snooping explicit-tracking	Enable Global Bridge	Shows the explicit host tracking information globally.
show ip igmp snooping explicit-tracking summary { **vlan** *VLANS* | **port** *PORTS* }		Shows the summary of IGMP snooping explicit-tracking information.
show ip igmp snooping explicit-tracking vlan *VLANS*		Shows the explicit host tracking information per VLAN. VLANS: VLAN ID (1-4094)
show ip igmp snooping explicit-tracking port *PORTS*		Shows the explicit host tracking information per port. PORTS: port number
show ip igmp snooping explicit-		Shows the explicit host tracking information per group.

tracking group *A.B.C.D*		A.B.C.D: multicast group address

i Explicit host tracking is enabled by default.

9.2.3.7 Multicast Router Port Configuration

The multicast router port is the port which is directly connected to a multicast router. A switch adds multicast router ports to the forwarding table to forward membership reports only to those ports. Multicast router ports can be statically specified or dynamically learned by incoming IGMP queries and PIM hello packets.

Static Multicast Router Port

You can statically configure Layer 2 port as the multicast router port which is directly connected to a multicast router, allowing a static connection to a multicast router.

To specify a multicast router port, use the following command.

Command	Mode	Description
ip igmp snooping mrouter port {*PORTS* | **cpu**}	Global	Specifies a multicast router port globally. PORTS: port number cpu: CPU port
ip igmp snooping vlan *VLANS* **mrouter port** {*PORTS* | **cpu**}		Specifies a multicast router port on a VLAN. VLANS: VLAN ID (1-4094)

To delete a specified multicast router port, use the following command.

Command	Mode	Description
no ip igmp snooping mrouter port {*PORTS* | **cpu**}	Global	Deletes a specified multicast router port.
no ip igmp snooping vlan *VLANS* **mrouter port** {*PORTS* | **cpu**}		

Multicast Router Port Learning

Multicast router ports are added to the forwarding table for every Layer 2 multicast entry. The switch dynamically learns those ports through snooping on PIM hello packets.

To enable the switch to learn multicast router ports through PIM hello packets, use the following command.

Command	Mode	Description
ip igmp snooping mrouter learn pim	Global	Enables to learn multicast router ports through PIM hello packets globally.

ip igmp snooping vlan *VLANS* **mrouter learn pim**		Enables to learn multicast router ports through PIM hello packets on a VLAN. VLANS: VLAN ID (1-4094)

To disable the switch to learn multicast router ports through PIM hello packets, use the following command.

Command	Mode	Description
no ip igmp snooping mrouter learn pim	Global	Disables to learn multicast router ports through PIM hello packets.
no ip igmp snooping vlan *VLANS* **mrouter learn pim**		

Multicast Router Port Forwarding

The multicast traffic should be forwarded to IGMP snooping membership ports and multicast router ports because the multicast router needs to receive muticast source information. To enable the switch to forward the traffic to multicast router ports, use the following command.

Command	Mode	Description
ip multicast mrouter-pass-through	Global	Enables to forward multicast traffic to the multicast router ports.
no ip multicast mrouter-pass-through		Disables to forward multicast traffic to the multicast router ports.

Displaying Multicast Router Port

To display a current multicast router port for IGMP snooping, use the following command.

Command	Mode	Description
show ip igmp snooping mrouter	Enable Global Bridge	Shows a current multicast router port for IGMP snooping globally.
show ip igmp snooping vlan *VLANS* **mrouter**		Shows a current multicast router port for IGMP snooping on a specified VLAN. VLANS: VLAN ID (1-4094)

9.2.3.8 TCN Multicast Flooding

When a network topology change occurs, the protocols for a link layer topology – such as spanning tree protocol (STP), etc – notify switches in the topology using a topology change notification (TCN).

When TCN is received, the switch where an IGMP snooping is running will flood multicast traffic to all ports in a VLAN, since a network topology change in a VLAN may invalidate previously learned IGMP snooping information. However, this flooding behavior is not desirable if the switch has many ports that are subscribed to different groups. The traffic could exceed the capacity of the link between the switch and the end host, resulting in

packet loss. Thus, a period of multicast flooding needs to be controlled to solve such a problem.

Enabling TCN Multicast Flooding

To enable the switch to flood multicast traffic when TCN is received, use the following command.

Command	Mode	Description
ip igmp snooping tcn flood	Global	Enables the switch to flood multicast traffic when TCN is received.
ip igmp snooping tcn vlan *VLANS* **flood**		Enables the switch to flood multicast traffic on a VLAN when TCN is received. VLANS: VLAN ID (1-4094)

To disable the switch to flood multicast traffic when TCN is received, use the following command.

Command	Mode	Description
no ip igmp snooping tcn flood	Global	Disables the switch to flood multicast traffic when TCN is received
no ip igmp snooping tcn vlan *VLANS* **flood**		

TCN Flooding Suppression

When TCN is received, the switch where an IGMP snooping is running will flood multicast traffic to all ports until receiving two general queries, or during two general query intervals by default. You can also configure the switch to stop multicast flooding according to a specified query count or query interval.

To specify a query count to stop multicast flooding, use the following command.

Command	Mode	Description
ip igmp snooping tcn flood query count <1-10>	Global	Specifies a query count to stop multicast flooding. 1-10: query count value (default: 2)
no ip igmp snooping tcn flood query count		Deletes a specified query count to stop multicast flooding.

To specify a query interval to stop multicast flooding, use the following command.

Command	Mode	Description
ip igmp snooping tcn flood query interval <1-1800>	Global	Specifies a query interval to stop multicast flooding in the unit of second. An actual stop-flooding interval is calculated by (query count) x (query interval). 1-1800: query interval value (default: 125)
no ip igmp snooping tcn flood query interval		Deletes a specified query interval to stop multicast flooding.

TCN Flooding Query Solicitation

Typically, if a network topology change occurs, the spanning tree root switch issues a query solicitation which is actually a global leave message with the group address 0.0.0.0. When a multicast router receives this solicitation, it immediately sends out IGMP general queries to hosts, allowing the fast convergence. You can direct the switch where an IGMP snooping is running to send a query solicitation when TCN is received.

To enable the switch to send a query solicitation when TCN is received, use the following command.

Command	Mode	Description
ip igmp snooping tcn query solicit [**address** *A.B.C.D*]	Global	Enables the switch to send a query solicitation when TCN is received. address: source IP address for query solicitation

To disable the switch to send a query solicitation when TCN is received, use the following command.

Command	Mode	Description
no ip igmp snooping tcn query solicit [**address**]	Global	Disables the switch to send a query solicitation when TCN is received.

IGMP Snooping TCN Debug

To enable debugging of all IGMP snooping TCN, use the following command.

Command	Mode	Description
debug igmp snooping tcn	Enable	Enables IGMP snooping Topology Change Notification (TCN) debugging.
no debug igmp snooping tcn		Disables IGMP snooping Topology Change Notification (TCN) debugging.

9.2.4 IGMPv3 Snooping

Immediate Block

IGMPv3 immediate block feature allows a host to block sources with the block latency, 0 (zero) by referring to the explicit tracking database. When receiving a membership report with the state-change record from a host that is no longer interested in receiving multicast traffic from a certain source, the switch compares the source list for the host in the explicit tracking database with the source list in the received membership report. If both are matching, the switch removes the source entry from the list in the database, and stops forwarding the multicast traffic to the host; no group-source-specific query message is needed for the membership leave process.

To enable IGMPv3 immediate block, use the following command.

Command	Mode	Description

ip igmp snooping immediate-block	Global	Enables immediate block globally.
ip igmp snooping vlan *VLANS* **immediate-block**		Enables immediate block on a VLAN. VLANS: VLAN ID (1-4094)

To disable IGMPv3 immediate block, use the following command.

Command	Mode	Description
no ip igmp snooping immediate-block	Global	Disables immediate block globally.
no ip igmp snooping vlan *VLANS* **immediate-block**		Disables immediate block on a VLAN. VLANS: VLAN ID (1-4094)

i IGMPv3 immediate block is enabled by default.

9.2.5 Displaying IGMP Snooping Information

To display a current IGMP snooping configuration, use the following command.

Command	Mode	Description
show ip igmp snooping [**vlan** *VLANS*]	Enable Global Bridge	Shows a current IGMP snooping configuration. VLAN: VLAN ID (1-4094)
show ip igmp snooping info [**vlan** *VLANS*]		

To display the collected IGMP snooping statistics, use the following command.

Command	Mode	Description
show ip igmp snooping stats port {*PORTS* | **cpu**}	Enable Global Bridge	Shows the collected IGMP snooping statistics. PORTS: port number

To clear the collected IGMP snooping statistics, use the following command.

Command	Mode	Description
clear ip igmp snooping stats port [*PORTS* | **cpu**]	Enable Global	Clears the collected IGMP snooping statistics PORTS: port number

To display the IGMP snooping table, use the following command.

Command	Mode	Description
show ip igmp snooping groups [*A.B.C.D* | **mac-based**]	Enable Global Bridge	Shows the IGMP snooping table globally. mac-based: lists groups on a MAC address basis.
show ip igmp snooping groups		Shows the IGMP snooping table per port.

port {*PORTS* | **cpu**} [**mac-based**]		PORTS: port number
show ip igmp snooping groups vlan *VLANS* [**mac-based**]		Shows the IGMP snooping table per VLAN. VLANS: VLAN ID (1-4094)
show ip igmp snooping groups summary { **port** *PORTS* | **vlan** *VLANS* }		Show the summary of IGMP snooping group membership information per port or VLAN ID

To display the IGMP snooping membership table, use the following command.

Command	Mode	Description
show ip igmp snooping table vlan *VLANS*	Enable Global Bridge	Shows the IGMP snooping membership table of specific VLAN ID.
show ip igmp snooping table port *PORTS*		Shows the IGMP snooping membership table of a port number.
show ip igmp snooping table group *A.B.C.D*		Shows the IGMP snooping membership table of specific multicast group address.
show ip igmp snooping table reporter *A.B.C.D*		Shows the IGMP snooping membership table of specific reporter's IP address.

9.2.6 Multicast VLAN Registration (MVR)

Multicast VLAN registration (MVR) is designed for applications using multicast traffic across an Ethernet network. MVR allows a multicast VLAN to be shared among subscribers remaining in separate VLANs on the network. It guarantees the Layer 2 multicast flooding instead of the forwarding via Layer 3 multicast, allowing to flood multicast streams in the multicast VLAN, but to isolate the streams from the subscriber VLANs for bandwidth and security reasons. This improves bandwidth utilization and simplifies multicast group management.

MVR also provides the fast convergence for topology changes in the Ethernet ring-based service provider network with STP and IGMP snooping TCN, guaranteeing stable multicast services.

MVR implemented for the OLT has the following restrictions, so you must keep in mind those, before configuring MVR.

- All receiver ports must belong to the both subscriber and multicast VLANs as un-tagged.
- IGMP snooping must be enabled before enabling MVR.
- A single group address cannot belong to more than two MVR groups.
- MVR and multicast routing cannot be enabled together.
- MVR only supports IGMPv2.

9.2.6.1 Enabling MVR

To enable MVR on the system, use the following command.

Command	Mode	Description
mvr	Global	Enables MVR.
no mvr		Disables MVR.

9.2.6.2 MVR Group

To configure MVR, you need to specify an MVR group and group address. If you specify several MVR groups, IGMP packets from the receiver ports are sent to the source ports belonging to the corresponding MVR group according to the group address specified in the packets.

To specify an MVR group and group address, use the following command.

Command	Mode	Description
mvr vlan *VLAN* **group** {*A.B.C.D* | **any**}	Global	Specifies an MVR group and group address. VLAN: VLAN ID (1-4094) A.B.C.D: IGMP group address
no mvr vlan *VLAN* **group** {*A.B.C.D* | **any**}		Deletes a specified MVR group and group address.

9.2.6.3 Source/Receiver Port

You need to specify the source and receiver ports for MVR. The followings are the definitions for the ports.

- **Source Port**
  This is connected to multicast routers or sources as an uplink port, which receives and sends the multicast traffic. Subscribers cannot be directly connected to source ports. All source ports belong to the multicast VLAN as tagged.
- **Receiver Port**
  This is directly connected to subscribers as a subscriber port, which should only receive the multicast traffic. All receiver ports must belong to the both subscriber and multicast VLANs as untagged for implementation reasons.

To specify a port as the source or receiver port, use the following command.

Command	Mode	Description
mvr port *PORTS* **type** {**receiver** | **source**}	Global	Specifies an MVR port. PORTS: port number
no mvr port *PORTS*		Deletes a specified MVR port.

9.2.6.4 MVR Helper Address

When being in a different network from an MVR group's, a multicast router sends the multicast traffic to each MVR group using Layer 3 multicast routing. In such an environment, when an IGMP packet from a subscriber is transmitted to the multicast router via the MVR group (multicast VLAN interface), the source address of the IGMP packet may not match the network address of the MVR group. In this case, the multicast router normally discards the IGMP packet. To avoid this behavior, you can configure the switch to replace the source address with a specified helper address. The helper address must belong to the MVR group's network.

To specify an MVR helper address to replace a source address of an IGMP packet, use the following command.

Command	Mode	Description
mvr vlan *VLAN* **helper** *A.B.C.D*	Global	Specifies an MVR helper address. VLAN: VLAN ID (1-4094) A.B.C.D: helper address
no mvr vlan *VLAN* **helper**		Deletes a specified MVR helper address.

9.2.6.5 Displaying MVR Configuration

To display an MVR configuration, use the following command.

Command	Mode	Description
show mvr	Enable Global	Shows an MVR configuration.
show mvr port		
show mvr vlan *VLANS*		

9.2.7 IGMP Filtering and Throttling

IGMP filtering and throttling control the distribution of multicast services on each port. IGMP filtering controls which multicast groups a host on a port can join by associating an IGMP profile that contains one or more IGMP groups and specifies whether an access to the group is permitted or denied with a port. For this operation, configuring the IGMP profile is needed before configuring the IGMP filtering. IGMP throttling limits the maximum number of IGMP groups that a host on a port can join.

Note that both IGMP filtering and throttling control only membership reports (join messages) from a host, and do not control multicast streams.

9.2.7.1 IGMP Filtering

Creating IGMP Profile

You can configure an IGMP profile for IGMP filtering in *IGMP Profile Configuration* mode. The system prompt will be changed from SWITCH(config)# to SWITCH(config-igmp-profile[N])#.

To create/modify an IGMP profile, use the following command.

Command	Mode	Description
ip igmp profile <1-2147483647>	Global	Creates/modifies an IGMP profile. 1-2147483647: IGMP profile number
no ip igmp profile <1-2147483647>		Deletes a created IGMP profile.

IGMP Group Range

To specify an IGMP group range to apply to IGMP filtering, use the following command.

Command	Mode	Description
range *A.B.C.D* [*A.B.C.D*]	IGMP Profile	Specifies a range of IGMP groups. A.B.C.D: low multicast address A.B.C.D: high multicast address
no range *A.B.C.D* [*A.B.C.D*]		Deletes a specified range of IGMP groups.

i A single IGMP group address is also possible.

IGMP Filtering Policy

To specify an action to permit or deny an access to an IGMP group range, use the following command.

Command	Mode	Description
{**permit** | **deny**}	IGMP Profile	Specifies an action for an IGMP group range.

Enabling IGMP Filtering

To enable IGMP filtering for a port, a configured IGMP profile needs to be applied to the port.

To apply an IGMP profile to ports to enable IGMP filtering, use the following command.

Command	Mode	Description
ip igmp filter port *PORTS* **profile** <1-2147483647>	Global	Applies an IGMP profile to ports PORTS: port number 1-2147483647: IGMP profile number
no ip igmp filter port *PORTS*		Releases an applied IGMP profile.

Before enabling IGMP filtering, please keep in mind the following restrictions.

- Plural IGMP profiles cannot be applied to a single port.
- IGMP snooping must be enabled before enabling IGMP filtering.
- To delete a created IGMP profile, all ports where the profile applied must be released.
- IGMP filtering only supports IGMPv2.

By the following command, OLT can permit or deny the IGMP packets by referring to its DHCP snooping binding table. This reference enables the system to permit IGMP messages only when the source IP address and MAC address of host have identified from the DHCP snooping binding table.

To permit/discard IGMP packets for the hosts authorized by the DHCP snooping, use the following command.

Command	Mode	Description
ip igmp filter port *PORTS* **permit dhcp-snoop-binding**	Global	Adds the entry to IGMP snooping table when it exists on the DHCP snooping binding table.
no ip igmp filter port *PORTS* **permit dhcp-snoop-binding**		Adds the entry to IGMP snooping table irrespective of DHCP snooping binding table.

To allow or discard IGMP messages by message type on a port, use the following command.

Command	Mode	Description
ip igmp filter port *PORTS* **packet –type** {**reportv1** | **reportv2** | **reportv3** | **query** | **leave** | **all**}	Global	Filters the specified IGMP messages on a port.
no ip igmp filter port *PORTS* **packet –type** {**reportv1** | **reportv2** | **reportv3** | **query** | **leave** | **all**}		Disables filtering the specified IGMP messages on a port.

9.2.7.2 IGMP Throttling

You can configure the maximum number of multicast groups that a host on a port can join. To specify the maximum number of IGMP groups per port, use the following command.

Command	Mode	Description
ip igmp max-groups port *PORTS* **count** <1-2147483647>	Global	Specifies the maximum number of IGMP groups for a port. PORTS: logical port number 1-2147483647: number of IGMP groups
ip igmp max-groups port sum count <1-2147483647>		Specifies the sum of IGMP groups for all of ports. sum: sum of all port counters
no ip igmp max-groups port {*PORTS* | **sum**}		Deletes a specified maximum number of IGMP groups.

To specify the maximum number of IGMP groups for the system, use the following command.

Command	Mode	Description
ip igmp max-groups system count <1-2147483647>	Global	Specifies the maximum number of IGMP groups for the system. 1-2147483647: number of IGMP groups
no ip igmp max-groups system		Deletes a specified maximum number of IGMP groups.

9.2.7.3 Displaying IGMP Filtering and Throttling

To display a configuration for IGMP filtering and throttling, use the following command.

Command	Mode	Description
show ip igmp filter [**port** *PORTS*]	Enable Global Bridge	Shows a configuration for IGMP filtering and throttling. PORTS: port number

To display existing IGMP profiles, use the following command.

Command	Mode	Description
show ip igmp profile [<1-2147483647>]	Enable Global Bridge	Shows existing IGMP profiles. 1-2147483647: IGMP profile number

9.2.8 IGMP Proxy

IGMP Proxy enables this L3 switch to issue IGMP host messages on behalf of hosts that the switch discovered through standard IGMP interfaces. The switch acts as a proxy for its hosts. The OLT supports IGMPv2.

IGMP Proxy can only work in a simple tree topology; where traffic is distributed to explicit upstream and downstream. You need to manually designate upstream and downstream interface on IGMP proxy switch. There are no multicast routers within the tree and the root of the tree is expected to be connected to a wider multicast infrastructure.

The IGMP proxy-enabled switch can deliver multicast traffic to the downward LANs or direct hosts without performing complex multicast routing protocol.

IGMP Proxy function is implemented with the following restrictions, so you must keep them in mind before setting IGMP Proxy related commands or parameters.

- It must be used only in a simple tree topology.
- User should manually set upstream and downstream interface for IGMP proxy opera tion.
- It doesn't support IGMPv3; if IGMPv3 runs on the interface, that interface should not be designated upstream and downstream interface of IGMP proxy switch. At the same time, if a certain interface is configured as upstream or downstream interface, IGMPv3 setting should not be made on that interface.
- It doesn't work with SSM mapping.
- IGMP proxy is a L3 feature and requires L3 interfaces to use for that function. Also, the **no shutdown** command should be preceded before configuring IGMP proxy in terfaces.
- If **ip igmp proxy-service sip first-reporter** is configured, the first reporter's source IP address of a group remains even though it leaves from the group. The information will be maintained until the group membership record is deleted.

9.2.8.1 Designating Downstream Interface

To specify the downstream interface for IGMP proxy operation, use the following command.

Command	Mode	Description
ip igmp mroute-proxy *NAME*	Interface	Designates the downstream interface of mroute proxy. NAME: interface name
no ip igmp mroute-proxy *NAME*		Release the downstream interface of mrouter proxy.

9.2.8.2 Designating Upstream Interface

To specify the upstream interface for IGMP proxy operation, use the following command.

Command	Mode	Description
ip igmp proxy-service *NAME*	Interface	Designates the upstream interfaces of mroute proxy. NAME: interface name
no ip igmp proxy-service		Releases the upstream interface of mroute proxy.

9.2.8.3 Configuring Upstream Interface Mode

When a single downstream interface is specified with multiple upstream interfaces, OLT supports two methods of IGMP proxy operation that are priority mode and load balancing mode. You can choose the way how to handle multicast traffic going to upstream interfaces. The priority mode is configured by default.

There are two modes for handling the multicast traffic toward upstream interfaces

- Priority mode: Each downstream interface joins one upstream interface of the highest priority based on its credit, priority and vid.
- Load balancing mode: It distributes multicast packets across multiple links of upstream interfaces with the largest credit value according to hash-threshold algorithm for IGMP group.

i

Every upstream interface has a credit unit value (default :100) and a priority. The upstream interfaces are specified a priority based on its credit value, the configured priority value and vid. The highest upstream interface has larger credit, higher priority and lower vid than other ones.

To specify the priority on an upstream interface, use the following command.

Command	Mode	Description
ip igmp proxy-service priority <0-255>	Interface	Specifies the priority on an upstream interface (default :0)
no ip igmp proxy-service priority		Deletes the configured priority of upstream interface.

To choose the upstream interface mode for IGMP proxy operation, use the following command.

Command	Mode	Description
ip igmp proxy-service multipath grpip	Global	Specifies load balancing mode for upstream interface
no ip igmp proxy-service multipath grpip		Specifies priority mode for upstream interface.

9.2.8.4 IGMP-Proxy IF Flap Discredit

IGMP IF is IGMP Proxy-enabled upstream or downstream interface that is used for IGMP proxy implementation.

IGMP IF flap discredit function is intended to apply a traffic flow penalty in IGMP interface due to its link down-up (Flap). All of IGMP IFs have 100 credit values by default.

An IGMP IF loses the specified credit value in case the flapping happens on this interface. Therefore, the forwarding path for the flow must be recalculated, causing low multicast forwarding performance.

Under the ECMP environment, if IGMP Proxy multi-uplink interface is load-balancing mode, a multicast traffic flow is split across the multipath according to the priority based on its credit unit value and configurations. The upstream interfaces with the largest credit would get the highest proxy-service priority.

If IGMP Proxy multi-uplink interface is specified the priority mode, one upstream interface of the highest priority based on its credit value, priority and vid handles a multicast traffic flow.

IGMP IF flap discredit function has been designed to minimize such a path recalculation caused by the IF flapping, which can increase the stability and quality for multicast service. Using this function, the OLT gives a discredit to a IGMP IF for every flapping time, and then the IF is not selected as a forwarding path until its credit is regenerated.

IGMP Proxy IF flap discredit function is implemented with the following restrictions, so you must keep them in mind before setting the related commands or parameters.

- If you configure recover-interval value as 0, the decreased IGMP IF credit is not recovered.
- If the credit unit becomes 0 because of the continuous flapping of IGMP IF, the credit is not recovered until **clear ip igmp if flap discredit** command is configured.

To enable/disable the IGMP IF flap discredit function, use the following command.

Command	Mode	Description
ip igmp if flap discredit	Global	Enables the IGMP IF flap discredit. (default)
no ip igmp if flap discredit		Disables the IGMP IF flap discredit.

To specify the discredit value in case of IGMP IF flapping, use the following command.

Command	Mode	Description
ip igmp if flap discredit unit <1-50>	Global	Specifies the discredit value for the IF flapping and decreases the credit unit as much as a specified value. (default: 5)
no ip igmp if flap discredit unit		Deletes a configured discredit value.

To set the IGMP IF flap credit regenerating rate, use the following command.

Command	Mode	Description
ip igmp if flap recover-interval <0-3600>	Global	Specifies the interval of recovering its credit as much as a specified value. (default: 10 seconds)
ip igmp if flap recover-unit <1-50>		Sets the regenerating value of the IF credit. (default: 5)
no ip igmp if flap {**recover-interval** | **recover-unit**}		Deletes a configured IF credit regenerating rate.

If you configure this rate as 0, the IGMP IF credit is not regenerated!

To set the current IGMP IF credit as the default (100), use the following command.

Command	Mode	Description
clear ip igmp if flap discredit [*NAME*]	Enable Global	Restores the current credit to a default value (100). NAME: IGMP interface name

9.2.8.5 Disabling Verification of Source IP of IGMP Packets

RPF (Reverse Path Forwarding) Check is basic operation to correctly forward multicast traffic down the distribution tree. A multicast router checks if the packet is received on the interface it would used to forward a unicast packet back to the source. If the RPF check is successful, the packet is forwarded. Otherwise, it is dropped.

However, IGMP Proxy switches do not perform RPF check on multicast traffic and only can verify if IGMP packets are received from connected network.

To disable the IGMP packet's source IP verification function, use the following command.

Command	Mode	Description
no ip igmp verify-sip	Global	Forwards IGMP packets without the source IP verification.
ip igmp verify-sip		Forwards IGMP packets after the source IP verification. If the source IP address is not within the incoming network segment, the packets are discarded. (default).

9.2.8.6 Specifying IGMP Report/Leave's Source IP Address

In IGMP proxy operation, the switch interacts with the router on its upstream interface through the exchange of IGMP messages on behalf of hosts and acts as the proxy. It performs the host portion of the IGMP task on the upstream interface by replacing the source IP address of IGMP messages, a membership report and leave group, with its own.

To specify the source IP address of IGMP membership report and leave group messages that is sent by IGMP proxy-service (upstream) interface, use the following command.

Command	Mode	Description
ip igmp proxy-service sip {*A.B.C.D* | **first-reporter**}	Interface	Configures the source IP address of IGMP membership report and leave group messages that is sent by proxy-service interface. A.B.C.D: Source IP address that manually entered by user first-reporter: Source IP address of the host that sent the first IGMP membership report. last-reporter: Source IP of the host that sent the last IGMP membership report. (Default : proxy-service interface IP address)
no ip igmp proxy-service sip		Removes the source IP configuration for IGMP membership report and leave group messages.

9.2.8.7 Querying with Real Querirer's Source IP Address

To send hosts queries with the actual source IP addresses, not with mroute-proxy interface's IP address, use the following command.

Command	Mode	Description
ip igmp mroute-proxy querier address proxy-service	Interface	Sets IGMP queries with original query's source IP address that is received on the mroute-proxy interface
no ip igmp mroute-proxy querier address proxy-service		Deletes the query's source IP configuration.

9.2.8.8 Displaying IGMP Proxy Information

To display IGMP proxy-service information, use the following command.

Command	Mode	Description
show ip igmp-proxy groups [**detail**]	Enable Global Bridge	Shows the IGMP group memberbership information of upstream interfaces. detail: IGMPv3 source infomation A.B.C.D: multicast group address NAME: interface name
show ip igmp-proxy groups *A.B.C.D* [**detail**]		
show ip igmp-proxy groups *NAME* [**detail**]		
show ip igmp-proxy groups [*NAME*] **summary**		

9.2.9 IGMP State Limit

You can use IGMP State Limit feature to limit the number of IGMP states that can be joined to a router on a per-interface or global level. Membership reports exceeding the configured limits are not entered into the IGMP cache and traffic for the excess membership reports is not forwarded.

To configure the IGMP State limit globally, use the following command.

Command	Mode	Description
ip igmp limit <1-2097152> [**except** {<1-99> | <1300-1999> | WORD}]	Global	Limits the number of IGMP membership reports globally: 1-2097152: the number of IGMP states allowed on a router 1-99: IP standard access list 1300-1999: IP standard access list (expanded) WORD: access list name
no ip igmp limit		Disables the globally configured IGMP state limit.

i If you want to exclude certain groups or channels from being counted against the IGMP limit so that they can be joined to an interface, use **except** option.

To configure the IGMP State limit on an interface, use the following command.

Command	Mode	Description
ip igmp limit <1-2097152> [**except** {<1-99> | <1300-1999> | WORD}]	Interface	Limits the number of IGMP membership reports on an interface: 1-2097152: the number of IGMP states allowed on a router (default:0) 1-99: IP standard access list 1300-1999: IP standard access list (expanded) WORD: access list name
no ip igmp limit		Disables a configured IGMP state limit per interface.

9.2.10 Multicast-Source Trust Port

Any port of OLT can be specified as a multicast-source trust port which is registered in the multicast forwarding table. Only multicast-source trust ports can be received the multicast traffic.

However, the reserved multicast packets should be sent to CPU even if these packets pass through a multicast-source trust port. This feature helps the switch to distinguish between general traffic receivers and multicast traffic receivers, and is a more efficient use of system resources because it sends the multicast traffic to specic hosts which want to receive the traffic.

To configure a specified port as a multicast-source trust port, use the following command.

Command	Mode	Description
ip multicast-source trust port *PORTS*	Global	Specifies multicast-source trust ports
no ip multicast-source trust port *PORTS*		Deletes the configured multicast-source trust ports

10 IPv6 Multicast

Multicast is the communication for a single or many source hosts to a specific group of destination hosts, which is interested in the information from the sources. This type of packet transmission can be deployed for a number of applications with more efficient utilization of the network infrastructure.

The point of implementing multicast is how to deliver source traffic to specific destinations without any burden on the sources or receivers using the minimized network bandwidth. The solution is to create a group of hosts with addressing the group, and to let the network determine how to replicate the source traffic to the receivers. The traffic will then be addressed to the multicast address and replicated to the multiple receivers by network devices.

An IPv6 multicast group is an arbitrary group of receivers that want to receive a particular data stream. This group has no physical or geographical boundaries--receivers can be located anywhere on the Internet or in any private network. Receivers that are interested in receiving data flowing to a particular group must join the group by signaling their local router. If you use these features IGMP in IPv4, This signaling is achieved with the MLD protocol in IPv6.

Routers use the MLD protocol to learn whether members of a group are present on their directly attached subnets. Hosts join multicast groups by sending MLD report messages. The network then delivers data to a potentially unlimited number of receivers, using only one copy of the multicast data on each subnet. IPv6 hosts that wish to receive the traffic are known as group members.

Packets delivered to group members are identified by a single multicast group address. Multicast packets are delivered to a group using best-effort reliability, just like IPv6 unicast packets.

The multicast environment consists of senders and receivers. Any host can send to a group. However, only the members of a group receive the message. A multicast address is chosen for the receivers in a multicast group. Senders use that address as the destination address of a datagram to reach all members of the group.

Membership in a multicast group is dynamic; hosts can join and leave at any time. There is no restriction on the location or number of members in a multicast group. A host can be a member of more than one multicast group at a time.

10.1 Multicast Listener Discovery (MLD)

The Multicast Listener Discovery (MLD) protocol is the multicast group management protocol for IPv6 and is used to exchange group information between multicast hosts and routers.

Multicast Listener Discovery (MLD) enables the IPv6 router to discover the presence of multicast listeners (that is, nodes wishing to receive multicast packets) on its directly attached links, and to discover specifically which multicast addresses are of interest to those neighboring nodes.

MLDv1 (RFC2710) is designed based on Internet Group Management Protocol version 2 (IGMPv2). MLDv2 (RFC3810) is designed based on IGMPv3. One important difference to note is that MLD uses ICMPv6 (IP Protocol 58) message types.

MLD Messages

There are three types of MLD messages of concern to the host-router interaction as shown below:

- **Query Message**
  A multicast router determines of any hosts are listening to a group by sending membership queries. The membership queries have two subtypes.
  - **General query**: In a query message, the multicast address field is set to 0 when MLD sends a general query. This is used to determine if any hosts are listening to any group.
  - **Multicast-address-specific query**: This is used to determine if any hosts are listening to a particular group. A group address is a multicast address.
- **Report Message**
  This is used by hosts to response to a query. The multicast address field is that of the specific IPv6 multicast address to which the sender is listening.
- **Done Message**
  This is used to indicate that a host stopped listening to a multicast address. The multicast address field is that of the specific IPv6 multicast address to which the source of the MLD message is no longer listening.

MLD has two versions that are supported by hosts and routers. MLD messages for each version are Query and Report types. Additionally, Done message is added to the version1.

The followings are the simple definitions of each version:

- **MLD Version 1**

MLDv1 is based on IGMP2.

0	4	8	16	32
Type		**Code**	**Checksum**	
Maximum Response Delay			**Reserved**	
Multicast Address (128 bits)				

Fig. 10.1 MLDv1 Message Format

MLDv1 Messages

- **Type**: MLD message types
  – **General query / Multicast-address-specific query message (ICMPv6 #130)**
  – **Multicast Listener report message (ICMPv6 #131)**
  – **Multicast Listener done message (ICMPv6 #132)**
- **Code**: This field is set to zero by the sender and ignored by receivers.
- **Checksum**: The standard ICMPv6 checksum, covering the entire MLD message of IPv6 header fields.
- **Maximum Response Delay**: This field is used only in Query messages, and specifies the maximum allowed delay before sending a responding Report, in units of milliseconds.
- **Multicast Address**
  – **In a Query message**: This field is set to zero when sending a General Query, and set to a specific IPv6 multicast address when sending a multicast-address-specific query.
  – **In a Report or Done message:** This field holds a specific IPv6 multicast address to which the message sender is listening to is ceasing to listen, respectively.

- **MLD Version 2**

MLDv2 is based on IGMP3. MLD v2 message consists of two messages as Listener Query and Listener Report. In addition, Query messages are classified into three types as General, Multicast-address-specific, Multicast-address-source-specific Query.

0 4 8 16 32

Type			**Code**	**Checksum**
Maximum Response Delay				**Reserved**
Multicast Address (128 bits)				
Reserved	**S**	**QRV**	**QQIC**	**Number of Sources (n)**
Source Address [1] 128bits				
…				
Source Address [n] 128bits				

Fig. 10.2 MLDv2 Query Message Format

MLDv2 Messages

• **S (S Flag; Suppress Router-Side Processing):** When a router sends or receives a query, it must update router's timer to reflect to correct timeout values for the multicast address or sources being queried. When set to one, the S Flag indicates to any receiving multicast routers that they have to suppress the normal timer updates they perform upon hearing a query.

• **QRV (Querier's Robustness Variable):** If this is non-zero, it contains the Robustness Variable value used by the sender of the Query. Routers should update their Robustness Variable to match the most recently received Query unless the value is zero.

• **QQIC (Querier's Query Interval Code):** This code is used to specify the Query Interval value used by the querier.

• **Number of Sources (n):** This field specifies how many source addresses are present in the Query. This number is zero in a General Query or a Multicast Address Specific Query, and non-zero in a Multicast Address and Source Specific Query. This number is limited by the network's MTU.

• **Source Address:** This fields are a vector of n IP unicast address, where n is the value in the value in the Number of Sources (N) field.

10.1.1 MLD Version

By default, this system runs MLDv2. To change the MLD protocol version on a current interface, use the following command.

Command	Mode	Description
ipv6 mld version <1-2>	Interface	Sets MLD version on a current interface. 1-2: MLD version (default: 2)
no ipv6 mld version		Returns to the default setting.

10.1.2 MLD Querier's Robustness Variable

You can statically configure the Querier's Robustness Variable (QRV) field in the query message. The MLD QRV allows tuning for the expected packet loss on a network. If a network is expected to be lossy, the QRV value may be increased. When receiving the query message that contains a certain QRV value from a querier, a host returns the report message as many as the specified QRV value.

To configure the QRV value on an interface, use the following command.

Command	Mode	Description
ipv6 mld robustness-variable <2-7>	Interface	Configures the MLD Querier's Robustness Variable (QRV) value on an interface. (default: 2)
no ipv6 mld robustness-variable		Deletes a specified MLD QRV value.

10.1.3 Clearing MLD Entry

To clear MLD entries, use the following command.

Command	Mode	Description
clear ipv6 mld	Enable Global	Deletes all MLD entries.
clear ipv6 mld if flap discredit [*IFNAME*]		Deletes MLD interface flapping.
clear ipv6 mld interface *IFNAME*		Deletes the MLD entries learned from a specified interface. IFNAME: interface name
clear ipv6 mld group {***** | *X:X::X:X* [*IFNAME*]}		Deletes MLD entries in a specified MLD group. *: all MLD groups *X:X::X:X*: MLD IPv6 group address

10.1.4 MLD Debug

To enable debugging of all MLD or a specific feature of MLD, use the following command.

Command	Mode	Description
debug mld {**all** | **decode** | **encode** | **events** | **fsm** | **tib**}	Enable	Enables MLD debugging. all: all MLD

		decode: MLD decoding encode: MLD encoding events: MLD events fsm: MLD Finite State Machine (FSM) tib: MLD Tree Information Base (TIB)
no debug mld {**all** | **decode** | **encode** | **events** | **fsm** | **tib**}		Disables MLD debugging.

i Tree Information Base (TIB) is the collection of state at a router that has been created by receiving MLD messages from local hosts.

To display the debugging information, use the following command.

Command	Mode	Description
show debugging mld snooping	Enable	Shows the debugging status of MLD.

10.1.5 MLD Access Control

Multicast routers send membership query messages to determine which multicast groups have members in the attached local networks of the router. If hosts respond to the queries, the routers then forward all packets addressed to the multicast group to these group members.

You can restrict hosts on a network to join multicast groups on the specified access list.

To control an access to multicast groups on an interface, use the following command.

Command	Mode	Description
ipv6 mld access-group *WORD*	Interface	Enables an MLD access-group control on an interface. WORD: IPv6 access list name
no ipv6 mld access-group		Disables a configured MLD access-group control.

10.1.6 MLD Querier Configuration

An MLD querier is the router periodically sends a General Query message for managing the multicast group. In MLD version1, the querier is a router with the lowest IPv6 address on the subnet. If the router hears no queries for the timeout period, it becomes the MLD querier.

10.1.6.1 MLD Query Interval

The MLD querier sends general query messages periodically to discover which multicast groups have members on the attached networks of the router.

To specify an interval to send MLD query messages, use the following command.

Command	Mode	Description
ipv6 mld query-interval <1-18000>	Interface	Specifies a general query interval. 1-18000: query interval (default: 125 seconds)
no ipv6 mld query-interval		Deletes a specified general query interval.

10.1.6.2 MLD Query Response Time

In MLD version 1 and 2, membership query messages include the maximum query response time field. This field specifies the maximum time allowed before sending a responding report. The maximum query response time allows a router to quickly detect that there are no more directly connected group members on a network segment.

To specify a maximum query response time advertised in membership query messages, use the following command.

Command	Mode	Description
ipv6 mld query-max-response-time <1-240>	Interface	Specifies a maximum query response time. 1-240: maximum response time (default: 10 seconds)
no ipv6 mld query-max-response-time		Deletes a specified maximum query response time.

10.1.6.3 MLD Querier Timeout

There should be a MLD querier on a network segment to prevent duplicating multicast traffic for connected hosts. When there are several routers, if the router has the lowest IPv6 address or if the router hears no queries during the timeout period, it becomes the querier.

To specify a timeout period before a router takes over as a querier for the interface after the previous querier has stopped querying, use the following command.

Command	Mode	Description
ipv6 mld querier-timeout <60-300>	Interface	Specifies an MLD queier timeout period. 60-300: MLD previous querier-timeout value (default: 255 seconds)
no ipv6 mld querier-timeout		Deletes a specified MLD queier timeout value.

10.1.6.4 MLD Last Member Query Count and Interval

When a host is not interested in receiving the multicast traffic for a particular group any more, it can explicitly leave the group by sending leave group messages.

Upon receiving a done message, a querier then sends out a Multicast-address-specific (MLDv1) or Multicast-address-source-specific query (MLDv2) message to determine if there is still any host interested in receiving the traffic. If there is no reply, the querier

stops forwarding the multicast traffic. However, MLD messages may get lost for various reasons, so you can specify the number of sending query messages and its interval.

To specify the number of sending Multicast-address-specific or Multicast-address-source-specific query messages, use the following command.

Command	Mode	Description
ipv6 mld last-member-query-count <2-7>	Interface	Specifies a last member query count. 2-7: last member query count value (default: 2)
no ipv6 mld last-member-query-count		Deletes a specified last member query count.

To specify the interval to send group-specific or group-source-specific query messages, use the following command.

Command	Mode	Description
ipv6 mld last-member-query-interval <1000-25500>	Interface	Specifies a last member query interval. 1000-25500: last member query interval (default: 1000 milliseconds)
no ipv6 mld last-member-query-interval		Deletes a specified last member query interval.

10.1.6.5 MLD Immediate Leave

Normally, a querier sends a Multicast-address-specific or Multicast-address-source-specific query message upon receipt of a done message from a host. If you want to set a leave latency as 0 (zero), you can omit the querying procedure. When the querying procedure is omitted, the router immediately removes the interface from the MLD cache for that group, and informs the multicast routing protocols.

To enable the MLD immediate leave feature on a current interface, use the following command.

Command	Mode	Description
ipv6 mld immediate-leave group-list *WORD*	Interface	Enables the MLD immediate leave. 1-99: IP standard access list 1300-1999: IP standard access list (extended range) WORD: IPv6 access list name
no ipv6 mld immediate-leave		Disables the IGMP immediate leave.

Use this command only on MLDv1 and MLDv2 interfaces to which one host is connected. If there is more than one host connected to a network segment through the same interface, and a certain host receives a done message, the router will remove all hosts on the interface from the multicast group. The router will lose contact with the hosts that should remain in the multicast group until they send join requests in response to the router's next general query.

10.1.6.6 MLD Static Join

The MLD static join feature has been developed to reduce the zapping time by statically creating a virtual host that behaves like a real on a port, even if there is no group member in the group where the port belongs. As a result, a multicast router realizes there is still group member, allowing multicast traffic to be permanently reachable on the group.

To configure the MLD static join, use the following command.

Command	Mode	Description
ipv6 mld static-group *X:X::X:X* **port** *PORT* [**source** {*SOURCE* | **ssm-map**]	Interface	Configures the MLD static join. X:X::X:X: MLD group address SOURCE: source address *X:X::X:X* reporter: host address
no ipv6 mld static-group *X:X::X:X* **port** *PORT* [**source** {*SOURCE* | **ssm-map**]		Deletes the configured MLD static join.

10.1.7 Displaying MLD Information

To display current MLD groups and relevant information, use the following command.

Command	Mode	Description
show ipv6 mld groups detail	Enable Global	Shows the multicast groups with receivers directly connected to the router and learned through MLD. X:X::X:X: IPv6 multicast group address IFNAME: interface name
show ipv6 mld groups X:X::X:X [**detail**]		
show ipv6 mld groups *IFNAME* [**detail**]		
show ipv6 mld groups *IFNAME* X:X::X:X [**detail**]		
show ipv6 mld interface *IFNAME*		

10.2 IPv6 Multicast Functions

This system provides various multicast functions including Layer 2 multicast forwarding, which allow you to achieve the fully effective and flexible multicast deployment.

10.2.1 Multicast Forwarding Database

Internally, this system forwards the multicast traffic referred to the multicast forwarding database (McFDB). The McFDB maintains multicast forwarding entries collected from multicast protocols and features, such as PIM, MLD etc.

10.2.1.1 Blocking Unknown Multicast Traffic

When certain multicast traffic comes to a port and the McFDB has no forwarding information for the traffic, the IPv6 multicast traffic is flooded to all ports by default. You can configure the switch not to flood unknown IPv6 multicast traffic.

To configure the switch to discard unknown IPv6 multicast traffic, use the following command.

Command	Mode	Description
ipv6 unknown-multicast block	Global	Configures the switch to discard unknown IPv6 multicast traffic. PORTS: unknown IPv6 multicast port number
ipv6 unknown-multicast port *PORTS*		
ipv6 unknown-multicast port *PORTS* **block**		
no ipv6 unknown-multicast block		Configures the switch to flood unknown IPv6 multicast traffic. (default) PORTS: unknown IPv6 multicast port number
no ipv6 unknown-multicast port *PORTS*		
no ipv6 unknown-multicast port *PORTS* **block**		

This command should not be used for the ports to which a multicast router is attached!

10.2.1.2 Forwarding Entry Aging

To specify the aging time for forwarding entries on the McFDB, use the following command.

Command	Mode	Description
ipv6 mcfdb aging-time <10-10000000>	Global	Specifies the aging time for forwarding entries on the McFDB. 10-10000000: IPv6 aging time (default: 300)
no ipv6 mcfdb aging-time		Deletes the specified aging time for forwarding entries.

To specify the maximum number of forwarding entries on the McFDB, use the following command.

Command	Mode	Description
ipv6 mcfdb aging-limit <256-65535>	Global	Specifies the maximum number of forwarding entries on the McFDB. 256-65535: number of entries (default: 5000)
no ipv6 mcfdb aging-limit		Deletes the specified maximum number of forwarding entries.

10.2.1.3 Displaying McFDB Information

To display McFDB information, use the following command.

Command	Mode	Description
show ipv6 mcfdb	Enable Global Bridge	Shows the current aging time and maximum number of forwarding entries.
show ipv6 mcfdb aging-entry [**vlan** *VLAN* | **group** *X:X::X:X*] [**mac-based** | **detail**]		Shows the current forwarding entries. VLAN: VLAN ID (1-4094) X:X::X:X: IPv6 multicast group address mac-based: lists entries on a MAC address basis

To clear multicast forwarding entries, use the following command.

Command	Mode	Description
clear ipv6 mcfdb [* | **vlan** *VLAN*]	Enable Global	Clears multicast forwarding entries. *: all forwarding entries VLAN: VLAN ID (1-4094)
clear ipv6 mcfdb vlan *VLAN* **group** *X:X::X:X* **source** *X:X::X:X*		Clears a specified forwarding entry. group: : IPv6 multicast group address source: IPv6 address

10.2.2 MLD Snooping Basic

Layer 2 switches normally flood multicast traffic within the broadcast domain, since it has no entry in the Layer 2 forwarding table for the destination address. Multicast addresses never appear as source addresses, therefore the switch cannot dynamically learn multicast addresses. This multicast flooding causes unnecessary bandwidth usage and discarding unwanted frames on those nodes which did not want to receive the multicast transmission. To avoid such flooding, MLD snooping feature has been developed.

The purpose of MLD snooping is to constrain the flooding of multicast traffic at Layer 2. MLD snooping, as implied by the name, allows a switch to snoop the MLD transaction between hosts and routers, and maintains the multicast forwarding table which contains the information acquired by the snooping. When the switch receives a join request from a host for a particular multicast group, the switch then adds a port number connected to the host and a destination multicast group to the forwarding table entry; when the switch receives a done message from a host, it removes the entry from the table.

10.2.2.1 Enabling MLD Snooping

You can enable MLD snooping globally or on each interface respectively. By default, MLD snooping is globally disabled.

To enable MLD snooping, use the following command.

Command	Mode	Description
ipv6 mld snooping	Global	Enables MLD snooping globally.
	Interface	Enables MLD snooping on the interface.

To disable MLD snooping, use the following command.

Command	Mode	Description
no ipv6 mld snooping	Global	Disables MLD snooping globally.
	Interface	Disables MLD snooping on the interface.

10.2.2.2 MLD Snooping Version

The membership reports sent to the multicast router are sent on the basis of the MLD snooping version of each interface. If you statically specify the MLD snooping version on a certain interface, the reports are always sent out only with the specified version.

If you do not statically specify the MLD snooping version, and a MLD version 1 query is received on the interface, the interface actively sends out a version 1 report to the router. If MLD snooping version 1 query is not consistently received on the interface for a timeout period (400 seconds), the interface version goes back to its default version (2).

To specify the static MLD snooping version, use the following command.

Command	Mode	Description
ipv6 mld snooping version <1-2>	Interface	Configures the MLD snooping version globally. 1-2: MLD snooping version (default: 2)

To delete the specified static MLD snooping version, use the following command.

Command	Mode	Description
no ipv6 mld snooping version	Interface	Deletes the specified MLD snooping version and returns to the default version.

10.2.2.3 MLD Snooping Robustness Value

The robustness variable allows you can tune to reflect expected packet loss on a congested network. If a network is expected to be lossy, you can increase the robustness variable to increase the number of times that packets are resent.

When receiving the query message that contains a certain robustness variable from an MLD snooping querier, a host returns the report message as many as the specified robustness variable.

To configure the robustness variable, use the following command.

Command	Mode	Description
ipv6 mld snooping robustness-variable <2-7>	Interface	Configures the robustness variable. (default: 2)

To delete a specified robustness variable, use the following command.

Command	Mode	Description
no ipv6 mld snooping robustness-variable	Interface	Deletes a specified robustness variable.

10.2.3 MLD Snooping

10.2.3.1 MLD Snooping Querier Configuration

MLD snooping querier should be used to support MLD snooping in a VLAN where PIM and MLD are not configured.

When the MLD snooping querier is enabled, the MLD snooping querier sends out periodic general queries that trigger membership report messages from a host that wants to receive multicast traffic. The MLD snooping querier listens to these membership reports to establish appropriate forwarding.

Enabling MLD Snooping Querier

To enable the MLD snooping querier, use the following command.

Command	Mode	Description
ipv6 mld snooping querier	Interface	Enables the MLD snooping querier.

To disable the MLD snooping querier, use the following command.

Command	Mode	Description
no ipv6 mld snooping querier	Interface	Disables the MLD snooping querier.

i If you do not specify a source address of an MLD snooping query, the IP address configured on the VLAN is used as the source address by default.

MLD Snooping Query Response Time

MLDv1/v2 membership query messages include the maximum query response time field. This field specifies the maximum time allowed before sending a responding report. The maximum query response time allows a router to quickly detect that there are no more hosts interested in receiving multicast traffic.

To specify a maximum query response time advertised in general query messages, use the following command.

Command	Mode	Description
ipv6 mld snooping query-max-response-time <1-240>	Interface	Specifies a maximum query response time. 1-240: maximum response time (default: 10 seconds)

To delete a specified maximum query response time, use the following command.

Command	Mode	Description
no ipv6 mld snooping query-max-response-time	Interface	Deletes a specified maximum query response time and resets the default.

10.2.3.2 MLD Snooping Fast Leave

Fast-leave can be used to speed up the reaction to MLD leave announcements.

This minimizes the leave latency of group memberships on an interface, as the switch does not send group-specific queries. As a result, the group entry is removed from the forwarding table as soon as a group done message is received.

To enable the MLD snooping fast leave, use the following command.

Command	Mode	Description
ipv6 mld snooping fast-leave	Interface	Enables the MLD snooping fast leave.

The MLD snooping fast-leave function is available only in the MLDv1 host.

In fast-leave processing, when there is more than one MLD host belonging to a group, and a certain host sends a done message, the MLD snooping querier will remove all host entries from the forwarding table. The switch lose contact with the hosts that should remain from the forwarding table until they send join requests in response to the switch's next general query message.

So, it is recommended that you use the fast leave command only if there is one receiver behind the interface for a given group.

To disable the MLD snooping fast leave, use the following command.

Command	Mode	Description
no ipv6 mld snooping fast-leave	Interface	Disables the MLD snooping fast leave.

10.2.3.3 MLD Snooping Last Member Query Interval

Upon receiving a done message, a switch with MLD snooping then sends out a multicast-address-specific query (MLDv1) or multicast-address-source-specific query (MLDv2) message to determine if there is still any host interested in receiving the traffic. If there is no reply, the switch stops forwarding the multicast traffic. However, MLD messages may get lost for various reasons, so you can specify an interval to send query messages.

To specify an interval to send multicast-address-specific or multicast-address-source-specific query messages, use the following command.

Command	Mode	Description
ipv6 mld snooping last-member-query-interval <1000-25500>	Interface	Specifies a last member query interval. 1000-25500: last member query interval value (default: 1000 milliseconds)

To delete a specified an interval to send multicast-address-specific or multicast-address-source-specific query messages, use the following command.

Command	Mode	Description
no ipv6 mld snooping last-member-query-interval	Interface	Deletes a specified last member query interval.

10.2.3.4 MLD Snooping Report Suppression

If an MLD querier sends general query messages, and hosts are still interested in the multicast traffic, the hosts should return membership report messages. For a multicast router, however, it is sufficient to know that there is at least one interested member for a group on the network segment. Responding a membership report per each of group members may unnecessarily increase the traffic on the network; only one report per

group is enough.

When the MLD snooping report suppression is enabled, a switch suppresses membership reports from hosts other than the first one, allowing the switch to forward only one membership report in response to a general query from a multicast router.

To enable the MLD snooping report suppression, use the following command.

Command	Mode	Description
ipv6 mld snooping report-suppression	Interface	Enables the MLD snooping report suppression.

To disable the MLD snooping report suppression, use the following command.

Command	Mode	Description
no ipv6 mld snooping report-suppression	Interface	Disables the MLD snooping report suppression.

10.2.3.5 Multicast Router Port Configuration

The multicast router port is the port which is directly connected to a multicast router. A switch adds multicast router ports to the forwarding table to forward membership reports only to those ports.

Static Multicast Router Port

You can statically configure Layer 2 port as the multicast router port which is directly connected to a multicast router, allowing a static connection to a multicast router.

To specify a multicast router port, use the following command.

Command	Mode	Description
ipv6 mld snooping mrouter port *PORTS*	Interface	Specifies a multicast router port. PORTS: port number

To delete a specified multicast router port, use the following command.

Command	Mode	Description
no ipv6 mld snooping mrouter port *PORTS*	Interface	Deletes a specified multicast router port.

Displaying Multicast Router Port

To display a current multicast router port for MLD snooping, use the following command.

Command	Mode	Description
show ipv6 mld snooping	Enable	Shows a current multicast router port for MLD snooping

mrouter *IFNAME*	Global	globally. IFNAME: VLAN interface name

10.2.4 MLD State Limit

You can use MLD State Limit feature to limit the number of MLD states that can be joined to a router on a per-interface or global level. The MLD group limits feature provides protection against DoS (denial of service) attacks caused by MLD packets. Membership reports exceeding the configured limits are not entered into the MLD cache and traffic for the excess membership reports is not forwarded.

To limit the number of MLD state globally, use the following command.

Command	Mode	Description
ipv6 mld limit <1-2097152> [**except** *WORD*]	Global	Limits the number of MLD membership reports globally. 1-2097152: the number of MLD states allowed on a router. (Default: 0) WORD: IPv6 access list name
no ipv6 mld limit		Disables the globally configured MLD state limit.

i

If you want to exclude certain groups or channels from being counted against the MLD limit so that they can be joined to an interface, use **except** option.

To limit the number of MLD state on an interface, use the following command.

Command	Mode	Description
ipv6 mld limit <1-2097152> **[except** *WORD* **]**	Interface	Limits the number of MLD membership reports on an interface. 1-2097152: the number of MLD states allowed on an interface (default:0) WORD: IPv6 access list name
no ipv6 mld limit		Disables the configured MLD state limit per interface.

10.2.5 MLD Snooping Debug

To enable the debugging of all MLD or a specific feature of the MLD, use the following command.

Command	Mode	Description
debug mld snooping {all | decode | encode | fsm | tib | events}	Enable	Enables MLD snooping debugging.

To disable the MLD snooping debugging, use the following command.

Command	Mode	Description
no debug mld snooping {all | decode | encode | fsm | tib | events}	Enable	Disables MLD snooping debugging.

To display the debugging information, use the following command.

Command	Mode	Description
show debugging mld snooping	Enable	Shows the debugging status of MLD.

10.2.6 MLD-Proxy IF Flap Discredit

MLD IF is MLD Proxy-enabled upstream or downstream interface that is used for MLD proxy implementation.

MLD IF flap discredit function is intended to apply a traffic flow penalty in MLD interface due to its link down-up (Flap). All of MLD IFs have 100 credit values by default.

A MLD IF loses the specified credit value in case the flapping happens on this interface. Therefore, the forwarding path for the flow must be recalculated, causing low multicast forwarding performance.

Under the ECMP environment, if MLD Proxy multi-uplink interface is load-balancing mode, a multicast traffic flow is split across the multipath according to the priority based on its credit unit value and configurations. The upstream interfaces with the largest credit would get the highest proxy-service priority.

If MLD Proxy multi-uplink interface is specified the priority mode, one upstream interface of the highest priority based on its credit value, priority and vid handles a multicast traffic flow.

MLD IF flap discredit function has been designed to minimize such a path recalculation caused by the IF flapping, which can increase the stability and quality for multicast service. Using this function, the OLT gives a discredit to a MLD IF for every flapping time, and then the IF is not selected as a forwarding path until its credit is regenerated.

MLD Proxy IF flap discredit function is implemented with the following restrictions, so you must keep them in mind before setting the related commands or parameters.

- If you configure recover-interval value as 0, the decreased MLD IF credit is not recovered.
- If the credit unit becomes 0 because of the continuous flapping of MLD IF, the credit is not recovered until **clear ipv6 mld if flap discredit** command is configured.

To enable/disable the MLD IF flap discredit function, use the following command.

Command	Mode	Description
ipv6 mld if flap discredit	Global	Enables the MLD IF flap discredit. (default)

no ipv6 mld if flap discredit		Disables the MLD IF flap discredit.

To specify the discredit value in case of MLD IF flapping, use the following command.

Command	Mode	Description
ipv6 mld if flap discredit-unit <1-50>	Global	Specifies the discredit value for the IF flapping and decreases the credit unit as much as a specified value. (default: 5)
no ipv6 mld if flap discredit-unit		Deletes a configured discredit value.

To set the MLD IF flap credit regenerating rate, use the following command.

Command	Mode	Description
ipv6 mld if flap recover-interval <0-3600>	Global	Specifies the interval of recovering its credit as much as a specified value. (default: 10 seconds)
ipv6 mld if flap recover-unit <1-50>		Sets the regenerating value of the IF credit. (default: 5)
no ipv6 mld if flap {**recover-interval** | **recover-unit**}		Deletes a configured IF credit regenerating rate.

If you configure this rate as 0, the MLD IF credit is not regenerated!

To set the current MLD IF credit as the default (100), use the following command.

Command	Mode	Description
clear ipv6 mld if flap discredit [*NAME*]	Enable Global	Restores the current credit to a default value (100). NAME: MLD interface name

11 GPON Configuration

Gigabit Passive Optical (GPON) technology has the active network elements OLT (Optical Line Termination) at the central office and ONU/ONT (Optical Network Unit / Termination) at the subscriber site.

Typical GPON configuration consists of a single PON port at the OLT and a number of ONUs connected to it over a single fiber feeder.

Generally, a Time Division Multiplexing (TDM) is used in the downstream data transmission. OLT broadcasts data to every ONUs using TDM approach. Every ONU receives each downstream frame and pinks up only that data addressed to it by the OLT.

To deliver data to OLT in upstream direction, the OLT implements a Time Division Multiple Access (TDMA) approach. ONU (ONT) receives data from the user ports and combines them into bursts. Each ONU (ONT) transmits its data in a strict accordance with the Bandwidth Map generated by OLT for the synchronization. Using DBA mechanism OLT can rearrange upstream bandwidth to provide more resources to those ONU tightly loaded with traffic.

The ONU provides network termination for a Passive Optical Network (PON) in the home or business. The ONU connects via a high speed interface to the PON network and provides subscriber access to data (Ethernet), voice (POTS) and video services. GPON gives edge networks an unparalleled bandwidth advantage in their ability to offer truly high speed triple play service (i.e. voice, video and data) especially when compared with existing cable or DSL services.

The following figure is the example of the GPON network set up.

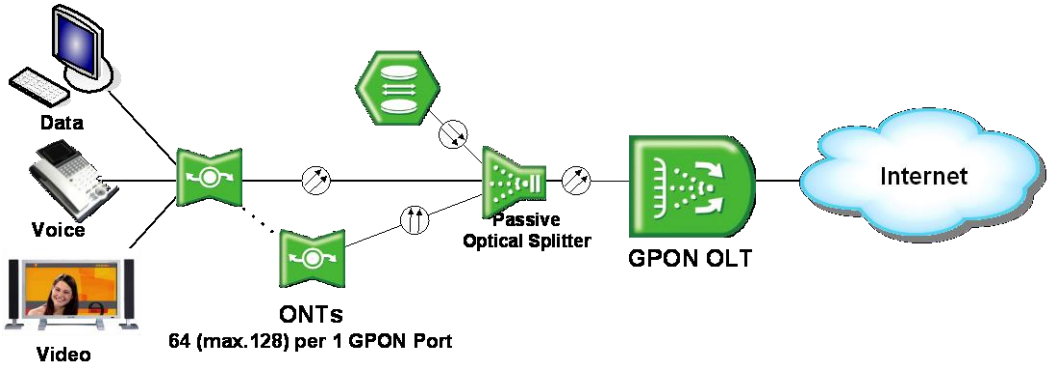


Fig. 11.1 Example of GPON Network

Basic Operation

- Configure OLT and ONU (ONT) in *GPON-OLT Configuration* mode.
- For common ONU (ONT) configuration, create a profile in *ONU Profile Configuration* mode.
- If the created profile is modified, the profile will be applied to the ONUs (ONTs) automatically.

Specifying OLT and ONU ID

When specifying an OLT ID in the CLI, you can simply put the number in the form of *PORT number* such as **1**, **2**, **3**, **4…7, 8**. Multiple input is also possible, e.g. **1, 2, 3** or **3-4**.

When specifying an ONU ID, just remember that the ONU ID is always between 1 and 128 or ONU serial number. Multiple input for the ONU ID is the same as the ONU ID, e.g. **1-3**, **8-22, FRKW1100282d**.

CLI Structure

To configure GPON functionalities, enter the **gpon** command in *Global Configuration* mode. The *GPON Configuration* mode is a stage of preparation for the detail PON configuration. In this mode, you can open *ONU/PM/Traffic/VoIP/DBA Profile Configuration* mode or *GPON-OLT Configuration* mode.

Fig. 11.2 shows the CLI structure of *GPON Configuration* mode.

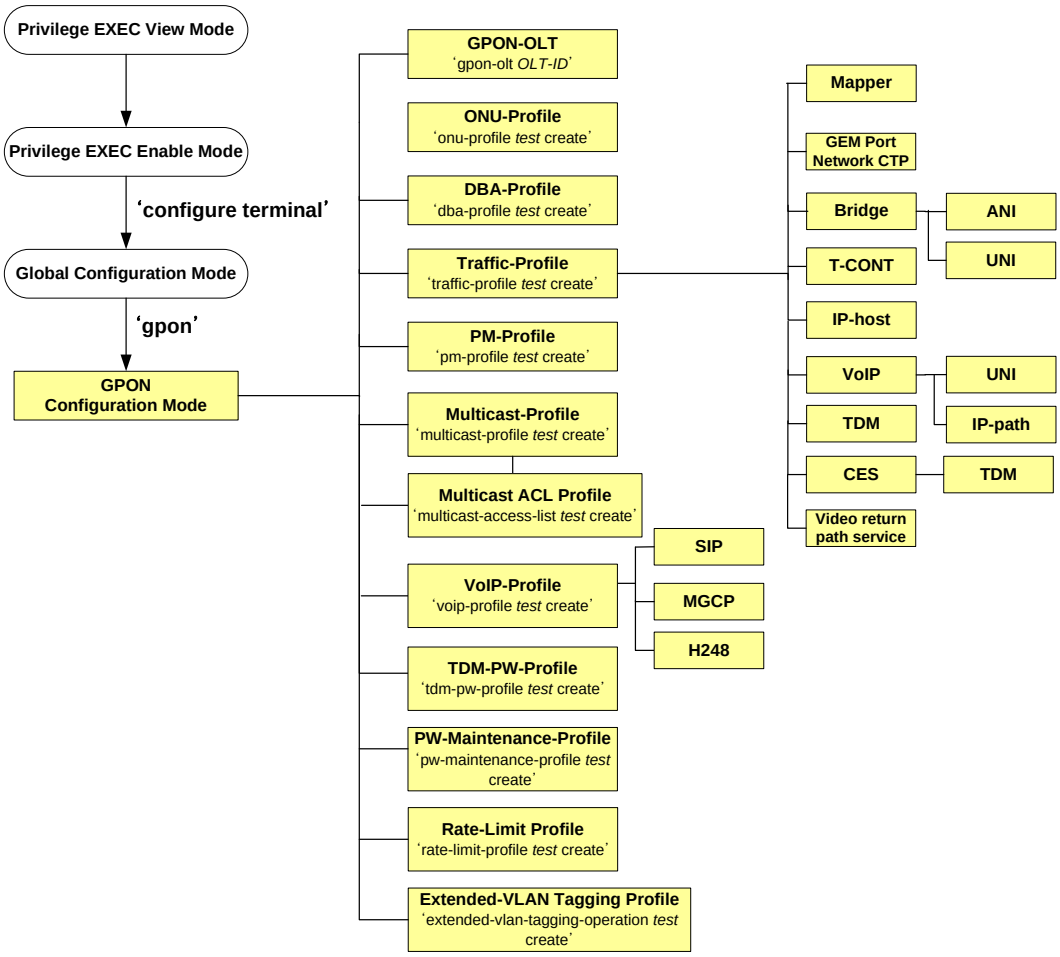


Fig. 11.2 CLI Structure of *GPON Configuration* Mode

The following shows the main commands of *GPON Configuration* mode.

```
SWITCH(config)# gpon
SWITCH(gpon)# ?
GPON configuration commands:
  clear                           Reset functions
  dba-profile                     Configure GPON DBA Profile
  debug                           Debugging functions
  do                              To run exec commands in config mode
  exit                            End current mode and down to previous mode
  extended-vlan-tagging-operation Configure Extended Vlan Tagging Operation
                                  (ME:171)
  gpon-olt                        Configure GPON-OLT
  help                            Description of the interactive help system
  multicast-profile               Configure Multicast Operation Profile
                                  (ME:309)
  no                              Negate a command or set its defaults
  olt                             OLT configuration
  onu                             ONU configuration
  onu-profile                     Configure GPON Profile
  pm-profile                      Configure GPON Performance Monitor Profile
  pw-maintenance-profile          Configure GPON PW Maintenance Private Profile
  remove                          Remove file
  show                            Show running system information
  tdm-pw-profile                  Configure GPON TDM PW Private Profile
  traffic-profile                 Configure GPON Traffic Profile
  voip-profile                    Configure VoIP Private Profile
  write                           Write running configuration to memory or
terminal

SWITCH(gpon)#
```

To open *GPON Configuration* mode, use the following command.

Command	Mode	Description
gpon	Global	Opens *GPON Configuration* mode.

11.1 OLT Management

This section describes how to manage an OLT. The OLT is managed in *GPON-OLT Configuration* mode.

11.1.1 Opening OLT Mode

To open *GPON-OLT Configuration* mode and enable an OLT, use the following command.

Command	Mode	Description
gpon-olt *OLT-ID*	GPON GPON-OLT	Opens *GPON-OLT Configuration* mode. OLT-ID: GPON port number (e.g. 1, 2, 3, 4)

11.1.1.1 OLT Description

To specify or modify a description of an OLT, use the following command.

Command	Mode	Description
olt description *DESCRIPTION*	GPON-OLT	Registers the OLT's description.
no olt description		Deletes the description of OLT.

To display a description of an OLT, use the following command.

Command	Mode	Description
show olt description [*OLT_ID*]	Enable/Global/GPON	Shows the OLT's description.
show olt description	GPON-OLT	

11.1.1.2 Activating OLT

To activate/deactivate an OLT, use the following command.

Command	Mode	Description
olt activate	GPON-OLT	Activates a specified OLT.
olt deactivate		Deactivates a specified OLT.

11.1.2 Downstream Encryption

This command requires a special request to operate and only available once negotiated. ONU encryption function is disabled by default.

Encryption of downstream data is automatic process performed by OLT for specified ONU-IDs configured as encrypted. GPON OLT uses encryption key of the ONU (ONT) associated with encrypted OLT-ID. To synchronize encryption and decryption keys between OLT and ONU (ONT), you have to activate the key exchange process. For security reasons, GPON standard requires periodic key exchange for all active ONUs (ONTs) that use downstream data traffic.

To enable/disable the encryption mode of downstream traffic, use the following command.

Command	Mode	Description
onu encryption *ONU-ID* **enable**	GPON-OLT	Enables the encryption mode. ONU-ID: ONU ID (1 to 128) or ONU serial number
onu encryption *ONU-ID* **disable**		Disables the encryption mode.

To start/stop an encryption key exchange process between OLT and ONU (ONT) and specify an interval of key exchange, use the following command.

Command	Mode	Description
olt key-exchange start <10-	GPON-OLT	Starts an encryption key exchange process between

3600>		OLT and ONU and specifies an exchange interval. 10-3600: interval for encryption key switchover
olt key-exchange stop		Stops periodic process of encryption key exchange.

To display the status of encryption mode or information of the encryption key exchange process, use the following command.

Command	Mode	Description
show onu encryption *OLT-ID*	Enable Global GPON	Shows the status of encryption mode. OLT-ID: GPON port number ONU-ID: ONU ID (1 to 128) or ONU serial number
show onu encryption [*ONU-ID*]	GPON-OLT	
show olt key-exchange [*OLT-ID*]	Enable Global GPON	Shows the configured interval and the encryption key exchange process information.
show olt key-exchange	GPON-OLT	

11.1.3 OLT Bandwidth

11.1.3.1 Upstream Bandwidth

To set the total amount of bandwidth in use for upstream traffic, use the following command.

Command	Mode	Description
olt total upstream-bw <1031616-1244160>	GPON-OLT	Sets the total amount of bandwidth in use for upstream traffic. 1031616-1244160: total upstream bandwidth (default: 1120000kbps)
no olt total upstream-bw		Deleted the configured total amount of bandwidth in use for upstream traffic.

To display the information of OLT's total upstream bandwidth, use the following command.

Command	Mode	Description
show olt total upstream-bw *OLT-ID*	Enable Global GPON	Shows the total upstream bandwidth of OLT
show olt total upstream-bw	GPON-OLT	

11.1.3.2 Bandwidth Scheduler

To allocate the bandwidth of the best effort traffic according to the fairness criterion, use the following command.

Command	Mode	Description
olt bw-scheduler be-fairness-method {**guaranteed** | **maximum**}	GPON-OLT	Configures the bandwidth scheduler. be-fairness-method: best effort fairness method configuration guaranteed: according to guaranteed bw maximum: according to maximum bw

To display the status of OLT's bandwidth scheduler, use the following command.

Command	Mode	Description
show olt bw-scheduler [*OLT-ID*]	Enable Global GPON	Shows the status of OLT's bandwidth scheduler.
show olt bw-scheduler	GPON-OLT	

11.1.4 Auto ONU Fault Detection

If a certain ONU's laser is enabled consistently by an optical module's fault, all other normal ONUs connected to the same OLT will be deregistered; a single ONU fault may cause a whole network disruption. Preventing such a problem, the OLT provides the auto ONU (ONT) fault detection feature. Normally, if an ONU (ONT) fault occurs, a specific error signal is followed by the fault. Thus, the OLT validates whether an ONU (ONT) fault occurs by detecting the specific error signal. The auto ONU fault detecting mechanism is as follows:

When detecting an error signal (an ONU fault) in a certain OLT, the OLT generates a corresponding syslog message, and then disables the laser of each ONU currently connected to the OLT one by one for 60 seconds. At the moment that the faulty ONU's laser is disabled, the error signal also disappears, then the system realizes that which the faulty ONU is and memorizes its serial number. After 60 seconds, when the disconnected ONUs (ONTs) start to enable their laser, if the ONU having the same serial number memorized before tries to enable its laser, the OLT disables the laser permanently. To resume the laser, the ONU needs a power reset.

To enable/disable the auto ONU fault detection, use the following command.

Command	Mode	Description
olt signal-check {**enable** | **disable**}	GPON-OLT	Enables/disables the auto ONU (ONT) fault detection. (When an ONU fault occurs, the system will only generate the syslog message.)

olt signal-check auto-onu-block {**enable** | **disable**}		Enables/disables the auto ONU (ONT) fault detection. (When an ONU fault occurs, the system will disable the ONU's laser permanently.)

To display a current configuration of the auto ONU fault detection, use the following command.

Command	Mode	Description
show olt signal-check *OLT-ID*	Enable Global GPON	Shows a current configuration of the auto ONU (ONT) fault detection.
show olt signal-check	GPON-OLT	

To guarantee a right operation of this feature, the OLT and an ONU (ONT) loaded with the newest firmware are needed.

11.1.5 Maximal Distance between OLT and ONU (ONT)

PON systems distribute the bandwidth of each fiber core among up to 64 (max.128) line termination points using splitters. The actual maximum distance between OLT and ONU (ONT) is typically 20 km. The logical handling of GPON data streams however allows a distance of up to 60 km.

To determine maximal GPON distance between OLT and ONU (ONT), use the following command.

Command	Mode	Description
olt max-distance default	GPON-OLT	Determine maximal distance between OLT and ONU. default: 0-20km 20-60: maximal distance (km)
olt max-distance <20-60>		

11.1.6 Forward Error Correction (FEC) Mode

Forward Error Correction (FEC) feature can improve the quality and reach of an optical link. FEC is implemented according to G984.3 standard, which defines the use of the code which is able to protect 239 bytes of the payload with 16 redundant bytes, allowing the receiver to detect and correct transmission errors.

To enable/disable downstream FEC mode, use the following command.

Command	Mode	Description
olt fec-mode ds enable	GPON-OLT	Enables downstream FEC mode per OLT ID.
olt fec-mode ds disable		Disables downstream FEC mode per OLT ID.

To enable/disable upstream FEC mode, use the following command.

Command	Mode	Description
olt fec-mode up enable	GPON-OLT	Enables upstream FEC mode per OLT ID. (Available max. bandwidth: 918912 Kbps)
olt fec-mode up disable		Disables upstream FEC mode per OLT ID.

11.1.7 MAC Aging Time

To manage a MAC table in the OLT system, use the following command.

Command	Mode	Description
olt mac aging-time <30-86400>	GPON-OLT	Specifies MAC aging time. 30-86400: aging time (default: 300s)

11.1.8 OLT Link Down Detection

If the power of ONU is turned off by user, this ONU is supposed to send the alarm message of dying-gasp to OLT. When the last ONU is deregistered from the OLT after it generates an alarm by ONU dying-gasp event, we can regard that the link of this GPON port is down and it's not the cable connection problem.

To enable/disable GPON link down detection, use the following command.

Command	Mode	Description
olt cable-down enable	GPON	Enables GPON link down detection
olt cable-down disable		Disables GPON link down detection

To set a number of ONUs that are deregistered without dying-gasp alarm message for detecting the PON link of OLT, use the following command.

Command	Mode	Description
olt cable-down reference-count <1-8>	GPON	Sets the number of deregistered ONUs without sending dying-gasp alarms. The numbers indicate the abnormal behavior that the link of GPON port is down. 1-8: count of inactive ONU (default: 3)
no olt cable-down reference-count		Deletes a configured number of deregistered ONUs and returns to the default value.

i To use this feature, the dying-gasp alarms should be enabled for each GPON-OLT node.

To display the state of GPON link down detection, use the following command.

Command	Mode	Description
show olt cable-down	Enable Global GPON	Shows the configuration of GPON link down detection.

11.1.9 Maximum Number of ONU

You can set the maximum number of ONUs (ONTs) connected to a specified OLT. To set the maximum number of ONUs, use the following command.

Command	Mode	Description
olt max-onu-count <1-128>	GPON-OLT	Sets the maximum number of ONU connections. 1-128: maximum number of ONUs connected to a specified OLT (default: 128)
no olt max-onu-count		Removes the maximum number of ONU.

To display the configured maximum number of ONUs, use the following command.

Command	Mode	Description
show olt max-onu-count [*OLT-ID*]	Enable Global GPON	Shows the configured maximum number of ONUs.
show olt max-onu-count	GPON-OLT	

11.1.10 OLT Anti-Spoofing

When the OLT learns the same MAC address from the two (or more) different ONUs on the same GPON, the system regards the latest ONU(s) as the fault operation, and make the ONU(s) block the inflow of sub-level MAC by MAC filtering. Through this anti-spoofing, the OLT can prevent the malicious spoofing attack.

To enable/disable the OLT anti-spoofing, use the following command.

Command	Mode	Description
olt anti-spoofing enable [**expire-timeout** <60-65535>]	GPON-OLT	Enables the OLT anti-spoofing. 60-65535: expire timeout (= MAC filtering operation time). After the configured expiration, the OLT system can learn again the MAC regarded as a fault.
olt anti-spoofing disable		Disables the OLT anti-spoofing.

To clear MAC filtering due to the anti-spoofing operation, use the following command.

Command	Mode	Description
clear olt anti-spoofing	GPON-OLT	Clears MAC filtering being operated currently occurred by anti-spoofing function.
clear olt anti-spoofing *ONU-ID*		

[*MAC VID*]		ONU-ID: ONU ID (1-128) or serial number MAC: MAC address VID: VID

To display the user configuration of the OLT anti-spoofing, use the following command.

Command	Mode	Description
show olt anti-spoofing [*OLT-ID*]	Enable Global GPON	Shows the user configuration of the OLT anti-spoofing.
show olt anti-spoofing	GPON-OLT	

To display the current OLT anti-spoofing status, use the following command.

Command	Mode	Description
show olt anti-spoofing status *OLT-ID*	Enable Global GPON	Shows the current anti-spoofing MAC filtering status per ONU, MAC and VID.
show olt anti-spoofing status	GPON-OLT	

11.1.11 Downstream Traffic Control

The OLT provides the function to control the downstream traffic based on MAC address and VLAN ID by each OLT. Basically, the OLT system creates MAC table through MAC learning with the incoming traffic from ONU, and transmits the downstream traffic to GEM port with the MAC table information. However, OLT can control this downstream traffic with MAC address and VLAN ID by user configuration.

To configure the downstream traffic control, use the following command.

Command	Mode	Description
olt ds-gem-mapping {**mac** | **mac-vid** | **vid** | **per-flow** [**key-mac**| **key-mac-vid**]}	GPON-OLT	Configures the GEM port mapping mode. mac, mac-vid: GEM port mapping with destination MAC address or destination MAC address and VLAN ID vid: GEM port mapping with VLAN ID (default: mac)
onu vlan-gem-mapping *ONU-ID* **vid** *RANGE* **mapper** *MAPPER-ID*		Maps GEM port of ONU and VLAN ID. (This configuration is valid only when the GEM port mapping mode is specified as 'vid' and the GEM port is assigned through ONU profile configuration.) ONU-ID: ONU ID or serial number RANGE: VLAN ID range (This value should be unique by each OLT port.) MAPPER-ID: mapper number configured on Traffic Profile
onu vlan-gem-mapping all vid *RANGE* {**multicast-gem** |		Maps the multicast or broadcast GEM port used by all ONUs and the specified VLAN ID.

broadcast-gem}		RANGE: VLAN ID range
no onu vlan-gem-mapping [*ONU-ID* [**vid** *RANGE*] | **all** [**vid** *RANGE*]]		Deletes the GEM port mapping configuration above.

i The traffic is not transmitted while the GEM port mapping mode is being changed due to user configuration.

To configure the downstream GEM port mode per flow, use the following command.

Command	Mode	Description
olt per-flow vid *RANGE* **mapping-method** {**mac** | **mac-vid** | **vid**}	GPON-OLT	Configures a downstream GEM port mapping based on flow.
no olt per-flow [**vid** *RANGE*]		Deletes the configured downstream GEM port mapping per flow.

If the OLT is configured in the downstream GEM mapping mode per flow, you can configure downstream QoS mapping mode based on MAC address / VLAN ID and the mapping between queue and CoS value. To configure the downstream traffic control by QoS mapping, use the following command.

Command	Mode	Description
olt ds-qos-mapping mode {**mac** | **vid** }	GPON-OLT	Configures the downstream QoS mapping mode. (This configuration is valid only when the downstream GEM port mapping mode is specified as 'flow'.) mac: QoS mapping mode based on destination MAC address vid: QoS mapping mode based on VLAN ID mac vid: QoS mapping mode based on MAC + VLAN ID
olt ds-qos-mapping queue-count {**2** | **4** | **8**} [**cos-map** <0-7> <0-7> <0-7> <0-7> <0-7> <0-7> <0-7> <0-7>]		Configures the queue count and priority value according to CoS value. 2 | 4 | 8 : queue count 0-7 : queue number per each CoS value (CoS 0 to CoS 7)
no olt ds-qos-mapping mode		Deletes the QoS mapping configuration mode.
no olt ds-qos-mapping		Deletes the queue count and CoS-Queue mapping table.

i The traffic is not transmitted while the GEM port mapping mode is being changed due to user configuration.

To display the configuration of downstream traffic control, use the following command.

Command	Mode	Description

show olt ds-gem-mapping [*OLT-ID*]	Enable Global GPON	Shows the GEM port mapping mode configured on the OLT.
show olt ds-gem-mapping	GPON-OLT	
show onu vlan-gem-mapping [*ONU-ID*]		Shows VLAN ID mapped to GEM port of ONU.
show olt per-flow [*VLANS*]		Shows the downstream GEM Port mode per flow.

To display the configuration of downstream QoS mapping, use the following command.

Command	Mode	Description
show olt ds-qos-mapping [*OLT-ID*]	Enable Global GPON	Shows the queue count and CoS-Queue mapping table of the GPON OLT.
show olt ds-qos-mapping mode [*OLT-ID*]		Shows the QoS mapping mode configured on the OLT.
show olt ds-qos-mapping	GPON-OLT	Shows the queue count and CoS-Queue mapping table status.
show olt ds-qos-mapping mode		Shows the downstream QoS mapping mode.

To configure the traffic control by selecting the method of upstream flow mapping, use the following command.

Command	Mode	Description
olt us-flow-mapping per-mapper	GPON-OLT	Selects the upstream flow mapping based on mapper. This method learns MAC addresses of incoming traffic from the several GEM port IDs associated with different ONUs to a MAPPER-defined GEM port ID.
olt us-flow-mapping per-gem		Selects the upstream flow mapping based on GEM port. This method learns MAC addresses of incoming traffic from the GEM port IDs associated with different ONUs to each GEM port ID, respectively.

To display the configured upstream flow mapping, use the following command.

Command	Mode	Description
show olt us-flow-mapping [*OLT-ID*]	Enable Global GPON	Shows the upstream flow mapping status.
show olt us-flow-mapping	GPON-OLT	

11.1.12 Multicast/Broadcast GEM Port Separation

All the downstream multicast and broadcast flows from the OLT are transmitted through a single GEM port ID. The multicast and broadcast flows need to be separated from each

other to properly forward all broadcast/multicast traffic for multiple ONTs.

To configure a multicast GEM port ID, use the following command.

Command	Mode	Description
olt multicast-gem <4094-4095>	GPON	Adds a specific GEM port ID to the multicast stream. 4094-4095: multicast GEM port ID
show olt multicast-gem	GPON GPON-OLT	Shows the specified GEM port ID for multicast stream.

To enable/disable the interworking with IGMP snooping table, use the following command.

Command	Mode	Description
olt interwork igmp-snooping {**enable** | **disable**}	GPON	Enables/disables the interworking with IGMP snooping table.

To add a static MAC address into the MAC table, use the following command.

Command	Mode	Description
olt static-mac *MACADDR* {**mcast** | **bcast**} [**vid** <1-4094>]	GPON-OLT	Adds a static MAC address for multicast/broadcast stream.
olt static-mac start *MACADDR* **end** *MACADDR* {**mcast** | **bcast**} [**vid** <1-4094>]		Adds a static range of MAC addresses for multicast/broadcast stream.
no olt static-mac *MACADDR* {**mcast** | **bcast**} [**vid** <1-4094>]		Deletes the configured static MAC address.
no olt static-mac start *MACADDR* **end** *MACADDR* {**mcast** | **bcast**} [**vid** <1-4094>]		Deletes the configured static MAC address range.

To display the configured static MAC address table, use the following command.

Command	Mode	Description
show olt static-mac *OLT-ID*	Enable Global GPON GPON-OLT	Shows the static MAC table.

11.1.13 Configuring Port/TCONT Threshold

When one GPON port is connected to a lot of ONTs with T-CONTs and GEM ports, you can specify the maximum numbers (threshold) of T-CONTs and GEM port count. So that an alarm is generated if a given threshold is exceeded.

To configure the threshold of GEM port count, use the following command.

Command	Mode	Description

olt threshold port <1-3966>	GPON-OLT	Sets the threshold of GEM port count for ONT. 1-3966 : threshold value
no olt threshold port		Deletes the configured threshold of GEM port.

To configure the threshold of dynamic / fixed T-CONT count for ONT, use the following command.

Command	Mode	Description
olt threshold tcont dynamic *DYNAMIC_VALUE* [**fixed** *FIXED_VALUE*]	GPON-OLT	Sets the threshold of Dynamic/Fixed T-CONT count for ONT. DYNAMIC_VALUE: 1 to 384 FIXED_VALUE: 1 to 384
olt threshold tcont fixed *FIXED_VALUE* [**dynamic** *DYNAMIC_VALUE*]		
no olt threshold tcont {**dynamic** | **fixed**}		Deletes the configured threshold of T-CONT count.

To display the configuration of GEM-port/ T-CONT threshold, use the following command.

Command	Mode	Description
show olt threshold port [*OLT-ID*]	Enable Global GPON	Shows the configured GEM-port/ T-CONT count threshold of ONTs.
show olt threshold tcont [*OLT-ID*]		
show olt threshold port	GPON-OLT	
show olt threshold tcont		

11.1.14 ONU Deactivation Monitoring

ONU deactivation monitoring function generates alarms based on ONU (ONT)'s deactivation. The system calculates the current percentage by the number change of active ONUs every hour. If the number of active ONU is reduced and the current percent is lower than a given alarm-raise percent, the deactive monitor alarm is on. If the current percent exceeds the configured alarm-clear percent, the deactive monitor alarm changes to off. To enable/disable ONU deactivation monitoring, use the following command.

Command	Mode	Description
olt deactive-monitor {**enable** | **disable**}	GPON-OLT	Enables/disables ONU deactivation monitoring function.

To configure ONU deactivation monitoring, use the following command.

Command	Mode	Description
olt deactive-monitor alarm-raise <1-99>	GPON-OLT	Sets the deactive ONU-raise percent. 1-99: (default: 30%)
olt deactive-monitor alarm-clear<1-99>		Sets the deactive ONU-clear percent. If the current percent becomes higher than this value, the alarm

		status changes to off. 1-99: (default: 70%)
olt deactive-monitor period <10-86400>		Sets the deactive ONU monitoring period. If the current percent is higher than a alarm-raise percent, the alarm is off and the current percent changes to 100% after a period. 10-86400: deactive ONU monitoring period (default: 10 seconds)
no olt deactive-monitor alarm-raise		Deletes the configured value of deactive ONU monitoring parameters.
no olt deactive-monitor alarm-clear		
no olt deactive-monitor period		

To display the configuration of ONU deactivation monitoring, use the following command.

Command	Mode	Description
show olt deactive-monitor [*OLT-ID*]	Enable Global GPON	Shows the configuration of ONU deactivation monitoring.
show olt deactive-monitor	GPON-OLT	

To clear the alarms of ONU deactivation monitoring, use the following command.

Command	Mode	Description
clear olt deactive-monitor alarm	GPON-OLT	Clears the collected alarms by ONU deactivation monitoring.

11.1.15 OLT Bit Error Ratio (BER)

You can configure the monitor direction and the alarm threshold of the bit error ratio. The system generates a bit error ratio (BER) alarm when the total number of error bits or bit error rate of the data transferred between the OLT and ONUs exceeds the alarm threshold. Both uplink and downlink data between OLT and ONU can be monitored.

To configure the OLT Bit Error Ratio (BER), use the following command.

Command	Mode	Description
olt ber ds-interval <1000-10000> [**olt ber sd-threshold** <4-9>] [**olt ber sf-threshold** <3-8>] [**olt ber us-interval** <1000-10000>]	GPON-OLT	Specifies the monitor direction and interval of the bit error ratio. ds-interval: Downstream BER interval from OLT to ONU us-interval: Upstream BER interval from ONU to OLT 1000-10000: downstream BER interval value (default: 5000ms) 1000-10000: upstream BER interval value (default: 2000ms)
olt ber us-interval <1000-10000> [**olt ber ds-interval** <1000-10000>] [**olt ber sd-threshold** <4-9>] [**olt ber sf-threshold** <3-8>]		

olt ber sd-threshold <4-9> [**olt ber ds-interval** <1000-10000>] [**olt ber us-interval** <1000-10000>] [**olt ber sf-threshold** <3-8>]		Sets the threshold for reporting of signal degrade (SD) BER or signal fail (SF) BER alarms. 4-9: SD threshold value (default: 8) 3-8: SF threshold value (default: 7)
olt ber sf-threshold <3-8> [**olt ber ds-interval** <1000-10000>] [**olt ber us-interval** <1000-10000>] [**olt ber sd-threshold** <4-9>]		

To display the information of OLT Bit Error Ratio (BER), use the following command.

Command	Mode	Description
show olt ber [*OLT-ID*]	Enable Global GPON	Shows OLT's Bit Error Ratio (BER) configuration (including upstream/downstream BER interval and threshold).
show olt ber	GPON-OLT	

11.1.16 OMCC Monitoring

If an error occurs on the ONT Management and Control Channel (OMCC), the OLT attemps to recover from an error and the ONUs are deactivated by the OLT until the OMCC is recovered.

To enable/disable the OMCC recovery monitoring function with ONU deactivation process, use the following command.

Command	Mode	Description
olt omcc-recovery enable	GPON-OLT	Enables the OMCC recovery monitoring function with ONU deactivation process.
olt omcc-recovery threshold <5-720>		Sets the threshold limit for OMCC recovery attempts. 5-720: the number of times OLT can atttemp to retry OMCC recovery (default: 5)
olt omcc-recovery mode deactivation		Sends the deactivation PLOAM when OLT detects the OMCC problem.
olt omcc-recovery mode reset		Sends the specific (ONT reset) PLOAM when OLT detects the OMCC problem.
olt omcc-recovery disable		Disables the OMCC recovery monitoring function with ONU deactivation process.

i

Disabling OMCC recovery monitoring with **olt omcc-recovery disable** command provides the data transmission service between OLT and ONU without ONU deactivation process even if an error occurs on the OMCC.

To display the information of OMCC recovery monitoring, use the following command.

Command	Mode	Description
show olt omcc-recovery [*OLT-ID*]	Enable Global GPON	Shows the status of OMCC recovery monitoring.
show olt omcc-recovery	GPON-OLT	

To configure the force MIB upload option to resolve the ONU deactivation issue because of OMCC error, use the following command.

Command	Mode	Description
onu mib-upload *ONU-ID*	GPON-OLT	Configures the force MIB upload of ONU to resolve the ONU deactivation caused by OMCC error.

11.1.17 PLOAM Message

To send a physical layer OAM (PLOAM) message to a specific ONU ID for debugging, use the following command.

Command	Mode	Description
olt specific-ploam*ONU-ID MSG_ID DATA*	GPON-OLT	Sends the PLOAM message to a specific ONU ID for ONU-ID: ONU ID number used in PLOAM messages (1-255) MSG_ID: Downstream PLOAM message ID value or private PLOAM ID defined by the G.984.3 (1-255) DATA: 10 bytes HEX

11.1.18 OLT Flow Control

To enable the flow control mode of an OLT, use the following command.

Command	Mode	Description
olt flow-contorl ds enable	GPON-OLT	Enables the down stream flow of OLT. (default: off)
olt flow-contorl ds disable		Disables the dowm stream flow .

To display the configured flow control mode of an OLT, use the following command.

Command	Mode	Description
show olt flow-contorl [*OLT-ID*]	GPON GPON-OLT	Shows the flow control information.

11.1.19 Transceiver Type Configuration

To configure the transceiver type of OLT, use the following command.

Command	Mode	Description
olt transceiver-type {fujitsu | neophotonics | neophotonics-a | hisense | optowiz | superxon | wtd | sourcephotonics}	GPON-OLT	Configures the transceiver type of OLT port.
show olt transceiver-type [*OLT_ID*]	Enable Global GPON GPON-OLT	Shows the transceiver type of OLT.

11.1.20 Statistics GEM Configuration

To configure the statistics gem avg of OLT, use the following command.

Command	Mode	Description
olt statistics gem avg {update-interval {<60-3600> | **one-time**}}	GPON-OLT	Configures the statistics GEM average of OLT. 60-3600: Update-interval in seconds. one-time: Configure update-interval one time.
no olt statistics gem avg		Deletes the statistics GEM average of OLT.

To display statistic gem avg, use the following command.

Command	Mode	Description
show olt statistics gem avg [*OLT-ID*]	GPON-OLT	Shows the statistic gem avg.
show olt gem avg [*OLT-ID*]	Enable Global GPON GPON-OLT	

11.1.21 Displaying OLT Information

To display GPON OLT information, use the following command.

Command	Mode	Description
show olt status [*OLT-ID*]	Enable Global GPON GPON-OLT	Shows the information of active/inactive GPON OLT IDs.

The following is an example of displaying active/inactive OLT IDs of the OLT.

```
SWITCH(gpon)# show olt status
-------------------------------------------------------------
 OLT_ID |  Status   |  Protect  | Distance | FEC mode(DS/US)
-------------------------------------------------------------
   1    |   Active |          |   20 Km |  enable/disable
   2    |   Active |          |   20 Km |  enable/disable
   3    |   Active |          |   20 Km |  enable/disable
   4    |   Active |          |   20 Km |  enable/disable
SWITCH(gpon)# show olt status 2
-------------------------------------------------------------
 OLT_ID |  Status   |  Protect  | Distance | FEC mode(DS/US)
-------------------------------------------------------------
   2     |   Active |          |   20 Km |  enable/disable
SWITCH(gpon)#
```

The Received Signal Strength Indication (RSSI) is a measurement of the power present in a received radio signal. The RSSI functionality in a newly released GPON OLT transceiver helps the operators monitor the received optical signal strength from each ONU (ONT).

To display the received signal power information from an ONU, use the following command.

Command	Mode	Description
show olt rx-power *OLT-ID* [*ONU-ID*]	Enable Global GPON	Shows OLT Rx signal power from an ONU.
show olt rx-power [*ONU-ID*]	GPON-OLT	Shows OLT Rx signal power from an ONU.

The following is an example of displaying the OLT RX power information of ONU ID 3.

```
SWITCH(config-gpon-olt[1])# show olt rx-power 3
----------------------------
  ONU  |     Rx Power
 ----------------------------
 3     | -16.0033 dBm
SWITCH(config-gpon-olt[1])#
```

11.1.21.1 OLT Traffic Statistics

To display traffic statistics of an OLT, use the following command.

Command	Mode	Description
show olt statistics *OLT-ID*	Enable/Global/GPON	Shows traffic statistics of an OLT.
show olt statistics	GPON-OLT	

show olt statistics onu *OLT-ID ONU-ID*	Enable/Global/GPON	Shows traffic statistics of a specified ONU (ONT) collected by an OLT.
show olt statistics onu *ONU-IDs*	GPON-OLT	
show olt statistics activation *OLT-ID*	Enable/Global/GPON	Shows traffic statistics of GPON activation data.
show olt statistics activation	GPON-OLT	
show olt statistics alarm *OLT-ID* [*ONU-IDs*]	Enable/Global/GPON	Shows the ONU alarm counter data. ONU-ID: ONU ID (1-128) or ONU serial number
show olt statistics alarm [*ONU-IDs*]	GPON-OLT	

The following is an example of displaying traffic statistics of the OLT 1.

```
SWITCH(config-gpon-olt[1])# show olt statistics

--------------------------------------------------------------------------------
OLT :  1                                Downstream            Upstream
--------------------------------------------------------------------------------
(Pon counter)
 Pon valid eth packets                 1829234499              N/A
 Pon CPU packets                         136329               N/A
 Pon ploams                              108609            19201764
 Pon invalid packets                        N/A                 2

 (perfomance monitoring counter)
 Rx valid packets                     1830563926              N/A
 Rx error packets                            0               N/A
 CPU valid packets                       1301425            1309616
 CPU dropped packets                           0                 0
 MAC loopup miss                               0               N/A
 Priority Q0 forwarded packets         1829262862         6507975825
 Priority Q0 dropped packets                   0                 0
 Priority Q1 forwarded packets                 0                 0
 Priority Q1 dropped packets                   0                 0
 Priority Q2 forwarded packets                 0                 0
 Priority Q2 dropped packets                   0                 0
 Priority Q3 forwarded packets                 0                 0
-more-
SWITCH(config-gpon-olt[1])#
```

To clear collected statistics, use the following command.

Command	Mode	Description
clear olt statistics [*OLT-ID*]	GPON-OLT	Clears collected traffic statistics of an OLT.
clear olt statistics activation		Clears the collected traffic statistics of GPON activation data.
clear olt statistics alarm [*OLT-ID*]		Clears the collected traffic statistics of alarm counter data.
clear olt statistics onu [*OLT-ID*]		Clears the traffic statistics collected by an OLT.

11.1.21.2 MAC Address

To display the MAC addresses and a total MAC entry counts of the ONUs (ONTs) connected to a current OLT, use the following command.

Command	Mode	Description
show olt mac	Enable Global GPON	Shows the MAC addresses of ONUs (ONTs) connected to OLT
show olt mac *OLT-ID* [*ONU-IDs*]		
show olt mac count		Shows the number of MAC entries of ONUs (ONTs) connected to a specified OLT.
show olt mac count *OLT-ID* [*ONU-IDs*]		

To add a MAC address of the ONUs (ONTs) connected to a current OLT, use the following command.

Command	Mode	Description
olt add-mac *ONU-ID MACADDR VLAN GEM-PORT*	GPON-OLT	Adds the static MAC addresses of ONU. ONU-ID: ONU ID (1-128) or serial number GEM-PORT: GEM port ID

To display a MAC address of the ONUs (ONTs) connected to a current OLT, use the following command.

Command	Mode	Description
show olt mac [*ONU-ID*]	GPON-OLT	Shows the MAC addresses currently learned on ONU. ONU-ID: ONU ID (1-128) or serial number VLANS: VLAN ID
show olt mac *ONU-ID* [*VLANS*]		
show olt mac count [*ONU-IDs*]		Shows the number of MAC addresses currently learned on a specified ONT.

To clear MAC addresses learned on a current OLT, use the following command.

Command	Mode	Description
clear olt mac [*ONU-ID*]	GPON-OLT	Clears MAC addresses learned on a current OLT.
clear olt mac *ONU-ID* [*MACADDR VLAN*]		Clears MAC addresses of specified ONU (ONT). MACADDR: MAC address VLAN: vlan ID

11.1.21.3 GPON Daemon Memory Usage

To display the memory usage of GPON, use the following command.

Command	Mode	Description
show memory gpon	Enable Global	Shows the memory usage of GPON daemon.

	Bridge	

11.1.21.4 GPON Profile Count

To display the total number of GPON-based profiles, use the following command.

Command	Mode	Description
show profile count	Enable Global GPON	Shows the profile list and the sum of saved GPON-based profiles.

11.2 ONU Management

This section describes how to manage an ONU (ONT). The OLT provides the centralized remote ONU (ONT) management concept, so you can manage every remote ONU (ONT) connected to the OLT without any local configuration for the ONUs (ONTs).

11.2.1 ONU Registration

The default ONU (ONT) registration mode is the auto mode in which an OLT registers ONUs automatically, when receiving the serial number from the ONU. For an optimized ONU configuration, however, the manual mode is recommended. Some options are only available in the manual mode.

The OLT is able to register ONU (ONT) automatically and manually.

- By default, the OLT registers ONUs automatically when the ONU is connected through its serial number registration. In this case, ONU ID is also given.
- Administrator can register specific ONUs (ONTs) manually with MAC address or serial number.

11.2.1.1 Activating/deactivating ONU

To activate/deactivate the ONU(ONT), use the following command.

Command	Mode	Description
onu activate *ONU-ID*	GPON-OLT	Activates the specified ONU ID.
onu deactivate *ONU-ID*		Deactivates the specified ONU ID.

11.2.1.2 ONU Registration Method

There are several methods to register an ONU. You use a different method to recognize an existing ONU during subsequent activations. For example, authenticating a newly activated ONU by serial number allows for increased security during normal operation, whereas authenticating an ONU by registration ID (PLOAM password) allows for flexibility during installation and repair.

To specify the ONU registration method, use the following command.

Command	Mode	Description
onu activation-mode serial-number	GPON	Configures the ONU's serial-number based registration mode. (default)
onu activation-mode registration-id		Configures the ONU's registration ID based registration mode.
onu activation-mode loid		Configures the ONU's logical ONU identification based registration mode.

i You should remove all ONU database before changing the ONU registration method.

Serial Number-based ONU Registration

For ONU (ONT) registration, OLT requests a serial number of the connected ONUs (ONTs) periodically. OLT registers a specific ONU which replies to OLT with its serial number. The OLT can allocate ONU-ID to an ONU which sends a valid serial number to OLT. When ONU with the specific serial number is activated, it is assigned the allocated ONU-ID.

To register/delete ONU (ONT) automatically by ONU's serial number acquisition, use the following command.

Command	Mode	Description
discover-serial-number start <1-1200>	GPON-OLT	Starts to register ONT by its serial number and specifies an interval for ONU's serial number acquisition. 1-1200: serial number acquisition interval
discover-serial-number stop		Stops discovering ONT using its serial number.
show discover-serial-number interval [*OLT-ID*]	Enable Global GPON	Shows the configured interval for requesting ONU's serial number.
show discover-serial-number interval	GPON-OLT	

To remove the serial number of ONU, use the following command.

Command	Mode	Description
onu remove serial-number *ONU-ID*	GPON-OLT	Removes the ONU serial number. ONU-ID: ONU ID (1-128) or ONU serial number

Registration ID-based ONU Registration

A registration ID is assigned to a subscriber at the management level, and provisioned both into the OLT and communicated to installation or repair personnel or even to the subscriber directly. The registration ID populates the ONU's PLOAM password, which is used by the OLT to recognize the ONU. The OLT may learn the value of the ONU's serial number for possible subsequent use in serial number based authentication.

To enter the registration ID into the ONU in the field, use the following command.

Command	Mode	Description
onu add *ONU-ID* **registration-id** *ID*	GPON-OLT	Adds ONU (ONT) with a specified resgistration ID. ID: registration ID (PLOAM password)

Logical ONU ID (LOID)-based ONU Registration

The operation of logical ONU ID (LOID) method is similar as registration ID (RID) method as both the OLT and the ONU agree on a pre-defined logical ID but LOID is more flexible

because it allows up to 24 characters to store information.

Similarly, ONU is registered first in the OLT with a specific and uniquelogical ID and this one must be also locally configured to ONU via ONT's Web UI. The logical ID includes two parts: an LOID (Logical ONU ID) and a Password.

So the OLT and the network management system based on logical identification of the ONU authentication should support two kinds of configuration: only LOID and LOID + Password.

To register ONU automatically by ONU's serial number acquisition, use the following command.

Command	Mode	Description
discover-serial-number start <1-1200>	GPON-OLT	Starts discovering ONT using its serial number. 1-1200: serial number acquisition interval
discover-serial-number stop		Stops discovering ONT using its serial number.

To register ONU by LOID or LOID + PASSWORD mode, use the following command.

Command	Mode	Description
onu add *ONU-ID* **loid** *LOID*	GPON-OLT	Adds ONU with specific LOID ONU-ID: 1-128 LOID: 1-24 characters
onu add *ONU-ID* **loid** *LOID PASSWORD*		Add ONU with specific LOID and Password LOID: 1-24 characters PASSWORD: 1-12 characters

i Also, the LOID and Password must be configured locally in ONT's Web UI.

To display LOID information of ONU, use the following command.

Command	Mode	Description
show onu loid status [*OLT_ID*]	Enable Global	Shows the ONU's loid information.
show onu loid status [*ONU_ID*]	GPON-OLT	

Displaying ONU Info Registered

To display the registered ONU (ONT) information, use the following command.

Command	Mode	Description
show onu active [*OLT-ID*]	Enable Global GPON	Shows the registered ONU (ONT) information. OLT-ID: GPON port number
show onu active count [*OLT-ID*]		Shows the number of active ONUs connected to a specified GPON port.
show onu active all [*OLT-ID*]		Shows the ONU information registered in manual and

		auto mode in case of configured as LOID mode.
show onu unprovisioned [*OLT-ID*]		Shows the ONU information registered in auto mode in case of configured as LOID mode.
show onu active [*ONU-ID*]	GPON-OLT	Shows the registered ONU information. Shows the ONU information registered in manual mode in case of configured as LOID mode. ONU-ID: ONU ID (1 to 128) or ONU serial number
show onu active all		Shows the ONU information registered in manual and auto mode in case of configured as LOID mode.
show onu unprovisioned		Shows the ONU information registered in auto mode in case of configured as LOID mode.
show onu active count		Shows the number of active ONUs.

The following is the sample output of displaying the ONUs connected to the OLT 1.

```
SWITCH(config-gpon-olt[1])# show onu active
--------------------------------------------------------------------------------
 OLT | ONU |  STATUS  |  MODE  |  Serial No.  |      Password      |  Link uptime
--------------------------------------------------------------------------------
 1   |   1 | Inactive | manual | CIGG09140025 | 00000000000000000000 | 00:00:00
 1   |   2 | Inactive | manual | FRKW11002829 | 00000000000000000000 | 00:00:00
 1   |   3 | Inactive | manual | CIGG09140017 | 00000000000000000000 | 00:00:00
 1   |   4 | Inactive | manual | CIGG92500094 | 00000000000000000000 | 00:00:00
 1   |   5 |   Active |   auto | FRKW1100282d | 00000000000000000000 | 00:03:34
-more-
SWITCH(config-gpon-olt[1])#
```

The following is the sample output of displaying the ONUs in case of configured as LOID mode.

```
SWITCH(config-gpon-olt[1])# show onu active all
--------------------------------------------------------------------------------
---
  OLT | ONU |  STATUS  |  MODE  |  Serial No.  |    Password(R-ID)    |  Link uptime
--------------------------------------------------------------------------------
---
    1 |   1 |   Active |   auto | FISA4b09a034 | 00000000000000000000 |   0:00:01:03
    1 |   2 |   Active |   auto | FRKW67006190 | 30303030303030310000 |   0:00:00:01
    1 |   3 |   Active |   auto | FRKW826f72ec | 20202020202020202020 |   0:00:01:02
    1 |   4 |   Active |   auto | FRKW4bf30c9e | 00000000000000000000 |   0:00:01:02
    1 |   5 |   Active |   auto | FRKW8e97df00 | 00000000000000000000 |   0:00:01:02
    1 |   6 |   Active |   auto | FRKW4bf7a600 | 00000000000000000000 |   0:00:01:02
    1 |   7 |   Active |   auto | FRKW82091123 | 20202020202020202020 |   0:00:01:02
    1 |   8 |   Active |   auto | FRKW5a010001 | 00000000000000000000 |   0:00:01:01
    1 |   9 |   Active | manual | FRKW68149d98 | 30303030303030310000 |   0:00:00:56
    1 |  10 |   Active |   auto | FRKW82010001 | 20202020202020202020 |   0:00:01:01
-more-
SWITCH(config-gpon-olt[1])#
```

```
SWITCH(config-gpon-olt[1])# show onu active
```

```
----------------------------------------------------------------------------------------
---
  OLT | ONU |  STATUS  |  MODE  |  Serial No.  |    Password(R-ID)    |  Link uptime
----------------------------------------------------------------------------------------
---
    1 |   9 |  Active | manual | FRKW68149d98 | 30303030303030310000 |   0:00:01:02


SWITCH(config-gpon-olt[1])# show onu active 7-11
----------------------------------------------------------------------------------------
---
  OLT | ONU |  STATUS  |  MODE  |  Serial No.  |    Password(R-ID)    |  Link uptime
----------------------------------------------------------------------------------------
---
    1 |   9 |  Active | manual | FRKW68149d98 | 30303030303030310000 |   0:00:01:10


SWITCH(config-gpon-olt[1])# show onu unprovisioned
-------------------------------------------------------------------------------
---
  OLT | ONU |  STATUS  |  MODE  |  Serial No.  |    Password(R-ID)    |  Link uptime
----------------------------------------------------------------------------------------
---
    1 |   1 |  Active |  auto | FISA4b09a034 | 00000000000000000000 |   0:00:01:27
    1 |   3 |  Active |  auto | FRKW826f72ec | 20202020202020202020 |   0:00:01:26
    1 |   4 |  Active |  auto | FRKW4bf30c9e | 00000000000000000000 |   0:00:01:26
    1 |   5 |  Active |  auto | FRKW8e97df00 | 00000000000000000000 |   0:00:01:26
    1 |   6 |  Active |  auto | FRKW4bf7a600 | 00000000000000000000 |   0:00:01:26
    1 |   7 |  Active |  auto | FRKW82091123 | 20202020202020202020 |   0:00:01:26
    1 |   8 |  Active |  auto | FRKW5a010001 | 00000000000000000000 |   0:00:01:25
    1 |  10 |  Active |  auto | FRKW82010001 | 20202020202020202020 |   0:00:01:25
    1 |  11 |  Active |  auto | FRKW826f72f7 | 20202020202020202020 |   0:00:01:25
    1 |  12 |  Active |  auto | FRKW826f7268 | 20202020202020202020 |   0:00:01:25
    1 |  14 |  Active |  auto | FRKW80103312 | 20202020202020202020 |   0:00:01:24
    1 |  15 |  Active |  auto | FRKW826f730d | 20202020202020202020 |   0:00:01:24
    1 |  16 |  Active |  auto | FRKW4b0067d3 | 00000000000000000000 |   0:00:01:24
```

11.2.1.3 Manual ONU (ONT) Registration Mode

To register/delete ONU (ONT) manually, use the following command.

Command	Mode	Description
onu add *ONU-ID SERIAL_NUM* {**auto-learning** | *PASSWD* [**enable** | **disable**]}	GPON-OLT	Registers ONU (ONT) with specified ONU-ID, serial number and password. Enables/disables the password auto-learning mode of the ONU (ONT) ONU-ID:ONU ID (1 to 128) or ONU serial number SERIAL_NUM: ONU's serial number PASSWD: ONU password
no onu *ONU-ID*		Deletes the registered ONU with ONU ID.

11.2.1.4 ONU Registration Mode

The default ONU registration mode is the auto mode in which an OLT registers ONUs automatically, when recognizing the optical signal from the ONUs. For an optimized ONU configuration, however, the manual mode is recommended. Some options are only available in the manual mode.

Upon registering an ONU automatically, the registration mode of the ONU will be changed to the manual mode. Note that when you use this command, the registration mode of the ONUs that are already registered in the auto mode will be changed to the manual mode as well.

To change the ONU registration mode from auto to manual mode, use the following command.

Command	Mode	Description
olt auto-to-manual *OLT-ID* **enable**	GPON	Sets the current ONU registration mode to the manual mode. OLT-ID: GPON port number
olt auto-to-manual enable	GPON-OLT	

To change the ONU registration mode from manual to auto mode, use the following command.

Command	Mode	Description
olt auto-to-manual *OLT-ID* **disable**	GPON	Sets the current ONU registration mode to the auto mode.
olt auto-to-manual disable	GPON-OLT	

To display the ONU registration mode, use the following command.

Command	Mode	Description
show olt auto-to-manual [*OLT-ID*]	Enable Global GPON	Shows the current ONU registration mode.
show olt auto-to-manual	GPON-OLT	

11.2.1.5 Changing ONU Registration Mode

If user wants to change automatically the states of ONU (ONT) to manage manually at a time, use the following command.

Command	Mode	Description
onu fix {**all** | *ONU-ID*}	GPON-OLT	Changes automatically registered ONUs (ONTs) to manage manually. ONU-ID: ONU ID (1 to 128) or ONU serial number

11.2.1.6 ONU Service Mode

Depending on the individual FTTH subscriber network deployment, the GPON link can be

terminated with different client-side equipment options like Single Family Unit (SFU) and Home Gateway Unit (HGU). To select the ONU network service mode, use the following command.

Command	Mode	Description
onu service-mode *ONU-ID* {**hgu** | **sfu**}	GPON-OLT	Specifies the network service mode of ONU. ONU-ID: ONU ID (1 to 128) or ONU serial number hgu: home gateway unit sfu: single family unit
no onu service-mode [*ONU-ID*]		Deletes the configure network service mode of ONU.

To display the configured ONU service mode, use the following command.

Command	Mode	Description
show onu service-mode [*OLT-ID*]	Enable Global GPON	Shows the configured ONU service mode. OLT-ID: OLT ID (PON port number) ONU-ID: ONU ID (1 to 128) or ONU serial number
show onu service-mode [*ONU-ID*]	GPON-OLT	

11.2.1.7 ONU Description

To specify or modify a description of an ONU, use the following command.

Command	Mode	Description
onu description *ONU-ID DESCRIPTION*	GPON-OLT	Registers the ONU's description. ONU ID (1 to 128) or ONU serial number
no onu description *ONU-ID*		Deletes the description of ONU.

To display a description of an ONU, use the following command.

Command	Mode	Description
show onu description *OLT-ID*	Enable Global GPON	Shows the ONU's description.
show onu description [*ONU-ID*]	GPON-OLT	

11.2.1.8 ONU Connectivity via Ping Test

To verify the network connectivity with the ONU, use the following command.

Command	Mode	Description
omci ping *ONU-ID*	GPON-OLT	Shows the network connectivity between OLT ID and ONU ID. ONU ID (1 to 128) or ONU serial number

11.2.1.9 OMCI Window-size

To configure the network connectivity with the ONU, use the following command.

Command	Mode	Description
omci window-size <1-255>	GPON-OLT	Configures the omic window size. 1-255: Allowed value for omic window size.
no omci window-size		Deletes configured window-size.

11.2.1.10 OMCI Config-status

To display OMCI config-status, use the following command.

Command	Mode	Description
show omci-config [*OLT_ID*]	Enable Global GPON	Shows the OMCI configurations.
show omci-config	GPON-OLT	

11.2.2 Assigning IP address

To configure the IP host service ID, IP address and gateway address for an ONU, use the following command.

Command	Mode	Description
onu static-ip *ONU-ID* **ip-host** *SERVICE-ID A.B.C.D/M* **gw** *A.B.C.D*	GPON-OLT	Configures the IP host service ID, IP address and gateway address for an ONU. ONU-ID: ONU ID (1 to 128) or ONU serial number SERVICE-ID: IP host service ID A.B.C.D/M: IP address A.B.C.D: IP gateway address
no onu static-ip *ONU-ID* **ip-host** *SERVICE-ID*		Deletes the configured IP host service ID, IP address and gateway address for the ONU.

To assign a static IPv6 address for IPv6 host of ONU, use the following command.

Command	Mode	Description
onu static-ip *ONU-ID* **ipv6-host** *SERVICE-ID X:X::X:X/M* **default-router** *X:X::X:X*	GPON-OLT	Configures the IPv6 host service ID, IPv6 address and IPv6 gateway address for an ONU. ONU-ID: ONU ID (1 to 128) or ONU serial number SERVICE-ID: IPv6 host service ID X:X::X:X/M: IPv6 address X:X::X:X: IPv6 address of default router
no onu static-ip *ONU-ID* **ipv6-host** *SERVICE-ID*		Deletes the configured static IPv6 address of IPv6 host.

i For the details of how to create and configure the IP host service, see 11.4.5 IP Host

Service Configuration. The IP assignment on IP host service configuration has to be specified as "**static**" when assigning IP address to ONU.

To display the configured IP host service ID on ONU, use the following command.

Command	Mode	Description
show onu ip-host *OLT-ID ONU-ID*	Enable Global GPON	Shows the configured IP host service ID on ONU.
show onu ip-host *ONU-ID*	GPON-OLT	

11.2.3 Activating Administration for UNI

To enable/disable the administration of the ONU (ONT) UNI port, use the following command.

Command	Mode	Description
onu port-admin *ONU-IDs* **uni** {**eth** | **pots** | **ces** | **virtual-eth** | **video** | **wifi**} *UNI-PORTs* {**enable** | **disable**}	GPON-OLT	Enables/disables the administration of UNI port on the specified ONU. ONU-ID: ONU ID (1 to 128) or ONU serial number eth/pots/ces/virtual-eth/Video: Ethernet / POTS / CES / virtual Ethernet/Video/Wi-Fi UNI-PORT: UNI port number

i To see the admin status of the ONU (ONT) UNI, use **show onu uni-status** command. (See 11.2.25 Displaying ONU Information)

11.2.4 Forward Error Correction (FEC) Mode

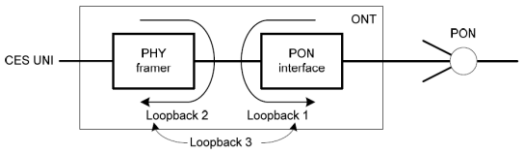
To enable/disable FEC mode for ONU ID, use the following command.

Command	Mode	Description
onu us-fec-mode *ONU-IDs* **enable**	GPON-OLT	Enables upstream FEC mode for ONU ID.
onu us-fec-mode *ONU-IDs* **disable**		Disables upstream FEC mode for ONU ID.

i If you want to enable the upstream FEC mode for ONU, you should enable upstream FEC mode for OLT first. For the detail of how to enable the upstream FEC mode for OLT, see 11.1.6 Forward Error Correction (FEC) Mode.

11.2.5 Loopback

To enable/disable the loopback for UNI of ONU, use the following command.

Command	Mode	Description
onu loopback *ONU-IDs* **uni eth** *UNI-PORTs* {**enable type 3** | **disable**}	GPON-OLT	Enables/disables the loopback for the specified Ethernet (type 3) UNI port of ONU. ONU-IDs: ONU ID (1 to 128) or ONU serial number UNI-PORTs: UNI port number
onu loopback *ONU-IDs* **uni ces** *UNI-PORTs* {**enable type** <1-5> | **disable**}		Enables/disables the loopback for the specified CES/TDM UNI port of ONU. ONU-IDs: ONU ID (1 to 128) or ONU serial number UNI-PORTs: UNI port number 1: payload loopback 2: line loopback 3: OpS-directed loopback 1 (loopback from/to PON side) 4: OpS-directed loopback 2 (loopback from/to CES UNI side) 5: OpS-directed loopback 3 (loopback of both PON side and CES UNI side) 

i To see the status of the ONU (ONT) UNI, use **show onu uni-status** command. (See 11.2.25 Displaying ONU Information)

11.2.6 ONU Laser Down

If a certain ONU's laser is enabled consistently by an optical transceiver's fault, all other normal ONUs connected to the same OLT will be deregistered; a single ONU fault may cause a whole network disruption.

To prevent such a problem, you can manually disable the laser (TX power of transceiver) of the faulty ONU considered as the cause of the problem. By the way, if you disable the laser without specifying laser-off time, the ONU needs a power reset to resume the laser.

To disable an ONU's laser, use the following command.

Command	Mode	Description
onu tx-off-optic *ONU-ID* [<1-65525>]	GPON-OLT	Disables an ONU's laser for specified time. After the time, the laser will be enabled. ONU-ID: 1-128 or ONU serial number 1-65525: disable transceiver during input times (unit:sec)

⚠ To guarantee a right operation of this feature, an ONU should be loaded with the newest firmware.

11.2.7 Source MAC address Monitoring

The OLT can monitor its source MAC table to find a defective ONUs (ONTs). Auto ONU (ONT) blocking function can be used to manage and troubleshoot the defective ONU-related problems.

To enable/disable OLT for source MAC address monitoring, use the following command.

Command	Mode	Description
olt srcmac-monitor enable	GPON-OLT	Enables the source MAC address monitoring.
olt srcmac-monitor enable auto-onu-block [**expire-timeout** <60-65535>]		Enables the source MAC address monitoring with auto ONU blocking feature auto-onu-block: When an ONU fault occurs, the system will disable the ONU's laser permanently. 60-65535: expire time (second)
olt srcmac-monitor disable		Disables the source MAC address monitoring.

To force the state of a blocked ONU ID to change to unblocked state, use the following command.

Command	Mode	Description
onu unblock *ONU-ID*	GPON-OLT	Forces the state of a blocked ONU ID to change to unblocked state.

To force the state of a unblocked ONU ID to change to blocked state, use the following command.

Command	Mode	Description
onu block *ONU-ID*	GPON-OLT	Forces the state of a unblocked ONU ID to change to blocked state.

To display the information of source MAC monitoring, use the following command.

Command	Mode	Description
show olt srcmac-monitor [*OLT-ID*]	Enable Global GPON	Shows the configured source MAC address monitoring for OLT.
show olt srcmac-monitor	GPON-OLT	

11.2.8 ONU MAC address Filtering

The MAC filter table lists MAC destination addresses associated with the bridge port, each with an allow/disallow forwarding indicator for traffic flowing out of the bridge port. In this way, the upstream traffic is filtered on the ANI-side bridge ports, and the downstream traffic is filtered on the UNI-side bridge ports.

To enable/disable the MAC filtering function for UNI-side bridge port, use the following command.

Command	Mode	Description
onu mac-filter *ONU-ID* **uni** { **eth** | **ip-host** | **ces** | **virtual-eth** } *PORT* { **filter** | **forward** } *MACADDR*	GPON-OLT	Enables the MAC filtering function for UNI-side bridge port. eth: Ethernet port ip-host: IP host service virtual-eth: virtual Ethernet ces: circuit emulation service PORT: port number forward: forwards a specific MAC address of UNI-side port filter: blocks a specific MAC address of UNI-side port MACADDR: MAC address
no onu mac-filter *ONU-ID* **uni** { **eth** | **ip-host** | **ces** | **virtual-eth** } *PORT* { **filter** | **forward** } *MACADDR*		Disables the MAC filtering function for UNI-side bridge port.

To enable/disable the MAC filtering function for ANI-side bridge port, use the following command.

Command	Mode	Description
onu mac-filter *ONU-ID* **ani** { **mapper** | **gem** } *PORT* { **filter** | **forward** } *MACADDR*	GPON-OLT	Enables the MAC filtering function per ANI-side mapper ID or GEM port ID.
no onu mac-filter *ONU-ID* **ani** { **mapper** | **gem** } *PORT* [{ **filter** | **forward** } *MACADDR*]		Disables the MAC filtering function per ANI-side mapper ID or GEM port ID.

To display the information of MAC filtering and MAC table data, use the following command.

Command	Mode	Description
show onu mac-filter *OLT-ID*	Enable/Global/GPON	Shows the MAC filtering function.
show onu mac-filter [*ONU-ID*]	GPON-OLT	
show onu mac *OLT-ID ONU-ID* **uni {eth | virtual-eth}** *UNI-PORT*	Enable/Global/GPON	Shows the MAC table data of ONU's UNI ports.
show onu mac *ONU-ID* **uni eth**	GPON-OLT	

UNI-PORT		

11.2.9 POTS Interface Configuration

To configure the parameters of POTS interface in an ONT, use the following command.

Command	Mode	Description
onu voip-sip *ONU-ID* **phone-number pots** *POTS-NUMBER NUMBER* [**display** *DISPLAY*]	GPON-OLT	Saves a phone number and a display information of a specified phone device connected to POTS interface at an ONU managed by OMCI protocol. ONU-ID: 1-128 or ONU serial number POTS-NUMBER: POTS port number NUMBER: phone number DISPLAY: display information
no onu voip-sip *ONU-ID* **phone-number pots** *POTS-NUMBER*		Deletes the configured data parameters of VoIP user.

For the enhanced system security, the OLT can use authentication for a VoIP user to have access to the softswitch.

To configure the authentication user name and password for VoIP user to have access to softswitch, use the following command.

Command	Mode	Description
onu voip-sip *ONU-ID* **auth pots** *POTS-NUM NAME* [*PASSWD*]	GPON-OLT	Configures an user ID and password for a specified VoIP device connected to an ONU to have access to softswitch. ONU-ID: 1-128 or ONU serial number POTS-NUM: POTS port number NAME: user name used for authentication PASSWD: password used for authentication
no onu voip-sip *ONU-ID* **auth pots** *POTS-NUM*		Deletes the configured authentication information for VoIP user.

i The user display name, phone number, authentication user name and password is limited to a maximum of 25 characters (bytes).

To display VoIP service and VoIP line status information, use the following command.

Command	Mode	Description
show onu voip line *OLT-ID ONU-ID*	Enable Global GPON	Shows the information of VoIP service and line status. ONU-ID: 1-128 or ONU serial number
show onu voip line *ONU-ID*	GPON-OLT	

11.2.10 VoIP MGC Configuration

11.2.10.1 Message ID Configuration

To configure the message ID according to the specific VoIP service, use the following command.

Command	Mode	Description
onu voip-mgc *ONU-ID* **message-id service** *VOIP_SERVICE MESSAGE_ID*	GPON-OLT	Configures the message ID according to the specific VoIP service. ONU-ID: ONU ID or serial number VOIP_SERVICE: VoIP service number MESSAGE_ID: message ID
no onu voip-mgc *ONU-ID* **message-id service** *VOIP_SERVICE*		Deletes the configured message ID.

i For the details of how to create and configure the VoIP service, see 11.4.6 VoIP Service Configuration (POTS UNI).

11.2.10.2 ONT Termination ID Configuration

The attribute specifies the base string for the MGC (H.248) physical termination ID(s) for the ONT. This string is intended to uniquely identify an ONT. Vendor-specific termination identifiers (i.e. port IDs) are optionally added to this string to uniquely identify a termination on a specific ONT.

To configure the termination ID on POTS interface of ONT, use the following command.

Command	Mode	Description
onu voip-mgc *ONU-ID* **termination-id pots** *POTS_NUM TERMINATION_ID*	GPON-OLT	Specifies the termination ID on POTS interface of ONT. ONU-ID: ONU ID or serial number POTS_NUM: POTS number TERMINATION_ID: termination ID
no onu voip-mgc *ONU-ID* **termination-id pots** *POTS_NUM*		Deletes the configured termination ID.

11.2.11 ONU Port Configuration

11.2.11.1 UNI Ethernet Port Configuration

To configure the UNI Ethernet port of ONU, use the following command.

Command	Mode	Description
onu port-config *ONU-IDs* **uni eth** *UNI-PORTs* **medium-mode** {**mdi** | **mdi-x** | **auto**}	GPON-OLT	Configures the medium mode of ONU UNI Ethernet port. ONU-ID: 1-128 or ONU serial number UNI-PORT: ONU UNI port number mdi: MDI mode mdi-x: MDIX mode auto: automatically
onu port-config *ONU-IDs* **uni eth** *UNI-PORTs* **speed** {**auto** | **1000** | **100** | **10**} **duplex** {**auto** | **full** | **half**}		Configures the speed and duplex mode of ONU UNI Ethernet port.
onu port-config *ONU-IDs* **uni eth** *UNI-PORTs* **power-control** {**enable** | **disable**}		Enables/disables the Power over Ethernet (PoE) port on the specified ONU.
onu uni-description *ONU-ID* **eth** *UNI-PORT DESCRIPTION*		Adds the description on the specified ONU UNI Ethernet port.
no onu uni-description *ONU-ID* **eth** *UNI-PORT*		Deletes the description of the specified ONU UNI Ethernet port.

To display the status of ONU UNI Ethernet port, use the following command.

Command	Mode	Description
show onu uni-status eth *OLT-ID*	Enable/Global/GPON	Shows the status of ONU UNI Ethernet port.
show onu uni-status eth [*ONU-IDs*]	GPON-OLT	

To display the configured description on ONU UNI port, use the following command.

Command	Mode	Description
show onu uni-description *OLT-ID*	Enable Global GPON	Shows the configured description on ONU UNI port.
show onu uni-description [*ONU-ID*]	GPON-OLT	

11.2.11.2 ANI RF Video Port Configuration

To configure the ANI RF video port of ONU, use the following command.

Command	Mode	Description
onu port-config *ONU-IDs* **ani video** *ANI-PORTs* **agc** *AGC_VALUE*	GPON-OLT	Configures the AGC value of ONU ANI RF video port. ONU-ID: 1-128 or ONU serial number ANI-PORT: ANI port number AGC_VALUE: Automatic Gain Control value (-12.7~12.7 dB)
no onu port-config *ONU-IDs* **ani video** *ANI-PORTs* **agc**		Deletes the AGC value of the specified ONU ANI video port.

To update the system or RF video status of ONU, use the following command.

Command	Mode	Description
onu video-status update {<1-1440> **| disable**}	GPON	Sets the ONU's RF video update 1-1440: update interval time (default: 4 minutes)
show onu video-status update	GPON	Shows the ONU's RF video update status.
show onu video status *OLT_ID ONU_IDs*	GPON-OLT	Shows the ONU's RF video status.

11.2.12 ONU Loop Detect Configuration

A loop may occur when double paths are used for the link redundancy between switches and one sends unknown unicast or multicast packet that causes endless packet floating on the LAN. That superfluous traffic eventually can result in network fault.

The ONU periodically sends the loop-detecting packet to all the ports with a certain interval, and then if the loop-detecting packet is received, the switch performs a pre-defined behavior such as "blocked". The user may need to change this state to "unblocked (normal)" via OLT.

To change the "blocked" state of ONU due to the loop detection into "unblocked", use the following command.

Command	Mode	Description
onu loop-detect unblock *ONU-IDs*	GPON-OLT	Changes the "blocked" state due to loop detect into "unblocked (normal)".

To display whether the specific ONU is in the state of "blocked" or "unblocked" due to the loop detect, use the following command.

Command	Mode	Description
show onu loop-detect [*OLT-ID*]	Enable Global GPON	Shows whether the ONU is in the state of "blocked" or "unblocked".

show onu loop-detect [*ONU-IDs*]	GPON-OLT	

11.2.13 ONU Inactive Aging-time

The ONU inactive aging-time can be used while the registration mode of the ONU is configured in the manual mode. If a number of days for an OLT to check the ONU's registration status pass without the ONU's activation, the ONU will be automatically deregistered.

To specify the registration aging time for the ONUs that are manually registered, use the following command.

Command	Mode	Description
onu inactive aging-time <1-30>	GPON-OLT	Specifies the maximum number of days that an ONU is inactive. If the ONU has been inactive during that number of days, the ONU will be automatically deregistered by OLT. 1-30: aging time measured in days
onu inactive aging-time disable		Sets the ONU aging time to be unlimited (default)

To display the configured aging time for the inactive ONUs, use the following command.

Command	Mode	Description
show onu inactive aging-time [*OLT-ID*]	Enable Global GPON	Shows the configured aging time for the inactive ONUs.
show onu inactive aging-time	GPON-OLT	

i

You can monitor how long the ONU has been inactive status displayed in the Inactive Time field using **show onu detail-info** command. If the ONU's activation status is active, the inactive time value remains unchanged at 0:00:00:00.

11.2.14 ONU Reset

For various reasons such as HW or SW error, you may need to reset an ONU (ONT). To reset an ONU, use the following command.

Command	Mode	Description
onu reset *ONU-IDs*	GPON-OLT	Reboots a specific ONU. ONU-ID: ONU ID (1 to128) or ONU serial number
onu restore-factory reset *ONU-IDs*		Restores the factory default settings of ONU. ONU-ID: ONU ID (1 to128) or ONU serial number
onu re-config *ONU-ID*		Resets the ONU for delete the ONU's MAC table.

11.2.15 ONU Password Type Configuration

To configure ONU password type, use the following command.

Command	Mode	Description
onu password-type {**hex** | **ascii**}	GPON	Configures ONU password type.

11.2.16 Diagnostic Monitoring for ONU's Optical Transceiver

The Digital Diagnostic Monitoring Interface (DDMI) feature provides diagnostic information about the module's present operating conditions. The transceiver generates this diagnostic data by digitization of internal analog signals.

To display the operating parameters of ONU's GPON module, use the following command.

Command	Mode	Description
show onu ani optic-module-info *OLT-ID ONU-ID* [**test-action**]	Enable Global GPON GPON-OLT	Shows the operating parameters of the GPON module, including the optical characteristics.
show onu ani optic-module-info *ONU_ID*	GPON-OLT	
show onu uni optic-module-info *OLT-ID ONU-ID PORT*	Enable Global GPON	Shows the operating parameters of the module of UNI port including the optical characteristics.
show onu uni optic-module-info *ONU-ID PORT*	GPON-OLT	

i To use the above command, ONU (ONT) should support DDMI feature and provide diagnostic information about the module's present operating conditions to OLT.

11.2.17 ONU System Account

To add system-account information for ONUs, use the following command.

Command	Mode	Description
onu system-account *ONU-ID USER* [*PASSWD*]	GPON-OLT	Creates the login account ID and password for ONU ID. ONU-ID: ONU ID (1 to128) or ONU serial number USER: user name PASSWD: password

To display the system-account information of ONU ID, use the following command.

Command	Mode	Description
show onu system-account *OLT-ID ONU-ID*	Enable/Global/GPON	Shows the system-account information of ONU.
show onu system-account *ONU-ID*	GPON-OLT	

11.2.18 ONU CoS Remarking

To configure CoS remarking feature based on the specific MAC/IP for ONU, use the following command.

Command	Mode	Description
onu cos-remarking *ONU_ID* {**src-mac** | **dst-mac**} *XX:XX:XX:XX:XX:XX* {**netmask** <1-48> | **cos** <0-7>}	GPON-OLT	Configures CoS remarking for ONU ID. ONU-ID: ONU ID (1 to 128) or ONU serial number dst-ip: Destination IP dst-mac: Destination MAC src-ip: Source IP src-mac: Source MAC
onu cos-remarking *ONU_ID* {**src-ip** | **dst-ip**} *A.B.C.D* {**netmask** <1-32> | **cos** <0-7>}		
no onu cos-remarking *ONU_ID*		Deletes the configured CoS remarking.
no onu cos-remarking *ONU_ID* {**src-mac** | **dst-mac**} *XX:XX:XX:XX:XX:XX* {**netmask** <1-48> | **cos** <0-7>}		
no onu cos-remarking *ONU_ID* {**src-ip** | **dst-ip**} *A.B.C.D* {**netmask** <1-32> | **cos** <0-7>}		

To display the configured CoS remarking information of ONU ID, use the following command.

Command	Mode	Description
show onu cos-remarking *ONU_ID*	GPON-OLT	Shows the CoS remarking information of ONU.
show onu cos-remarking *OLT_ID*	Enable Global GPON	Shows the CoS remarking of ONU configured on an OLT.

11.2.19 ONU Extended VLAN Tagging Operation

To associate the extended VLAN tagging operation profile to the specified ONU ID and configure the inner tag treatment, use the following command.

Command	Mode	Description
onu extended-vlan *ONU-ID NAME* **double-tagged-frame** *TABLE* **treat inner vid** {<0-4094> | **copy-inner** | **copy-outer**} **cos** {<0-7> | **copy-inner** | **copy-outer** | **dscp-to-pbit**}	GPON-OLT	Associates the extended VLAN tagging operation profile to ONU ID and configures the inner tag treatment for filtered double-tagged frames. ONU-ID: ONU ID (1 to128) or ONU serial number NAME: Extended VLAN tagging operation profile name TABLE: rule table name (1 to 32) 0-4094: uses this value as the VID in the inner VLAN tag. copy-inner: copies value from inner tag of received frame. copy-outer: copies value from outer tag of received frame. 0-7: uses this value as the priority in the inner VLAN tag.
onu extended-vlan *ONU-ID NAME* **single-tagged-frame** *TABLE* **treat inner vid** {<0-4094> | **copy-inner** } **cos** {<0-7> | **copy-inner** | **dscp-to-pbit**}		Associates the extended VLAN tagging operation profile to ONU ID and configures the inner tag treatment for filtered single-tagged frames.
onu extended-vlan *ONU-ID NAME* **untagged-frame** *TABLE* **treat inner vid** <0-4094> **cos** {<0-7> | **dscp-to-pbit**}		Associates the extended VLAN tagging operation profile to ONU ID and configures the inner tag treatment for filtered untagged frames.
no onu extended-vlan *ONU-ID NAME* { **double-tagged-frame** | **single-tagged-frame** | **untagged-tagged-frame** }		Removed the extended VLAN tagging operation profile association from ONU ID and the configured inner tag treatment.

i For the details of how to create and configure the extended VLAN tagging operation profile, see 11.6 Extended VLAN Tagging Operation Profile.

11.2.20 ONU RateLimit Configuration

To enable Network Address Translation (NAT) mode of ONU, use the following command.

Command	Mode	Description
onu nat-mode *ONU_IDs* {**enable** | **disblae**}	GPON-OLT	Enables NAT mode of ONU. ONU_ID: ONU ID or ONU serial number.
no onu nat-mode [*ONU_IDs*]		Configures the Not use the NAT mode function.

To configure the upstream/downstream traffic for GEM port of ONU, use the following command.

Command	Mode	Description
onu rate-limit *ONU_ID* **mapper** *MAPPER_ID* **gemport**	GPON-OLT	Sets the down/upstream traffic for GEM port of ONU. ONU_ID: ONU ID or ONU Serial Number

GEMPORT_RANGE {**upstream** | **downstream**} *PIR_VALUE*		MAPPER_ID: 802.1p mapper ID (1-32) GEMPORT_RANGE: gem port PIR_VALUE: PIR (Bandwidth in steps of 64Kbps)

To configure the rate limit profile for GEM port of ONU, use the following command.

Command	Mode	Description
onu rate-limit *ONU_ID* **mapper** *MAPPER_ID* **gemport** *GEMPORT_RANGE* **profile** *PROF_NAME*	GPON-OLT	Sets the rate limit profile for GEM port of ONU. PROF_NAME: profile name

To display the information of NAT mode and rate-limit, use the following command.

Command	Mode	Description
show onu nat-mode [*OLT_ID*]	Enable Global GPON	Shows the NAT mode status.
show onu nat-mode [*ONU_IDs*]	GPON-OLT	
show onu rate-limit	Enable Global GPON	Shows the information of rate-limit configured for ONU
show onu rate-limit [*ONU_ID*]	GPON-OLT	

The following is an example of NAT mode synchronized with GPON OLT.

```
LD3016(config-gpon-olt[8])# show running-config gpon-olt 8
gpon-olt 8
discover-serial-number start 5
onu add 1 FRKW6308f340 auto-learning
onu nat-mode 1 enable
onu-profile 1 LD322_HSI
!
LD3016# show onu nat-mode 8
-------------------------------
OLT | ONU | NAT Mode
-------------------------------
8 | 1 | Enable
LD3016(config-gpon-olt[8])# onu nat-mode 1 disable
LD3016(config-gpon-olt[8])# show onu nat-mode
-----------------------------------------------------------------------
OLT | ONU | STATUS | Serial No. | NAT Mode | NAT Oper
-----------------------------------------------------------------------
8 | 1 | Inactive | FRKW6308f340 | Disable | Not Support
LD3016(config-gpon-olt[8])#
LD3016(config-gpon-olt[8])# no onu nat-mode 1
LD3016(config-gpon-olt[8])# show onu nat-mode
-----------------------------------------------------------------------
```

```
OLT | ONU | STATUS | Serial No. | NAT Mode | NAT Oper
-----------------------------------------------------------------------
8 | 1 | Inactive | FRKW6308f340 | None | Not Support
```

The following is an example of rate-limit configuration and snmp get.

```
LD3016(config-gpon-olt[8])# onu rate-limit 1 mapper 1 gemport 1 upstream 64
LD3016(config-gpon-olt[8])# onu rate-limit 1 mapper 1 gemport 2 upstream 64
LD3016(config-gpon-olt[8])# onu rate-limit 1 mapper 1 gemport 2 down 256 128
LD3016(config-gpon-olt[8])# show running-config gpon-olt 8
gpon-olt 8
discover-serial-number start 5
onu add 1 FRKW6308f340 auto-learning
onu nat-mode 1 enable
onu-profile 1 LD322_HSI
onu rate-limit 1 mapper 1 gemport 1-2 upstream 64
onu rate-limit 1 mapper 1 gemport 2 downstream 256 128
!
LD3016(config-gpon-olt[8])#

LD3016# show onu rate-limit 8 1
-----------------------------------------------------------------------
OLT | ONU | MAPPER | GEM | DIRECTION | SIR | PIR
-----------------------------------------------------------------------
8 | 1 | 1 | 1 | Up | 0 | 64
8 | 1 | 1 | 2 | Up | 0 | 64
8 | 1 | 1 | 2 | Down | 128 | 256
```

11.2.21 ONU Authentication from RADIUS Server

You can use the RADIUS authentication process when an ONU (ONT) is activated and it attempts to access an OLT. The RADIUS Access-Request message is sent from the OLT to the RADIUS server. If the ONU is valid, the RADIUS server consults a database of ONUs to find the ONU which matches the authentication attributes in the connection request. If the RADIUS server has the valid ONU-related information, it sends the configuration settings placed into a RADIUS Access-Accept message to the OLT for the ONU registration. The OLT receives the service profile settings from the RADIUS server and it assigns a new service profile to ONU.

RADIUS Authentication Process

① **Upload MIB Info**: During the initial connection between OLT and ONU, the ONU uploads the MIB information. On the OLT side, the OLT checks the ONU validation using ONU model name, firmware version and serial number.

② **Sends RADIUS message**: If the RADIUS authentication is required when the OLT and ONU are connected each other, the OLT sends Access-Request message with the authentication attributes (user name, user password, OLT-ID, ONU-ID, ONT model name, serial number, firmware version) to the RADIUS server.

③ **Receive Response message**: If the RADIUS message is sent by a valid ONU, and if the authentication attributes contain the correct values, the Access-Accept message of ONU configuration settings is sent by the RADIUS server.

④ **Set the configuration**: The OLT receives the service profile information from the RADIUS server. The new service profile settings are assigned to ONU.

The RADIUS server sends Disconnect messages (DM) request in order to terminate a user session on a network access server, whereas it sends Change-of-Authorization (CoA) request messages to modify session authorization attributes of ONU.

The OLT checks that the key of DM message from the RADIUS server is valid. If the key value is invalid, the packets are silently discarded.

Tab. 11.1 shows the RADIUS message format and types.

Message Type	Authentication Attributes (RADIUS Code Field)
Access-Request (OLT → server)	(a) Service-Type: “Authenticate Only (8)”. (b) User-Name & User-Password: ONU Model Name

	(c) Vendor-Specific Vendor ID: IANA registered Furukawa (10428) (d) Vendor-Specific Attribute: OLT_ID, ONT_ID, Model Name, Serial Number, Firmware Version info. (e) Message-Authenticator: KEY and MD5
Access-Accept (server → OLT)	(a) Furukawa-Gpon-Onu-Profile (b) Furukawa-Gpon-Onu-Static-Ip (c) Furukawa-Gpon-Onu-Voip-Sip-Number (d) Furukawa-Gpon-Onu-Voip-Sip-Auth (e) Furukawa-Gpon-Onu-Uni-Port-Admin (f) Furukawa-Gpon-Onu-VoIP-Mgc-Msg-Id (g) Furukawa-Gpon-Onu-VoIP-Mgc-Term-Id (h) Furukawa-Gpon-Onu-Description (i) Furukawa-Gpon-Onu-Uni-Eth-Port-Medium (j) Furukawa-Gpon-Onu-Uni-Eth-Auto-Detect (k) Furukawa-Gpon-Onu-Mac-Filter (l) Furukawa-Gpon-Onu-Mgmt-Mode-Ip-Path-Ftp (m) Furukawa-Gpon-Onu-Mgmt-Mode-Ip-Path-Tftp (n) Furukawa-Gpon-Onu-Mgmt-Mode-Ip-Path-Uri
CoA-Request (server → OLT)	(a) User-Name (b) User-Password (c) Furukawa-Gpon-Olt-Id (d) Furukawa-Gpon-Onu-Id (e) Furukawa-Gpon-Onu-Model-Name (f) Furukawa-Gpon-Onu-Serial-Num (g) Furukawa-Gpon-Onu-Firmware-Version (h) Furukawa-Gpon-Onu-Profile (i) Furukawa-Gpon-Onu-Static-Ip (j) Furukawa-Gpon-Onu-Voip-Sip-Number (k) Furukawa-Gpon-Onu-Voip-Sip-Auth (l) Furukawa-Gpon-Onu-Uni-Port-Admin (m) Furukawa-Gpon-Onu-VoIP-Mgc-Msg-Id (n) Furukawa-Gpon-Onu-VoIP-Mgc-Term-Id (o) Furukawa-Gpon-Onu-Description (p) Furukawa-Gpon-Onu-Uni-Eth-Port-Medium (Not support yet) (q) Furukawa-Gpon-Onu-Uni-Eth-Auto-Detect (Not support yet) (r) Furukawa-Gpon-Onu-Mac-Filter
DM-Request (server → OLT)	(a) User-Name (b) User-Password (c) Furukawa-Gpon-Olt-Id (d) Furukawa-Gpon-Onu-Id (e) Furukawa-Gpon-Onu-Model-Name (f) Furukawa-Gpon-Onu-Serial-Num (g) Furukawa-Gpon-Onu-Firmware-Version

Tab. 11.1 RADIUS Authentication Message Type

To configure IP address and key value of RADIUS server for ONU authentication, use the following command.

Command	Mode	Description

onu auth radius-server host *A.B.C.D* **key** *WORD* [**auth-port** <0-65535>]	GPON	Specifies an IP address with key value and UDP port of RADIUS server. A.B.C.D: RADIUS server IP address WORD: RADIUS authorization key value 0-65535: UDP port (default: 1812)
onu auth radius-username { **serial-number** | **model-name**}		Sends the ONU's serial number-based or its model name-based ID key value on the authentication message to RADIUS server. serial-number: uses GPON serial number of ONU (default) model-name: uses model name of ONU
onu auth radius-password { **serial-number** | **model-name**}		Sends the ONU's serial number-based or its model name-based password on the authentication message to RADIUS server.
no onu auth radius-server host *A.B.C.D*		Deletes the configured RADIUS server address.

To display the information of RADIUS server for ONU authentication, use the following command.

Command	Mode	Description
show onu auth radius-server	GPON	Shows the information of RADIUS server for ONU authentication.

i You can see the status of ONU authentication via RADIUS server by the **debug gpon rauth** command.

To enable/disable the ONU authentication for ONU profile, use the following command.

Command	Mode	Description
onu auth-control {**enable** | **disable** }	GPON-OLT	Enables/disables the authentication control function for the specified OLT port.
onu auth-control reauthenticate		Performs re-authentication processing for ONU.

To display the information of ONU authentication status and profile, use the following command.

Command	Mode	Description
show onu auth-status [*OLT-ID*]	GPON	Shows the current authentication status of ONU.
show onu auth-status [*ONU-ID*]	GPON-OLT	

11.2.22 CFM OAM for ONU Management

CFM OAM is now standardized as IEEE 802.1ag. CFM contains the concepts of maintenance domains and supports autonomy for customers, providers, operators, etc. It enables end-to-end management of connectivity and services, each domain can run its own OAM. By CFM OAM feature, the service providers who own the network end-to-end may be able to guarantee services over networks they own.

CFM OAM Elements

You need to know conceptual information of CFM OAM. CFM OAM consists of the following management elements.

- **Maintenance Entity (ME)**
  An OAM entity that requires management. An MD is owned by a ME. It is a relationship between two Maintenance association end points (MEPs) within a single MA.
- **Maintenance Domain (MD)**
  In Ethernet CFM, an MD is a management space for monitoring and administering of a network. A network controlled by an operator that supports connectivity between MEPs.
- **Maintenance Association (MA)**
  A set of MEPs that belong to the same MA identifier and MD level within one service instance to verify the integrity of the service.
- **Maintenance Association End Point (MEP)**
  A provisioned reference point that can initiate/terminate proactive OAM frames. Each MEP has a unique MEP ID within its MA.
- **Maintenance Association Intermediate Point (MIP)**
  A provisioned reference point that can respond to diagnostic OAM frames initiated by a MEP.
- **Service Instance**
  CFM OAM defines that a service instance is one entity within MD.

CFM Messages

There are different types of CFM messages:

- **Continuity Check Message (CCM)**
  Each MEP sends periodic CCMs to other MEPs with a multicast destination address. The loss of CCMs that ride along the data path would indicate a connectivity failure.
- **Loopback Message/Response (LBM/LBR)**
  A LBM is sent to a unicast destination MAC address. MEP at the destination MAC address responds to the LBM with an LBR. These messages are useful for verifying connectivity with a specific L2 destination.
- **LinkTrace Message/Response (LTM/LTR)**
  A LTM is sent to a multicast MAC address. Each MIP at the same MD level responds with a LTR. LTM is then forwarded to the next hop until it reaches the destination MAC address. These messages are used for tracing the L2 path to a specific L2 destination.

CFM OAM Features

The important features provided by 802.1ag CFM OAM are:

- Supports Connectivity Check Message (CCM), LinkTrace (LTM) and LoopBack messages (LBM)
- Helps service providers assign selected subscribers restricted access to manage all functions for their own domains
- Fault detection, notification and verification
- Traces the path to another MEP or MIP in the same domain

A CFM maintenance domain (MD) is a management space on a network that is owned and operated by a single entity and defined by a set of ports internal to it, but at its boundary. To use CFM OAM, you should create MD. MD is defined by a given MD name and level that are configured by user. MD level determines the MEPs/MIPs that are interested in the contents of the CFM frame and through which the CFM frame is allowed to pass.

To create a CFM Maintenance Domain (MD) and configure its name and level, use the following command.

Command	Mode	Description
onu cfm md *DOMAIN* **level** <0-7>	GPON	Creates a MD name and specifies a MD's level DOMAIN: Maintenance Domain's name 0-7: MD's level to use (default: 0)
no onu cfm md *DOMAIN*		Deletes the configured MD with a unique name.

i Each MD has an index, an unique name and MD level. Several MDs can have same level. But one single MD cannot have several levels.

MEPs periodically exchange Continuity Check OAM messages to detect loss of continuity or incorrect network connections. To create a Maintenance Association (MA) with its name as a service instance for a specific MD and specify the interval of Continuity Check Messages (CCMs) that are sent by MEPs in the specified MA, use the following command.

Command	Mode	Description
onu cfm ma <1-65535> *MA_NAME* **md** *DOMAIN* **ccm interval** { **100ms** | **1s** | **10s** | **1m** | **10m** | **disable** }	GPON	Specifies a MA for MD and the interval of sending continuity check messages (CCMs). 1-65535: MA index MA_NAME: name of MA DOMAIN: Maintenance Domain's name
no onu cfm ma <1-65535>		Deletes the configured MA.

i There is at least one MA within a signle MD.

To configure a MIP and its level on the VLAN ID, use the following command.

Command	Mode	Description
onu cfm *ONU_ID* **mip level** *LEVEL* **vlan** *VLANS*	GPON-OLT	Specifies a MIP and its level on the VLAN ID. ONU_ID: ONU ID (1 to128) or ONU serial number LEVEL: MIP's level (0 to 7) VLAN: VLAN list (maximum 12)
no onu cfm *ONU_ID* **mip** [**level** *LEVEL*]		Removes the configured MIP.

To specify the ONU ID and bridge's UNI Ethernet port or ANI mapper to which the MEP is attached, use the following command.

Command	Mode	Description
onu cfm *ONU_ID* **mep** { **uni eth** *PORT* | **ani mapper** *PORT* } **mep-id** *MEP_ID* **ccm** { **enable** | **disable** }	GPON-OLT	Enables/disables the continuity check messages (CCMs) exchange and specifies an ONU ID and MEP ID. ONU-ID: ONU ID (1 to128) or ONU serial number PORT: ONU's UNI Ethernet port number or ANI mapper port number MEP_ID: MEP ID (1 to 8191)
onu cfm *ONU_ID* **mep** { **uni eth** *PORT* | **ani mapper** *PORT* } **mep-id** *MEP_ID* **primary-vlan** *VLANS* **peer-mep-id** *ID* **ma** <1-65535>		Configures a MEP on the ONU ID and assigns a remote MEP ID and primary VLAN ID. MEP_ID: MEP ID (1 to 8191) VLANS: primary VLAN ID ID: remote MEP ID (1 to 8191) 1-65535: MA index
no onu cfm *ONU_ID* **mep** [{**uni eth** *PORT* | **ani mapper** *PORT*} [**mep-id** *MEP_ID*]]		Removes the configured MEP ID from ONU.

Ethernet Loopback function supports fault verification through Loopback Messages (LBM) and Loopback Reply (LBR). These messages are used during initial set-up or after a fault has been detected to verify that the fault has occurred between two end points. CFM OAM allows both unicast and multicast loopback. Ethernet Traceroute function is used to retrieve adjacency relationship between a MEP and a remote MEP or MIP. And it is also used for fault localization. The sends LinkTrace Message (LTM) frames to discover a path for a link trace.

To configure the source / destination MEP to send the LoopBack Message (LBM) or LinkTrace message (LTM), use the following command.

Command	Mode	Description
onu cfm test loopback *ONU_ID* **mep** { **uni eth** *PORT* | **ani mapper** *PORT* } **mep-id** *MEP_ID* {**rmep-id** <1-8191> | **rmac** *MACADDR*} [**count** *NUMBER*]	GPON-OLT	Performs the Loopback/Traceroute test for ONU and specifies MEP ID and remote MEP ID/ MAC address to send LBM/LTM from the ONU. ONU_ID: ONU ID (1 to128) or ONU serial number PORT: ONU's UNI Ethernet port number or ANI mapper port number
onu cfm test traceroute *ONU_ID* **mep** { **uni eth** *PORT* | **ani mapper**		

PORT } **mep-id** *MEP_ID* {**rmep-id** <1-8191> | **rmac** *MACADDR*} [**ttl** <1-64>]		MEP_ID: MEP ID 1-8191: destination MEP ID MACADDR: destination MAC address to send LBMs/LTMs NUMBER: the number of attempts for sending LBMs (default:1) 1-64: LBM/LTM's TTL value (default: 64)

To display the information of CFM OAM, use the following command.

Command	Mode	Description
show onu cfm mep *OLT_ID*	Enable Global GPON	Shows the information of MEP configured on an OLT.
show onu cfm mip *OLT_ID*		Shows the information of MIP configured on an OLT.
show onu cfm ma [<1-65535>]	GPON	Shows the information of MA.
show onu cfm md [*DOMAIN*]		Shows the configured MD and level.
show onu cfm mep *ONU_ID*	GPON-OLT	Shows the status of MEP configured on an ONU.
show onu cfm mep ccm-db *ONU_ID* {**uni eth** *PORT* | **ani mapper** *NUMBER*} **mep-id** *MEP_ID*		Shows the information of a MEP in the CCM database.
show onu cfm mip [*ONU_ID*]		Shows the status of MIP configured on an ONU.

11.2.23 ONU DBA Profile

To specify the bandwidth of ONU port by mapping between T-CONT ID and DBA profile, use the following command.

Command	Mode	Description
onu dba-profile *ONU_ID* **tcont** *TCONT-ID PROF_NAME*	GPON-OLT	Specifies the bandwidth of ONU by mapping between the DBA profile and T-CONT ID. Sets T-CONT's bandwidth by specifying the DBA profile ONU_ID:ONU ID or ONU serial number TCONT_ID: TCONT ID (1-32) PROF_NAME: DBA profile name
no onu dba-profile *ONU_ID* **tcont** *TCONT-ID*		Deletes the configured DBA profile.

11.2.24 ONU Firmware Upgrade

The provides the remote ONU (ONT) upgradeability. This feature allows the system administrators not to offer the local service for a single ONU (ONT) upgrade at the customer premise. To upgrade an ONU (ONT) successfully, you need to download a new ONU (ONT) firmware in the system.

11.2.24.1 Manual Upgrade (1)

(1) Downloading Firmware to OLT

To download ONU (ONT) firmware in the system, use the following command.

Command	Mode	Description
copy {**ftp** | **tftp**} **onu download** [**vrf** *VRFNAME*]	Enable	Downloads ONU firmware via FTP or TFTP.

The following is an example of downloading ONU (ONT) firmware in the system.

```
SWITCH# copy ftp onu download
 To exit : press Ctrl+D
--------------------------------------
IP address or name of remote host (FTP): xxx.xxx.xxx.xxx
Download File Name : XXXXXX.x
User Name : user
Password:
```

To remove the downloaded ONU (ONT) firmware in OLT, use the following command.

Command	Mode	Description
remove onu firmware *FILE-NAME*	Enable Global GPON	Removes the downloaded ONU (ONT) firmware in OLT.

To display the list of the downloaded ONU (ONT) firmware in OLT, use the following command.

Command	Mode	Description
show onu firmware-list	Enable Global GPON GPON-OLT	Shows the downloaded ONU (ONT) firmware list in OLT.

(2) Downloading Firmware to ONU (Upgrading)

To download the specified ONU (ONT) firmware in the ONU (ONT), use the following command.

Command	Mode	Description
onu firmware download *ONU-ID FILE_NAME* [**os1** | **os2**]	GPON-OLT	Downloads ONU (ONT) firmware in the ONU (ONT). ONU-ID: ONU ID (1-128) or ONU serial number FILE_NAME: ONU firmware name

i You can see the status of ONU firmware by the **show onu firmware version** command as follows:

To display the status of ONU firmware, use the following command.

Command	Mode	Description
show onu firmware version *OLT-ID* [*ONU-IDs*]	Enable Global GPON	Shows the status of ONU firmware. OLT-ID: GPON port number ONU-ID: ONU ID (1-128) or ONU serial number
show onu firmware version [*ONU-IDs*]	GPON-OLT	Shows the status of ONU firmware. ONU-ID: ONU ID (1-128) or ONU serial number

```
SWITCH(config-gpon-olt[1])# show onu firmware version
                            (D):Default-OS (R):Running-OS
-------------------------------------------------------------------------
OLT | ONU |   Upgrade Status   |       OS1       |      OS2
-------------------------------------------------------------------------
1 |   1 |                 -    |          #2.13m |    (D)(R) #2.13m
```

(3) Specifying Default OS of ONU

To specify the default OS of ONU (ONT), use the following command.

Command	Mode	Description
onu firmware commit *ONU-ID* [**os1** | **os2**]	GPON-OLT	Specifies the default OS of ONU (ONT).

(4) Restarting ONU

In order to use the new upgraded firmware, you should restart the ONU (ONT). At this time, the upgraded OS should be specified as a default OS by using **onu firmware commit** command.

⚠ Before restarting the ONU (ONT), you should check the service status of ONU, whether to save the other configuration, or else.

To display the status of ONU firmware, use the following command.

Command	Mode	Description
show onu firmware version *OLT-ID* [*ONU-IDs*]	Enable Global GPON	Shows the status of ONU firmware. OLT-ID: GPON port number ONU-ID: ONU ID (1-128) or ONU serial number
show onu firmware version [*ONU-IDs*]	GPON-OLT	Shows the status of ONU firmware. ONU-ID: ONU ID (1-128) or ONU serial number

- **Changing Active Firmware**

If an ONU supports the dual OS, you can change the active firmware using the following command. To change the active firmware, use the following command.

Command	Mode	Description
onu firmware active-change *ONU-ID*	GPON-OLT	Changes the active OS of ONU (with ONU reboot). ONU-ID: ONU ID (1 to 128) or ONU serial number

11.2.24.2 Manual Upgrade (2)

(1) Downloading Firmware to OLT

To download ONU (ONT) firmware in the system, use the following command.

Command	Mode	Description
copy {**ftp** | **tftp**} **onu download**	Enable	Downloads ONU firmware via FTP or TFTP.

The following is an example of downloading ONU (ONT) firmware in the system.

```
SWITCH# copy ftp onu download
 To exit : press Ctrl+D
--------------------------------------
IP address or name of remote host (FTP): xxx.xxx.xxx.xxx
Download File Name : XXXXXX.x
User Name : user
Password:
```

To remove the downloaded ONU (ONT) firmware in OLT, use the following command.

Command	Mode	Description
remove onu firmware *FILE-NAME*	Enable Global GPON	Removes the downloaded ONU (ONT) firmware in OLT.

To display the list of the downloaded ONU (ONT) firmware in OLT, use the following command.

Command	Mode	Description
show onu firmware-list	Enable Global GPON GPON-OLT	Shows the downloaded ONU (ONT) firmware list in OLT.

(2) Upgrading Firmware

To upgrade an ONU (ONT) with the downloaded ONU (ONT) firmware, use the following command.

Command	Mode	Description
onu upgrade *ONU-ID FILENAME* {**ftp** *A.B.C.D USER PASSWD* | **tftp** *A.B.C.D*}	GPON-OLT	Upgrades an ONU (ONT) with a specified firmware. ONU-ID: ONU ID (1-128) or ONU serial number FILENAME: firmware file name A.B.C.D: FTP/TFTP server IP address USER: FTP server user name PASSWD: FTP server password
onu upgrade bootloader *ONU-ID FILENAME*		Upgrades the bootloader image of ONU (ONT) ONU-ID: ONU ID (1-128) or ONU serial number FILENAME: bootloader image file name

i If you execute the **onu upgrade** command, the firmware stored in OLT is downloaded to the standby (not running) OS of the specified ONU (ONT), and the standby OS is specified as default one. For example, if OS1 is running, the firmware is downloaded to OS2, and the OS2 is specified as the default.

i It may take about 10 minutes to upgrade the firmware of ONU (ONT).

i When completing the firmware upgrade, the related Syslog message is reported.

(3) Restarting ONU

In order to use the new upgraded firmware, you should restart the ONU (ONT).

⚠ Before restarting the ONU (ONT), you should check the service status of ONU, whether to save the other configuration, or else.

To display the status of ONU firmware, use the following command.

Command	Mode	Description
show onu firmware version *OLT-ID* [*ONU-IDs*]	Enable Global GPON	Shows the status of ONU firmware. OLT-ID: GPON port number ONU-ID: ONU ID (1-128) or ONU serial number
show onu firmware version	GPON-OLT	Shows the status of ONU firmware.

[*ONU-IDs*]		
show onu bootloader version *OLT-ID* [*ONU-IDs*]	Enable Global GPON	Shows the ONU bootloader version information. OLT-ID: GPON port number ONU-ID: ONU ID (1-128) or ONU serial number
show onu bootloader version [*ONU-IDs*]	GPON-OLT	

- **Changing Active Firmware**

If an ONU supports the dual OS, you can change the active firmware using the following command. To change the active firmware, use the following command.

Command	Mode	Description
onu firmware active-change *ONU-ID*	GPON-OLT	Changes the active OS of ONU (with ONU reboot). ONU-ID: ONU ID (1 to 128) or ONU serial number

11.2.24.3 Auto Upgrade

For efficient system maintenance, the provides the auto upgrade functionality for ONU firmware in the operational environment. You can simply upgrade the ONU firmware without an effort for every single ONU.

(1) Downloading Firmware to OLT

To download ONU (ONT) firmware in the system, use the following command.

Command	Mode	Description
copy {**ftp** | **tftp**} **onu download**	Enable	Downloads ONU firmware via FTP or TFTP.

The following is an example of downloading ONU (ONT) firmware in the system.

```
SWITCH# copy ftp onu download
 To exit : press Ctrl+D
-------------------------------------
IP address or name of remote host (FTP): xxx.xxx.xxx.xxx
Download File Name : XXXXXX.x
User Name : user
Password:
```

To remove the downloaded ONU (ONT) firmware in OLT, use the following command.

Command	Mode	Description
remove onu firmware *FILE-NAME*	Enable Global GPON	Removes the downloaded ONU (ONT) firmware in OLT.

To display the list of the downloaded ONU (ONT) firmware in OLT, use the following command.

Command	Mode	Description
show onu firmware-list	Enable Global GPON GPON-OLT	Shows the downloaded ONU (ONT) firmware list in OLT.

(2) Auto Upgrade Configuration (on *GPON Configuration* mode)

To configure the auto upgrade for ONU, use the following command.

Command	Mode	Description
onu auto-upgrade firmware *NAME FW_NAME*	GPON	Configures to be auto-upgraded with the specified firmware for the ONU. NAME: ONU model name FW_NAME: ONU firmware name
onu auto-upgrade firmware *NAME FW_NAME* {**ftp** *A.B.C.D USER PASSWD* | **tftp** *A.B.C.D*}		Configures to be auto-upgraded with the specified firmware for the ONU through the TFTP/FTP server. NAME: ONU model name FW_NAME: ONU firmware name A.B.C.D: FTP/TFTP server IP address USER: FTP server user name PASSWD: FTP server password
no onu auto-upgrade firmware *NAME*		Deletes the auto-upgrade configured for the specified ONU. NAME: ONU model name

i The firmware downloaded by **copy** {**ftp** | **tftp**} **onu download** command is deleted when the OLT system restarts. If you want to perform auto-upgrade even when the firmware does not exist in the OLT, you should specify the TFTP/FTP server from which the firmware can be downloaded.

To display the information of TFTP/FTP server specified for auto-upgrade, use the following command.

Command	Mode	Description
show onu auto-upgrade firmware info	Enable Global GPON	Shows the information of TFTP/FTP server specified for auto-upgrade.

The following is an example of displaying the information of the specified TFTP/FTP server.

```
SWITCH(gpon)# show onu auto-upgrade firmware info
 ---------------------------------------------------------------------------------
          Firmware Name        | T/FTP |       IP       |    User    |  Password
```

```
--------------------------------------------------------------------------------
G_ONU_N_2.77-1123.01.G420R.x |  TFTP |      10.55.2.4 |       XXX |   XXXX
```

To specify the execution condition of ONU auto upgrade configuration above, you should specify a target version of ONU firmware with (or without) **exclude** option. Through the target version and the option, auto upgrade execution condition is determined.

To set the target version for ONU, use the following command.

Command	Mode	Description
onu auto-upgrade target-version *NAME VERSION* [**exclude**]	GPON	Sets the target version for ONU. NAME: ONU model name VERSION: target version
no onu auto-upgrade target-version *NAME*		Deletes the configured target version for ONU.

i

If **exclude** option is used, the auto-upgrade is performed only when the ONU's existing firmware version is *different from* the specified target version. Otherwise, if **exclude** option is not used, the auto-upgrade is performed only when the ONU's existing firmware version is *same as* the specified target version.

To display the target version configuration for ONU auto upgrade, use the following command.

Command	Mode	Description
show onu auto-upgrade target-version	Enable Global GPON	Shows the target version configuration for ONU auto upgrade.

(3) Specifying Time and Retry Count

- **Specifying Time for Auto Upgrade**

You should set the clock of switch to start auto upgrade of ONU (download to ONU) at specified time. To specify the time to start auto upgrade of ONU, use the following command.

Command	Mode	Description
onu auto-upgrade model-name *NAME* **start-time** <0-23> **end-time** <0-23>	GPON	Specifies the time to start auto upgrade of ONU. NAME: ONU model name 0-23: start/end time (unit: o'clock)
onu auto-upgrade model-name *NAME* **start-time disable**		Deletes the specified time.
no onu auto-upgrade model-name *NAME* **start-time**		

i To see the ONU model name, use **show onu model-name** command. (See 11.2.25 Displaying ONU Information)

- **Retry Count for Auto Upgrade**

The retry count argument specifies how many times to retry the auto upgrading of ONU if the first attempt fails. To specify the retry count of auto upgrade, use the following command.

Command	Mode	Description
onu auto-upgrade retry-count <3-10>	GPON	Specifies the retry count of auto upgrade. 3-10 : retry count (default: 3)
no onu auto-upgrade retry-count		Deletes the configured retry count.

(4) Configuration of ONU Restart

To use the upgraded ONU firmware, the ONU must restart.

You can configure the upgrade-completed ONU to restart at specified time. To specify the time that the upgrade-completed ONU restarts, use the following command.

Command	Mode	Description
onu auto-upgrade reboot-time [*NAME*] {<0-23> | **immediately**}	GPON	Specifies the time that the upgrade-completed ONU restarts. NAME: ONU model name 0-23: restart time (unit: o'clock)
onu auto-upgrade reboot-time [*NAME*] **disable**		Deletes the specified time.

(5) Enabling Auto Upgrade (on *GPON-OLT Configuration* mode)

To enable/disable ONU auto upgrade on the specific OLT port, use the following command.

Command	Mode	Description
onu auto-upgrade {**enable** | **disable**} [*ONU_ID*]	GPON-OLT	Enables/disables ONU auto upgrade configuration on the OLT port.

i In order to apply the auto upgrade for ONU, you should enable the configured auto upgrade on the specific OLT port by **onu auto-upgrade enable** command on *GPON-OLT Configuration* mode.

(6) Displaying Auto-upgrade Configuration

To display the ONU auto upgrade configuration, use the following command.

Command	Mode	Description
show onu auto-upgrade info	Enable Global GPON GPON-OLT	Shows a progress of ONU auto-upgrade.
show onu auto-upgrade model-list [*NAME*]		Shows a list of ONU model names configured to be auto-upgraded. NAME: ONU model name

The following is an example of displaying the progress of ONU auto-upgrade and a list of ONU model name configured to be auto-upgraded.

```
SWITCH(gpon)# show onu auto-upgrade info
 ---------------------------------------------------------------------------------
  Auto-upgrade Start Time  : 17 (End Time : 18)
  Auto-upgrade Reboot Time : 17
 ---------------------------------------------------------------------------------
  OLT |   Mode  |     Upgrade Status     | Version Match | Invalid Version Match
 ---------------------------------------------------------------------------------
  3   | enable |   Upgrade ONU Progress |      enable  |     enable
  4   | disable |   Upgrade ONU Progress |      enable  |     enable


SWITCH(config-gpon-olt[3])# show onu auto-upgrade info
 ---------------------------------------------------------------------------------
  Auto-upgrade Start Time  : 17 (End Time : 18)
  Auto-upgrade Reboot Time : 17
 ---------------------------------------------------------------------------------
  OLT |   Mode  |     Upgrade Status     | Version Match | Invalid Version Match
 ---------------------------------------------------------------------------------
  3   | enable |   Upgrade ONU Progress |      enable  |     enable


SWITCH(config-gpon-olt[3])# show onu auto-upgrade model-list
 ---------------------------------------------------------------------------------
  OLT | ONU |    Model    |  Upgrade Status    | Fail-CNT |        Active
 ---------------------------------------------------------------------------------
  3   |   1 | FK_ONT_G420R|              -     |       0 |          22.0.8.26
SWITCH(config-gpon-olt[3])#
```

To display the firmware for ONU auto-upgrade, use the following command.

Command	Mode	Description
show onu auto-upgrade firmware	Enable Global GPON	Shows the firmware information of auto-upgraded ONU.

The following is an example of displaying the firmware for ONU auto-upgrade.

```
SWITCH(config-gpon-olt[3])# show onu auto-upgrade current-fw
Current Firmware : G_ONU_N_2.77-1123.01.G420R.x
```

```
SWITCH(gpon)# show onu auto-upgrade firmware
 ---------------------------------------------------------------------------------
      Model    |         Firmware Name        |     Version    |       Status
 ---------------------------------------------------------------------------------
  FK-ONT_G420R |G_ONU_N_2.77-1123.01.G420R.x |     22.1.8.33  | Download Complete
```

To display the status of ONU firmware, use the following command.

Command	Mode	Description
show onu firmware version *OLT-ID* [*ONU-IDs*]	Enable Global GPON	Shows the status of ONU firmware. OLT-ID: GPON port number ONU-ID: ONU ID (1-128) or ONU serial number
show onu firmware version [*ONU-IDs*]	GPON-OLT	Shows the status of ONU firmware. ONU-ID: ONU ID (1-128) or ONU serial number

- **Changing Active Firmware**

If an ONU supports the dual OS, you can change the active firmware using the following command. To change the active firmware, use the following command.

Command	Mode	Description
onu firmware active-change *ONU-ID*	GPON-OLT	Changes the active OS of ONU (with ONU reboot). ONU-ID: ONU ID (1 to 128) or ONU serial number

11.2.25 Displaying ONU Information

To display the ONU (ONT) information, use the following command.

Command	Mode	Description
show onu info [*OLT-IDs*]	Enable Global GPON	Shows the information of ONU (ONT) per OLT ID. OLT-IDs: GPON port number
show onu detail-info [*OLT-ID*]		Shows the ONU (ONT) information in detail. OLT-ID: GPON OLT port number ONU-ID: ONU ID (1 to 128) or ONU serial number
show onu detail-info [*ONU-ID*]	GPON-OLT	
show onu info [*ONU-ID*]		Shows the ONU (ONT) information.
show onu feature-list [*OLT-ID*]	Enable Global GPON	Shows the ONU feature list.
show onu feature-list [*ONU-ID*]	GPON-OLT	
show onu alarm-status [*ONU-ID*]		Shows the alarm status of ONUs.

To display the registered ONU (ONT) information, use the following command.

Command	Mode	Description
show onu active [*OLT-ID*]	Enable Global	Shows the registered ONU (ONT) information. OLT-ID: GPON port number

show onu active count [*OLT-ID*]	GPON	Shows the number of active ONUs connected to a specified GPON port.
show onu active [*ONU-ID*]	GPON-OLT	Shows the registered ONU (ONT) information. ONU-ID: ONU ID (1 to 128) or ONU serial number
show onu active count		Shows the number of active ONUs.

To display the link status of ONUs, use the following command.

Command	Mode	Description
show onu block status *OLT-ID* [*ONU-ID*]	Enable/Global/GPON	Shows the link status of ONUs OLT-ID: GPON port number ONU-ID: ONU ID (1 to 128) or ONU serial number
show onu block status [*ONU-ID*]	GPON-OLT	

To display a reason of ONU deactivation, use the following command.

Command	Mode	Description
show onu deactive-reason *OLT-ID*	Enable/Global/GPON	Shows the reason of inactive ONUs.
show onu deactive-reason	GPON-OLT	

To display the model names of the ONUs connected to a specified OLT, use the following command.

Command	Mode	Description
show onu model-name *OLT-ID*	Enable/Global/GPON	Shows the model names of the ONUs. ONU-ID: ONU ID (1 to 128) or ONU serial number
show onu model-name [*ONU-ID*]	GPON-OLT	

To display the number of MAC addresses currently learned in an ONU, use the following command.

Command	Mode	Description
show onu mac-address *OLT-ID*	Enable/Global/GPON	Shows the number of MAC addresses currently learned in ONUs connected to a current OLT.
show onu mac-address [*ONU-ID*]	GPON-OLT	

To display a host name of the specified ONU, use the following command.

Command	Mode	Description
show onu hostname *OLT-ID*	Enable Global GPON	Shows a host name of the specified ONU.
show onu hostname [*ONU-IDs*]	GPON-OLT	

To display the IGMP group list of ONU (ONT), use the following command.

Command	Mode	Description
show onu igmp-group-list *OLT-ID ONU-ID*	Enable Global GPON	Shows the current IGMP group list of the ONU. ONU-ID: ONU ID (1 to 128) or ONU serial number
show onu igmp-group-list *ONU-ID*	GPON-OLT	

To display the status of the ONU (ONT) UNI, use the following command.

Command	Mode	Description
show onu uni-status [*OLT-ID*]	Enable Global GPON	Shows the status of the ONU UNI. ONU-ID: ONU ID (1 to 128) or ONU serial number
show onu uni-status [*ONU-IDs*]	GPON-OLT	
show onu uni-status eth *OLT-ID*	Enable Global GPON	Shows the status of ONU UNI Ethernet port.
show onu uni-status eth [*ONU-IDs*]	GPON-OLT	

To display the configured description on ONU UNI port, use the following command.

Command	Mode	Description
show onu uni-description *OLT-ID*	Enable Global GPON	Shows the configured description on ONU UNI port.
show onu uni-description [*ONU-ID*]	GPON-OLT	

To display the configured IP host service ID on ONU, use the following command.

Command	Mode	Description
show onu ip-host *OLT-ID ONU-ID*	Enable Global GPON	Shows the configured IP host service ID on ONU.
show onu ip-host *ONU-ID*	GPON-OLT	

To display the system or RF video status of ONU, use the following command.

Command	Mode	Description
show onu system-status *OLT-ID ONU-ID*	Enable Global	Shows the status of ONU system.

	GPON	
show onu system-status *ONU-ID*	GPON-OLT	
show onu video status *OLT-ID ONU-ID*	Enable Global GPON	Shows the ONU's RF video status.
show onu video status *ONU-ID*	GPON-OLT	

To display the status of ONU supporting Power over Ethernet (PoE) feature, use the following command.

Command	Mode	Description
show onu poe status *OLT-ID ONU-ID*	Enable Global GPON	Shows the status of PoE ONU system.
show onu poe status *ONU-ID*	GPON-OLT	

To display the multicast counter information per UNI Ethernet port of ONU, use the following command.

Command	Mode	Description
show onu igmp-pm-data *OLT-ID ONU-ID* **uni eth** *UNI-PORT*	Enable Global GPON	Shows the IGMP message counters per UNI port of ONU. The counters are a total number of successful/unsuccessful joins, leave messages, general queries, specific queries and invalid IGMP messages. ONU-ID: 1-128 or ONU serial number UNI-PORT: UNI port number
show onu igmp-pm-data *ONU-ID* **uni** {**eth** | **virtual-eth**} *UNI-PORT*	GPON-OLT	
clear onu igmp-pm-data *ONU-ID* **uni** {**eth** | **virtual-eth**} *UNI-PORT*		Clears the collected IGMP message counters.

To display the PPPoE information of ONU, use the following command.

Command	Mode	Description
show onu pppoe account *OLT-ID*	Enable Global GPON	Shows the PPPoE account of ONU.
show onu pppoe status *OLT_ID*		Shows the ONU status information for PPPoE.
show onu pppoe account *ONU-ID*	GPON-OLT	Shows the PPPoE account of ONU.
show onu pppoe status *ONU_ID*		Shows the ONU status information for PPPoE.

To display the system or RF video status of ONU, use the following command.

Command	Mode	Description
show onu video-status update	Enable	Shows the ONU's RF video update status.

show onu video status *OLT_ID ONU_IDs*	Global GPON GPON-OLT	Shows the ONU's RF video status.

To display DBA profile information of ONU, use the following command.

Command	Mode	Description
show onu dba-profile {*OLT_ID* | *ONU_ID*}	Enable Global GPON	Shows the ONU's DBA profiles.
show onu dba-profile [*ONU_ID}*	GPON-OLT	

11.2.26 ONU's Basic Configurations via OLT

Basically, to connect the ONT to the WAN for VoIP and the Internet services, you should have the ONT get the basic configuration via OLT. The following sections explain how to perform the configuration on the connected OLT.

11.2.26.1 Upgrade of ONT

You may have to upgrade ONT first for the purpose of perfect support for the services before the basic ONT configuration.

The following command lines show an example for the ONT upgrade.

```
OLT# copy tftp onu down ❶
        To exit : press Ctrl+D
-------------------------------------
IP address or name of remote host (TFTP): 10.45.33.227
Download File Name : G_ONU_N_NewVersion.420R.x
Now 10.45.33.227 ONU Firmware download from via tftp.
Downloading file ....
Received 16058792 bytes

OLT(config-gpon-olt[2])# onu upgrade 2 G_ONU_N_NewVersion.420R.x ❷
...

OLT(config-gpon-olt[2])# show onu firmware version 2 ❸
                                          (D):Default-OS (R):Running-OS
-----------------------------------------------------------------------
  OLT | ONU |      Upgrade Status     |          OS1          |         OS2
-----------------------------------------------------------------------
  2   | 2 |     Commit Complete     | (D) NewVersion | (R) OldVersion

OLT(config-gpon-olt[2/2])# onu reset 2 ❹
```

❶ Download ONT OS file to OLT
❷ Upgrade ONT with the downloaded OS
❸ Check out the upgrade result
❹ Reboot the ONT. The ONT will be restarted with "Default-OS (*NewVersion*)".

11.2.26.2 Pre-settings for Traffic Profile (Step1)

Basically, it is required that a series of configuration including traffic profile and IP host is predefined at the ONT in order to get access to the Internet and serve the VoIP and data service. This section describes how to have the ONT get the configuration, with a detail sample config on the basis of a sample scheme, for easier understanding and usage of config copy.

The following diagram shows a sample scheme for it.

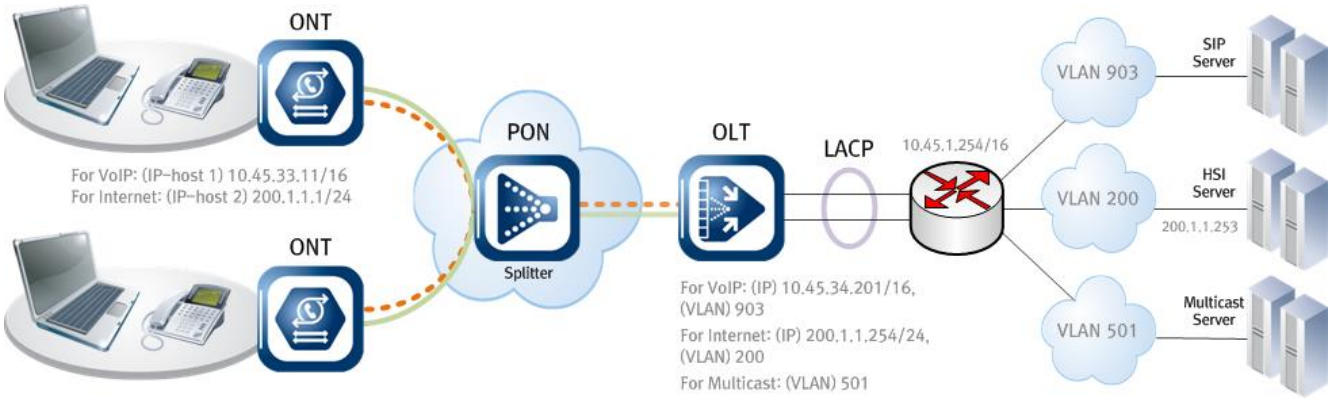


Fig. 11.3 PON Structure Sample Scheme for VoIP and Internet Connection of ONT

The following config command lines show a sample config for pre-settings of traffic-profile corresponding to the sample scheme above.

```
OLT(gpon)# show running-config
...
gpon
...
olt multicast-gem 4094 ❶
olt interwork igmp-snooping enable
!
...
dba-profile BE create ❷
  mode sr
  sla fixed 128
  sla maximum 1031616
  apply
!
dba-profile VOIP create ❷
  mode sr
  sla fixed 128
  sla maximum 4096
  apply
!
...
multicast-profile V501 create ❸
  igmp tag-control add vid 501 cos 0
```

```
  igmp access-list vid 501 dst-ip start 224.0.0.1 end 239.255.255.255 gem 4094
  apply
!
...
 extended-vlan-tagging-operation V200 create ❹
  downstream-mode enable
  untagged-frame 1
   treat inner vid 200 cos 0 tpid 0x8100
  apply
 !
 extended-vlan-tagging-operation V903 create ❹
  downstream-mode enable
  untagged-frame 1
   treat inner vid 903 cos 0 tpid 0x8100
  apply
!
extended-vlan-tagging-operation V501 create ❹
  downstream-mode enable
  untagged-frame 1
   treat inner vid 501 cos 0 tpid 0x8100
  apply
 !
...
voip-profile SIP create ❺
  codec-nego 1 codec pcma packet-period 10 silence-suppression 1
  codec-nego 2 codec pcmu packet-period 10 silence-suppression 1
  codec-nego 3 codec g729 packet-period 10 silence-suppression 1
  codec-nego 4 codec g723 packet-period 10 silence-suppression 1
  protocol sip
   proxy-server 10.45.2.1
   outbound-proxy-server 10.45.2.2
   register-server 10.45.2.3
   host-part-server 10.45.2.4
   dns primary 168.126.63.1
  apply
!
...
```

❶ Add a specific GEM port ID (`4094`) to the multicast stream.

❷ Create DBA profiles (`BE` - for Internet service, `VOIP` - for VoIP service). And then configure the corresponding settings.

❸ Create a multicast profile (`V501`). And then configure the corresponding settings.

❹ Create extended VLAN tagging operation profiles (`V200` - for Internet service, `V903` - for VoIP service, `V501` - for multicast service). And then configure the corresponding settings.

❺ Create a VoIP profile (`SIP`). And then configure the corresponding settings.

11.2.26.3 Traffic Profile Configuration (Step2)

The following command lines show a sample config of traffic profile corresponding to the sample scheme. You can find out which configurations are required for ONT's VoIP and

data service through each annotation.

```
OLT(gpon)# show running-config traffic-profile TRAFFIC

 traffic-profile TRAFFIC create ❶

  mgmt-mode uni eth 1 non-omci link virtual-eth 1 ❷
  mgmt-mode uni eth 2 omci
  mgmt-mode uni eth 3 omci
  mgmt-mode uni eth 4 omci

  tcont 1
   gemport 1/1-1/4
   dba-profile BE ❸
  tcont 2
   gemport 2/1-2/4
   dba-profile BE ❸
  tcont 3
   gemport 3/1
   dba-profile VOIP ❸
  mapper 1
   gemport count 4
  mapper 2
   gemport count 4
  mapper 3
   gemport count 1

  bridge 1
   ani mapper 1
   uni eth 1
    extended-vlan-tagging-operation V200 ❹

  bridge 2
   ani mapper 2
   uni eth 2
    multicast-profile V501 ❺
    extended-vlan-tagging-operation V501 ❹
   uni eth 3
    multicast-profile V501 ❺
    extended-vlan-tagging-operation V501 ❹
   uni eth 4
    multicast-profile V501 ❺
    extended-vlan-tagging-operation V501 ❹

  bridge 3
   ani mapper 3
   link ip-host-config 1

  ip-host-config 1 ❻
   ip address static
   dns primary 168.126.63.1
   link voip-service 1
   extended-vlan-tagging-operation V903

  ip-host-config 2 ❼
   ip address static
```

```
   extended-vlan-tagging-operation V200

  voip-service 1 ❽
   manage-method omci
   voip-profile SIP
   uni pots 1
   uni pots 2
  apply
!
```

❶ Create a traffic profile (`TRAFFIC`).

❷ If you want to set "Bridge", then you should use `omci`.
Otherwise, if you want to set "NAT" or "PPPoE", then you should use `non-omci`.
Basically, `non-omci` configures an interface as "NAT". For the PPPoE, PPPoE enabling on web interface is required additionally.

❸ Associate the created DBA profiles (`BE` - for Internet & multicast service, `VOIP` - for VoIP service) to T-CONT.

❹ Associate the created extended VLAN tagging operation profile to each Ethernet port (`extended-vlan-tagging-operation V200` - for Internet service (`eth 1` in this config), `extended-vlan-tagging-operation V501` - for multicast service (`eth 2` to `eth 4` in this config)).

❺ Associate the created multicast profile (`V501`) to the Ethernet ports for multicast service (`eth 2` to `eth 4` in this config).

❻ Configure `ip-host-config 1`.
The `ip-host-config 1` is a host only for VoIP.
- Configure IP address assignment (`static` in this config).
- Associate a VoIP service (`voip-service 1`) to this configuration (`ip-host-config 1`).
- Associate the created extended VLAN tagging operation profile (`extended-vlan-tagging-operation V903`) to this configuration (`ip-host-config 1`).

❼ Configure `ip-host-config 2`.
The `ip-host-config 2` is a host only for `non-omci`-configured interfaces.
- Configure IP address assignment (`static` in this config).
- Associate the created extended VLAN tagging operation profile (`extended-vlan-tagging-operation V200`) to this configuration (`ip-host-config 2`).

i In case of `ip address static`, it is required to configure DNS. Otherwise, it is set to the Furukawa-specified value, by default, which may cause to limit any service.

❽ Create a VoIP service (`voip-service 1`) to be associated to IP host configuration for VoIP (`ip-host-config 1`). And then configure the corresponding settings. Here, associate the created VoIP profile (`SIP`).

11.2.26.4 ONU Profile & IP Host Configuration (Step3)

The following command lines show a sample config for OLT port corresponding to the sample scheme above.

```
OLT(gpon)# show running-config
```

```
...
onu-profile ONU create ❶
  traffic-profile TRAFFIC
  apply
!
...

OLT(config-gpon-olt[2])# show running-config gpon-olt 2
gpon-olt 2
  olt auto-to-manual enable
  olt anti-spoofing enable expire-timeout 60
  discover-serial-number start 10
  onu add 2 FRKW4bd68b38 auto-learning ❷
  onu-profile 2 ONU ❸
  onu static-ip 2 ip-host 1 10.45.33.11/16 gw 10.45.1.254 ❹
  onu static-ip 2 ip-host 2 200.1.1.1/24 gw 200.1.1.254 ❹
  onu voip-sip 2 phone-number pots 1 07070177670
  onu voip-sip 2 auth pots 1 07070177670 39588102947
```

❶ Create an ONU profile (`ONU`). And then configure the corresponding settings. Here, associate the created traffic profile (`TRAFFIC`) to this profile (`ONU`).

❷ Register an ONT (`FRKW4bd68b38`) to the OLT with specifying its ID (`2`).

❸ Apply the created ONU profile (`ONU`) to the specified ONT (OLT port: `2`, ONU ID: `2`).

❹ Assign the planned static IP addresses to the configured IP hosts (`ip-host 1` for POTS, and `ip-host 2` for LAN1 port on sample config in this guide). Here, `ip-host 1` uses network 10.45.x.x, and `ip-host 2` uses 200.1.1.x.

i To assign static IP address to the IP hosts, `ip address static` should be set in `ip-host-config` of traffic profile first.

i The `ip-host 1` is a host only for VoIP, and the `ip-host 2` is a host only for `non-omci`-configured interfaces.

i If you want to have the VoIP host assigned the same IP as NAT host, you should perform the following: All of the POTS interfaces have to be set to `non-omci` (`mgmt-mode uni pots 1 non-omci` and `mgmt-mode uni pots 2 non-omci`). This tells an IP host binding. The `non-omci`-configured interfaces are all affected by `ip-host 2`.

You can check whether the IP hosts are assigned IP addresses normally and VoIP service is registered normally with the following commands.

```
OLT(config-gpon-olt[2])# show onu ip-host 2
-----------------------------------------------------------------
 OLT : 2, ONU : 2, Host : 1(0x0001)
-----------------------------------------------------------------
 IP Option            : Static ❶
 MAC Address          : b8:26:d4:d6:8b:38
 Config IP            : 10.45.33.11 ❶
 Config Mask          : 255.255.0.0
 Config Gateway        : 10.45.1.254 ❶
 Config Primary DNS    : 168.126.63.1
```

```
 Config Secondary DNS  : 0.0.0.0
 Host name            :
-------------------------------------------------------------
 OLT : 2, ONU : 2, Host : 2(0x0002)
-------------------------------------------------------------
 IP Option            : Static ❶
 MAC Address          : b8:26:d4:d6:8b:38
 Config IP            : 200.1.1.1 ❶
 Config Mask          : 255.255.255.0
 Config Gateway       : 200.1.1.254 ❶
 Config Primary DNS   : 0.0.0.0
 Config Secondary DNS : 0.0.0.0
 Host name            :

OLT(config-gpon-olt[2])# show onu voip line 2
-----------------------------------------------------------------------
OLT : 2, ONU : 2, POTS : 1
-----------------------------------------------------------------------
Line Status                  : Registered ❷
Used Codec                   : Auto select
Session Type                 : Idle
1st Protocol Period / Dest Addr :  20 / 0.0.0.0
2nd Protocol Period / Dest Addr :  20 / 0.0.0.0

-----------------------------------------------------------------------
OLT : 2, ONU : 2, POTS : 2
-----------------------------------------------------------------------
Line Status                  : None/initial
Used Codec                   : Auto select
Session Type                 : Idle
1st Protocol Period / Dest Addr :  20 / 0.0.0.0
2nd Protocol Period / Dest Addr :  20 / 0.0.0.0
```

❶ Check whether IP host configuration is applied normally. (`Host 1` for VoIP, `Host 2` for Internet service)
Ping to the gateway (200.1.1.254) for checking connection with OLT by using PC connected to the ONT.
Ping to the HSI server (200.1.1.253) for checking Internet access by using PC connected to the ONT.

❷ Check whether the VoIP service is registered normally.

11.2.27 Generic Status Portal (GSP)

The generic status portal managed entity provides a way for the OLT to discover the status and configuration information of a non-OMCI management domain within an ONU. The non-OMCI management domain is indicated by the virtual Ethernet interface point associated with this generic status portal.

The generic status portal ME uses two attributes which are **status** and **config** to convey status and configuration from a non-OMCI managed domain to the OMCI. Each of these attributes uses an XML document to present this information.

Whenever the information in this table changes, and after a soak interval, the ONU issues an AVC to the OLT. The rate at which AVCs are issued is controlled by the **avc-report** attribute.

To configure GSP, follow these steps.

Step 1 You need to open *ONU Profile Configuration* mode to configure an ONU profile. To create an ONU profile, use the following command.

Command	Mode	Description
onu-profile *NAME* **create**	GPON	Creates an ONU profile. NAME: ONU profile name

Step 2 To enable GSP function, use the following command.

Command	Mode	Description
gsp {**disable** | **enable**}	ONU-Profile	Enables generic status portal. (default: disable)
gsp avc-report enable {**10min** | **sec**}		Configures the rate of AVC report. 10min: ONU issues one AVC report to the OLT per 10 minutes sec: ONU issues one AVC report to the OLT per seconds enable: Whenever the information changes, ONU generates AVC report. (Not recommended.) disable: Not generating the report to the OLT
gsp avc-report disable		Disables the configured avc-report.

Step 3 You need to apply a created ONU profile to connected ONU, open GPON-OLT Configuration mode where you want to apply the profile.

Command	Mode	Description
gpon-olt *PORT*	GPON	Opens *GPON-OLT Configuration* mode. PORT: OLT's port number

Step 4 To apply the ONU profile to connected ONUs use the following command.

Command	Mode	Description
onu-profile *ONU-IDs NAME*	GPON-OLT	Applies an ONU profile to specified ONUs. ONU-IDs: ONU ID (1 to 128) or ONU serial number NAME: ONU profile name

Step 5 To update GSP information, use the following command.

Command	Mode	Description
onu gsp update {**status** | **config**} *ONU_ID*	GPON-OLT	Updates GSP. ONU_ID: ONU ID (1 to128) or ONU serial number

i In case of **enable** status, whenever the information in the table changes, GSP will be automatically updated according to ***Step 2*** avc-report rate settings.

Step 6 To display a current configured GSP information, use the following command.

Command	Mode	Description
show onu gsp {**config** | **status**} *ONU_ID*	GPON-OLT	Shows the configured GSP information. config: configuration document table status: status document table ONU_ID: ONU ID (1 to128) or ONU serial number TAG_NAME: tag name
show onu gsp {**status** | **config**} *ONU_ID* **tag** *TAG_NAME*		
show onu gsp {**status** | **config**} *ONU_ID* **tag-list**		

The following is an example of configuring a GSP.

```
...
SWITCH(gpon)# onu-profile LD3211 create
SWITCH(config-onu-profile[LD3211])# gsp enable
SWITCH(config-onu-profile[LD3211])# apply
!
...
SWITCH(config-onu-profile[LD3211])# exit
SWITCH(gpon)# gpon-olt 1/1
SWITCH(config-gpon-olt[1/1])# show onu model-name 11
-------------------------------

 OLT | ONU | Model Name

-------------------------------

 1/1 | 11 | LD3211

SWITCH(config-gpon-olt[1/1])# onu-profile 11 LD322
SWITCH(config-gpon-olt[1/1])# onu gsp update config 11
SWITCH(config-gpon-olt[1/1])# show onu gsp config 11
  <?xml version="1.0"?>
  <gspResponse type="config">
      <ONTSystemInfo>
            <SoftImage type="0" Active="1">1.42-0001</SoftImage>
            <SoftImage type="1" Active="0">1.42-0001</SoftImage>
            <PONTrafficStatus PONMode="GPON">up</PONTrafficStatus>
            <DeviceInfo>
                  <ModelName>LD3211</ModelName>
                  <SystemMacAddress>b8:26:d4:00:38:88</SystemMacAddress>
```

```
            <LANMacAddress>b8:26:d4:00:38:8f</LANMacAddress>

            <SystemUpTime>4 hour/5 min/56 sec</SystemUpTime>

        </DeviceInfo>
...
```

11.3 ONU Profile

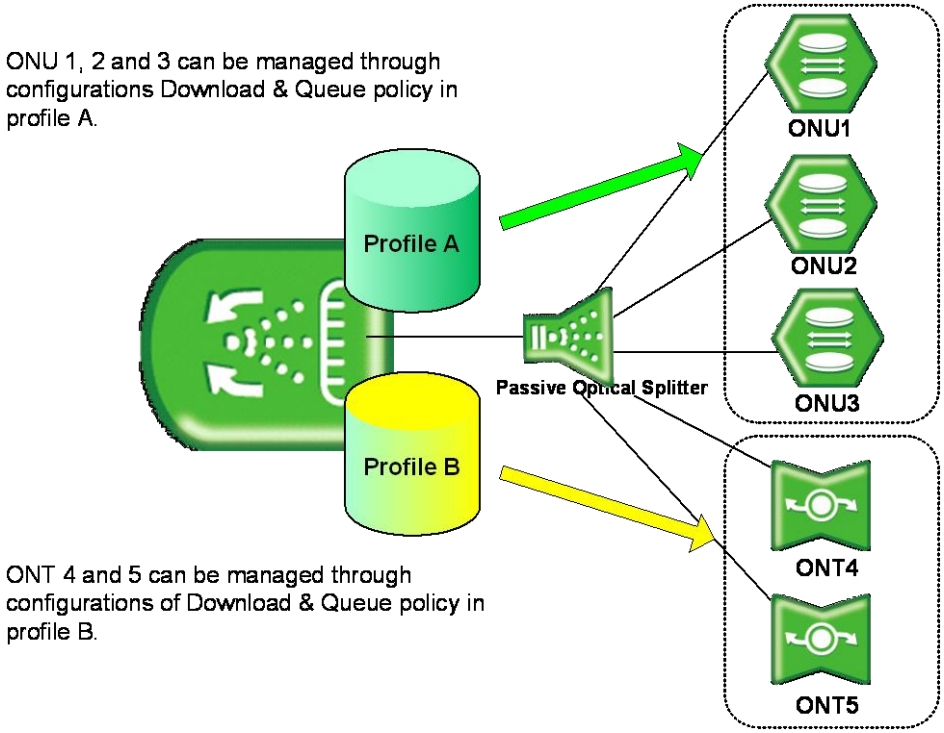


Fig. 11.4 ONU Profile

The provides the easy and efficient management solution for various service environments with the ONU profile.

The ONU profile is a collection of configurations for the operation of an ONU (ONT). You can manage all ONUs connected to an OLT by simply applying the configured profile to ONUs without any local configuration. In case of a modification of a profile, the modified configurations will be automatically applied to ONUs, which are managed by the profile.

This will prevent unnecessary resources to configure every single ONU (ONT), allowing the maintenance efficiency to dramatically increase.

⚠ One ONU profile can be applied to several ONUs (ONTs), but one ONU cannot be managed by several ONU profiles.

11.3.1 Creating ONU Profile

You need to open *ONU Profile Configuration* mode to configure an ONU profile. To create an ONU profile, use the following command.

Command	Mode	Description
onu-profile *NAME* **create**	GPON	Creates an ONU profile. NAME: ONU profile name

To modify an existing ONU profile, use the following command.

Command	Mode	Description
onu-profile *NAME* **modify**	GPON	Modifies an ONU profile. NAME: ONU profile name

To delete a created ONU profile, use the following command.

Command	Mode	Description
no onu-profile {*NAME* | **all**}	GPON	Deletes an ONU profile. NAME: ONU profile name

11.3.2 Configuring ONU Profile

11.3.2.1 RX Optical Power Threshold

The ONUs periodically monitor the RX optical power and send the alarm message to their OLT when the RX optical power exceeds the user-defined threshold. To set the transmit rate of an UNI port, use the following command.

Command	Mode	Description
rx-power threshold {**low** *VALUE* [**high** *VALUE*] | **high** *VALUE* [**low** *VALUE*] }	ONU-Profile	Sets the RX optical power threshold and sends RX power high/low alarm to OLT when the RX power exceeds the threshold or it is below the threshold. VALUE: -127 to 0 dBm
no rx-power threshold [**low** | **high**]		Deletes the configured RX optical power threshold.

11.3.2.2 Rogue ONU

The first method is that after detecting the existence of a rogue ONT, the rouge ONT is identified and isolated from the service by the OLT.

GPON OLT allocates the time slot for each ONU to transmit upstream traffic similarly to the TDM method. The allocated time is announced by the bandwidth map that is contained in the downstream GEM frame and the ONT only transmits the traffic based on the allocated bandwidth map. Due to this nature of GPON technology, the wrong transmit time of the ONT makes collision in upstream direction. This can be resulted from continuous transmitting data of the malfunctioned ONT which is called “Rogue ONT”.

The polling interval attribute represents the interval of polling optical transceiver at the ONT. And the polling count for rogue ONT attribute represents the number of consecutive polling, which results in abnormality, for declaring the optical transceiver as abnormal.

To configure a polling interval and count for rogue ONT, use the following command.

Command	Mode	Description
rogue onu polling [<10-60000> <1-250>]	ONU-Profile	Specifies a polling interval and count for rogue ONT. 10-60000: polling interval value (unit: millisecond) 1-250: polling count
rogue onu polling disable		Deletes the specified polling interval and count.

To enable/disable the alarm for rogue ONU and specify the alarm count that is the maximum number of retransmission of alarms in case of no response from OLT, use the following command.

Command	Mode	Description
rogue onu alarm enable <1-5>	ONU-Profile	Enables the alarm after detecting a rogue ONU. 1-5: alarming count
rogue onu alarm disable		Disables the alarm after detecting a rogue ONU.

To set the waiting time for OLT's response, use the following command.

Command	Mode	Description
rogue onu waiting-time <100-50000>	ONU-Profile	Sets the waiting time for OLT's response 100-50000: waiting time (unit: millisecond)
rogue onu waiting-time disable		Deletes the specified waiting time for OLT's response.

11.3.2.3 Card Type Configuration

You need to select a card type in case that ONT is provided with the configurable circuit pack (e.g., T1/E1). To set a card type on the configurable circuit pack, use the following command.

Command	Mode	Description
circuit-pack card-config c-ds1-e1 {**ds1** | **e1**}	ONU-Profile	Selects a card type on the configurable circuit pack. c-ds1-e1: Configurable DS1/E1 module c-ds1-e1-j1: Configurable DS1/E1/J1 module
circuit-pack card-config c-ds1-e1-j1 {**ds1** | **e1** | **j1**}		
no circuit-pack card-config {**c-ds1-e1** | **c-ds1-e1-j1**}		Deletes the configuration of card type on the configurable circuit pack.

11.3.2.4 Loop Detect Configuration

A loop may occur when double paths are used for the link redundancy between switches and one sends unknown unicast or multicast packet that causes endless packet floating on the LAN. That superfluous traffic eventually can result in network fault.

The provides the function to configure the ONU's loop detecting. The loop detecting mechanism is as follows:

The ONU periodically sends the loop-detecting packet to all the ports with a certain interval, and then if the loop-detecting packet is received, the switch performs a pre-defined behavior.

To enable/disable the loop detection, use the following command.

Command	Mode	Description
loop-detect {**enable** | **disable**}	ONU-Profile	Enables/disables the loop detection.

To define the behavior when a loop is occurred, use the following command.

Command	Mode	Description
loop-detect block	ONU-Profile	Enables the blocking option. This configures to automatically change the state to BLOCKED when a loop is detected. (default: disable)
loop-detect block block-timer {<1-65535> | **unlimited**}		Sets the interval of changing the state of BLOCKED to NORMAL. 1-65535: interval (unit: second, default: 600) unlimited: do not change the state
no loop-detect block		Disables the blocking option.

To set the interval of sending the loop-detecting packet, use the following command.

Command	Mode	Description
loop-detect send-period <1-65535>	ONU-Profile	Sets the interval of sending the loop-detecting packet. 1-65535: interval (unit: second)

11.3.2.5 ONU Threshold

To set the threshold of ONU CPU load, use the following command.

Command	Mode	Description
cpu-load threshold <0-100>	ONU-Profile	Sets the threshold of CPU load in the unit of percent (%). 0-100: ONU CPU load threshold value
no cpu-load threshold		Deletes the configured threshold of CPU load.

To set the threshold of ONU temperature, use the following command.

Command	Mode	Description
temperature high-threshold <-40-100>	ONU-Profile	Sets the threshold of ONU temperature in the unit of centigrade (°C). -40-100: ONU temperature
temperature low-threshold <-40-100>		
no temperature { **high-threshold** | **low-threshold** }		Deletes a configured threshold of ONU temperature.

To set the threshold of ONU memory in use, use the following command.

Command	Mode	Description
memory-usage threshold <0-100>	ONU-Profile	Sets the threshold of ONU memory in the unit of percent (%). 0-100: ONU memory in use
no memory-usage threshold		Deletes the configured threshold of ONU memory.

11.3.2.6 IGMP Configuration

To specify the maximum number of IGMP groups, use the following command.

Command	Mode	Description
igmp max-groups <0-255>	ONU-Profile	Specifies the maximum number of IGMP groups. 0-255: maximum number of IGMP groups
no igmp max-groups		Deletes the specified maximum number of IGMP groups.

IGMP rate limiting restricts the number of IGMP messages from ONUs within this ONU-profile. To configure the upstream IGMP rate limit of ONUs, use the following command.

Command	Mode	Description
igmp us-rate-limit <1-65535>	ONU-Profile	Sets the maximum number of upstream IGMP messages. 1-65535: the number of IGMP messages (unit: messages per second)
no igmp us-rate-limit		Deletes the configured upstream IGMP rate limit.

11.3.2.7 Rate-limit Configuration

To configure the rate limit for downstream traffic of ONUs, use the following command.

Command	Mode	Description
rate-limit downstream {*RATE* | **unlimited**}	ONU-Profile	Sets the downstream traffic bandwidth for ONU. RATE: 0 to 2147483584 (in steps of 64Kbps)
no rate-limit downstream		Deletes the configured rate limit

11.3.2.8 GPON Optic Module Threshold of ONU

The ONU's GPON optic module can operate depending on monitoring type of temperature, RX/TX power, voltage or Txbias. To set the threshold of GPON optical transceiver of ONU, use the following command.

Command	Mode	Description
ani-rx-power threshold {**low** *VALUE* [**high** *VALUE*] | **high** *VALUE* [**low** *VALUE*] }	ONU-Profile	Configures the RX optical power threshold and sends the configured threshold value to ONUs. The ONUs monitors the change of values and sends RX power

		high/low alarm to OLT when the RX power exceeds the threshold or it is below the threshold. VALUE: RX power threshold value (-127 to 0 dBm)
ani-tx-power threshold {**low** *VALUE* [**high** *VALUE*] | **high** *VALUE* [**low** *VALUE*] }		Configures the TX optical power threshold and sends the configured threshold value to ONUs. The ONUs monitors the change of values and sends TX power high/low alarm to OLT when the TX power exceeds the threshold or it is below the threshold. VALUE: TX power threshold value (-127 to 0 dBm)
ani-temperature threshold {**low** *VALUE* [**high** *VALUE*] | **high** *VALUE* [**low** *VALUE*] }		Configures the temperature threshold and sends the configured threshold value to ONUs. The ONUs monitors the change of values and sends temperature high/low alarm to OLT when the temperature exceeds the threshold or it is below the threshold. VALUE: temperature threshold value (-128～127℃)
ani-tx-bias threshold {**low** *VALUE* [**high** *VALUE*] | **high** *VALUE* [**low** *VALUE*] }		Configures the txbias threshold and sends the configured threshold value to ONUs. The ONUs monitors the change of values and sends txbias high/low alarm to OLT when the txbias exceeds the threshold or it is below the threshold. VALUE: tx-bias threshold value (0～ 131 mA)
ani-voltage threshold {**low** *VALUE* [**high** *VALUE*] | **high** *VALUE* [**low** *VALUE*] }		Configures the voltage threshold and sends the configured threshold value to ONUs. The ONUs monitors the change of values and sends voltage high/low alarm to OLT when the voltage exceeds the threshold or it is below the threshold. VALUE: voltage threshold value (0～ 10.0 V)

To delete the threshold of module operation depending on specified monitoring type, use the following command.

Command	Mode	Description
no {**ani-rx-power** | **ani-voltage** | **ani-tx-bias** | **ani-tx-power** | **ani-temperature**} **threshold** [{**low** | **high**}]	ONU-Profile	Deletes the configured threshold.

11.3.2.9 CPU Packet Limit

ONU CPU packet limitation is one of important protecting mechanism from traffic attacking. For example, the ONU CPU packet forwarding is configured with 1000 PPS for broadcast packet, 1000 broadcast packet per second will be forwarded by ONU CPU.

To configure maximum PPS of ONU for Broadcast / Unknown-multicast / L2 DLF type of packet, use the following command.

Command	Mode	Description
cpu-packet-limit {**broadcast** | **multicast** | **dlf**} *RATE*	ONU-Profile	Limits the broadcast / unknown-multicast / L2 DLF packets per second forwarded by ONU CPU.

		RATE: 100 to 40000 PPS (Unit: packet per second)
no cpu-packet-limit {**broadcast** | **multicast** | **dlf**}		Deletes the configured CPU packet limit.

11.3.2.10 DLF Trap to CPU

To enable/disable the upstream Destination Lookup Failure (DLF) packet forwarding to a CPU, use the following command.

Command	Mode	Description
trap-to-cpu dlf enable	ONU-Profile	Forwards the upstream DLF packets to a CPU.
trap-to-cpu dlf disable		Forwards the upstream DLF packets according to the VLAN rules.

11.3.2.11 MAC Full Policy

By default, ONT will block new source MAC address frame when ONT MAC table is full. The protecting mechanism can be configurable by 'block or forwarding', thus you can configure the basic policy of ONT when MAC table is full.

To block/forward new source MAC address frame when MAC table is full, use the following command.

Command	Mode	Description
mac-full policy forward	ONU-Profile	Forwards new source MAC address frame when ONU MAC table is full.
mac-full policy drop		Blocks new source MAC address frame when ONU MAC table is full.

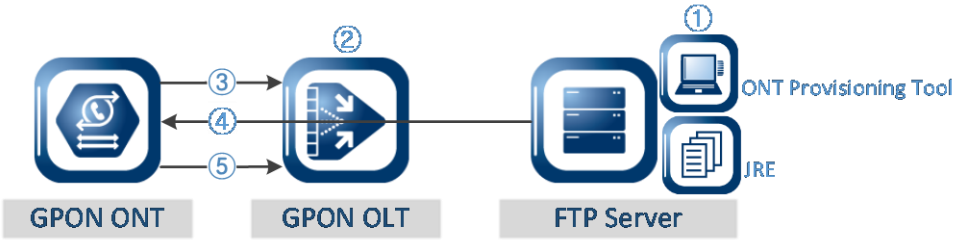
11.3.2.12 ONT Auto-configuration and Service Provisioning

Automated provisioning and remote management of ONTs are vital service delivery activities of ISPs and operators - helping to reduce costs, lead times and complexity as well as to deploy new subscriber services.

ONT provisioning method simplifies network operations by eliminating the need to configure every network element interface between the OLT ingress and subscriber ports of our ONTs for diverse GPON service applications.

If the ONT service provisioning settings in XML file are saved in a FTP server prior to installation/activation of ONTs, the OLT can relay the configured XML file from the FTP server to the activated ONTs using the commands.

ONT Provisioning Process



① **ONT Provisioning Tool & JRE Installation**: Install JRE (version 1.6) and provisioning tool (ONTProvisionTool.exe) to FTP server. Create a new XML configuration file and modify the ONT settings for ONT provisioning. The ONT configuration parameters can be changed or saved in XML.

② **File Transfer from FTP server to ONT**: For the ONT configuration file (XML file) transfer, the ONT provisioning-related commands should be executed on the OLT. The OLT is capable to relay the user-defined XML file from the FTP server to the activated ONTs.

③ **ONT Activation**

④ **Receive XML configuration file from FTP server**: The ONT receives the ONT service configuration file in XML from FTP server. The new service settings are assigned to this ONT.

⑤ **Send File Transfer Message**: On the OLT side, the OLT can monitor a file transfer status by receiving the messages ("File transfer in progress", "File transfer complete", "Remote failure", "Local failure") from ONT.

IP-Path Management

To configure the ONT provisioning feature in *GPON-OLT Configuration* mode and specify a FTP server and GPON provisioning file, use the following command.

Command	Mode	Description
onu mgmt-mode ip-path *ONU_ID* **ftp id** *ID* **password** [*PASSWORD*]	GPON-OLT	Sets an user name and password to access FTP server for GPON ONT provisioning. ONU-ID: 1-128 or ONU serial number ID: user name PASSWD: password
onu mgmt-mode ip-path *ONU_ID* **uri** *URI* **file** {*FILE_NAME* | **none**}		Specifies a FTP server and ONT provisioning file (XML file) name. URI: FTP server address FILE_NAME: ONT provisioning file name **none**: The file name is named after GPON serial number of each ONT. The ONT is supposed to ask .xml provisioning file named after its own GPON serial number. If selecing this option, it is necessary that the FTP server has each .xml provisioning file corresponding to each ONT.
no onu mgmt-mode ip-path		Deletes the configurations of GPON provisioning.

ONU_ID		

To configure the ONT provisioning feature in *ONU-Profile Configuration* mode and specify a FTP server and GPON provisioning file, use the following command.

Command	Mode	Description
mgmt-mode mode ip-path	ONU-Profile	Selects the MGMT IP-Path mode for ONT provisioning.
mgmt-mode ip-path ftp id *ID* **password** [*PASSWORD*]		Sets an user name and password to access FTP server for GPON ONT provisioning. ID: user name PASSWD: password
mgmt-mode ip-path uri *URI* **file** {*FILE_NAME* | **none**}		Specifies a FTP server and ONT provisioning file (XML file) name. URI: FTP server address FILE_NAME: ONT provisioning file name **none**: The file name is named after GPON serial number of each ONT. The ONT is supposed to ask .xml provisioning file named after its own GPON serial number. If selecing this option, it is necessary that the FTP server has each .xml provisioning file corresponding to each ONT.
no mgmt-mode mode		Deletes the configured GPON provisioning mode.
no mgmt-mode ip-path		Deletes the configurations of GPON provisioning per ONT.

i You can configure ONT provisioning in both *ONU-Profile* and *GPON-OLT* Configuration modes. The configuration in *GPON-OLT* mode has higher priority in the system.

To display the GPON provisioning configuration for each ONT, use the following command.

Command	Mode	Description
show onu mgmt ip-path *OLT-ID*	Enable Global GPON	Shows the information of ONT provisioning configuration.
show onu mgmt ip-path *ONU-ID*	GPON-OLT	

TR-069 Management

One of the provisioning methods is the standard open protocol TR-069. The TR-069 protocol is HTTP-based and provides communication between the ONT and an ACS (Auto Configuration Server). TR-069 protocol simplifies ONT management by specifying the use of an ACS to perform remote, centralized management of ONTs. The supports TR-069 to provision and manage ONTs.

To enable/disable the TR-069 management, use the following command.

Command	Mode	Description
mgmt-mode mode tr-069	ONU-Profile	Enables the TR-069 management mode.
no mgmt-mode mode		Disables the TR-069 management mode.

To configure the TR-069 management mode, use the following command.

Command	Mode	Description
mgmt-mode tr-069 uri *URI*	ONU-Profile	Configures TR-069 management server address. URI: URI address of the TR-069 management server
mgmt-mode tr-069 access id *ID* **password** *PASSWD*		Specifies the user name and password to access management server. ID: user name PASSWD: password
mgmt-mode tr-069 associated-tag *VLAN*		Specifies a VLAN ID for TR-069 traffic.
no mgmt-mode tr-069 uri		Deletes the configured server address.
no mgmt-mode tr-069 access		Deletes the defined user name and password.
no mgmt-mode tr-069 associated-tag		Deletes the VLAN ID for TR-069 management.

11.3.2.13 Applying Traffic & PM Profile

To add/delete the user-defined Traffic profile to a specified ONU profile, use the following command.

Command	Mode	Description
traffic-profile *NAME*	ONU-Profile	Adds the existing Traffic profile to ONU profile. NAME: Traffic profile name
no traffic-profile *NAME*		Removes the Traffic profile from ONU profile.

i For the details of how to create and configure the traffic profile, see 11.4 Traffic Profile.

To add/delete the user-defined PM profile to a specified ONU profile, use the following command.

Command	Mode	Description
pm-profile *NAME*	ONU-Profile	Adds the existing PM profile to ONU profile. NAME: Traffic profile name
no pm-profile		Removes the PM profile from ONU profile.

i For the details of how to create and configure the PM profile, see 11.10 Performance Monitoring (PM) Profile.

11.3.3 Overwriting Traffic Profile Configuration

Basically, one traffic profile can be applied to the ONU profile. So, if a number of cases for traffic profile configuration are required on the ONU profile, the user should create the corresponding traffic profiles and apply them to the ONU profile.

The overwriting traffic profile configuration can help reducing the count of creating and applying the traffic profile. This configuration overwrites the corresponding setting of the applied traffic profile.

11.3.3.1 VLAN Configurations

To configure a VLAN tagging operation for a specific UNI port, use the following command.

Command	Mode	Description
uni eth *UNI-PORT* **vlan-operation us-oper keep**	ONU-Profile	Sets the policy of VLAN tagging for upstream frame. keep: keeps forwarding the existing tagged/untagged frame
uni eth *UNI-PORT* **vlan-operation us-oper** {**add** | **overwrite**} <1-4094> <0-7>		Sets the policy of VLAN tagging for upstream frame. add: adds a specified VID (double tagging) with tag in case of tagged frame overwrite: replaces an existing tagged/untagged frame to a specified VID with tag. 1-4094: VLAN ID 0-7: CoS value
uni eth *UNI-PORT* **vlan-operation ds-oper** {**keep** | **remove**}		Sets the policy of VLAN tagging for downstream frame. keep: keeps forwarding the incoming tagged frame from OLT to UNI. remove: removes a tag from the incoming tagged packet and forwards it to UNI.
no uni eth *UNI-PORT* **vlan-operation us-oper**		Deletes the configured policy of VLAN tagging operation.
no uni eth *UNI-PORT* **vlan-operation ds-oper**		

11.3.3.2 Max Host

To configure the maximum number of hosts for a MAC bridge ID, use the following command.

Command	Mode	Description
bridge *BRIDGE-ID* **max-hosts** <0-255>	ONU-Profile	Sets the maximum number of hosts that can connect to the specified MAC bridge ID. BRIDGE-ID: MAC bridge ID 0-255: the maximum number of hosts (0: unlimited)

11.3.3.3 Rate Limit

To configure the rate limit for downstream traffic of an ONU, use the following command.

Command	Mode	Description
uni eth *UNI-PORT* **rate-limit downstream** *PIR_BANDWIDTH* [*SIR_BANDWIDTH*]	ONU-Profile	Sets the downstream traffic bandwidth for UNI port. SIR_BANDWIDTH: 0 to 2147483584 (in steps of 64Kbps) PIR_BANDWIDTH: 0 to 2147483584
no uni eth *UNI-PORT* **rate-limit**		Deletes the configured rate limit

11.3.3.4 IGMP Group List

You can configure the maximum number of multicast groups that a host on a port can join. To specify the maximum number of IGMP groups per UNI-side port, use the following command.

Command	Mode	Description
uni eth *UNI-PORT* **igmp max-groups** <0-255>	ONU-Profile	Specifies the maximum number of IGMP groups for a port. UNI-PORT: UNI port number 0-255: number of IGMP groups (default: 16)
no uni eth *UNI-PORT* **igmp max-groups**		Deletes a specified maximum number of IGMP groups.

11.3.3.5 Activating Administration for Ethernet UNI

To enable/disable the administration of the Ethernet UNI port, use the following command.

Command	Mode	Description
uni eth *UNI-PORT* **port-admin** {**enable** | **disable**}	ONU-Profile	Enables/disables the administration of Ethernet UNI port on the specified ONU.

i

To see the admin status of the ONU (ONT) UNI, use **show onu uni-status** command. (See 11.2.25 Displaying ONU Information)

11.3.3.6 Mapping between T-CONT ID and DBA profile

To specify the GEM ports (priority queue) per T-CONT and the bandwidth of GEM port by mapping between T-CONT ID and DBA profile, use the following command.

Command	Mode	Description
tcont *TCONT-ID* **dba-profile** *DBA-PROFILE*	ONU-Profile	Specifies the priority queues of T-CONT by mapping between the DBA profile and T-CONT ID. Sets T-CONT's bandwidth by specifying the DBA profile DBA-PROFILE: DBA profile name
no tcont *TCONT-ID* **dba-profile**		Disables the mapping between T-CONT ID and DBA profile.

11.3.4 Saving Profile

After configuring an ONU profile, you need to save the profile with the following command.

Command	Mode	Description
apply	ONU-Profile	Saves an ONU profile configuration.

Even if you modify a running profile, you also need to use the **apply** command to apply the changes to ONUs (ONTs).

11.3.5 Applying ONU Profile

If you want to apply a created ONU profile to connected ONUs (ONTs), open *GPON-OLT Configuration* mode where you want to apply the profile.

```
SWITCH(config-gpon-profile[AAA])# exit
SWITCH(gpon)# gpon-olt 1
SWITCH(config-gpon-olt[1])#
```

To apply/release an ONU profile to/from connected ONUs (ONTs), use the following command.

Command	Mode	Description
onu-profile *ONU-IDs NAME*	GPON-OLT	Applies an ONU profile to specified ONUs. ONU-IDs: ONU ID (1 to 128) or ONU serial number NAME: ONU profile name
no onu-profile *ONU-IDs*		Releases an ONU profile from connected ONUs. ONU-ID: ONU ID (1 to 128) or ONU serial number

11.3.6 Checking ONU Profile Configuration

To display the status of ONU profile configuration, use the following command.

Command	Mode	Description
show onu status [*OLT-ID*]	Enable Global GPON	Shows the status of ONU profile configuration.
show onu status [*ONU-ID*]	GPON-OLT	

You should check the status of ONU profile configuration by using the **show onu status** command. If the configuration is normal, the system shows “success”. Otherwise, if the configuration fails, it shows the reason of failure.

The following is an example of displaying the status of ONU profile configuration.

```
SWITCH(config-gpon-olt[1])# show onu status
-----------------------------------------------------------------------
  OLT | ONU |  ACTIVE  |    Fail Reason     | Profile Name
-----------------------------------------------------------------------
  1   |   1 |  Active  |        Success     | 420R
```

11.3.7 Assigning IP Host of SNMP Agent

To assign IP host of SNMP agent, use the following command.

Command	Mode	Description
snmp agent-address ip-host <1-32>	ONU-Profile	Assigns an IP host of SNMP agent. 1-32: IP host number
no snmp agent-address ip-host		Deletes the configured IP address of SNMP agent

11.3.8 SNMP Trap Host

To set an SNMP trap host, use the following command.

Command	Mode	Description
snmp trap-host *A.B.C.D* [port <1-65535>]	ONU-Profile	Specifies an SNMP trap v1 host.
no snmp trap-host		Deletes a SNMP trap v1 host.

11.3.9 Displaying ONU profile

To display a configured ONU profile, use the following command.

Command	Mode	Description
show onu-profile [*NAME*]	GPON GPON-OLT ONU-Profile	Shows a configured ONU profile. NAME: ONU profile name

To display the list of ONUs (ONTs) where an ONU profile is applied, use the following command.

Command	Mode	Description
show onu-profile onu-list *NAME*	Enable Global GPON	Shows the list of ONUs (ONTs) where an ONU profile is applied. NAME: ONU profile name

To display the information of current profile, use the following command.

Command	Mode	Description

show current-profile	Current-Profile	Shows the information currently configured for the profile.

11.4 Traffic Profile

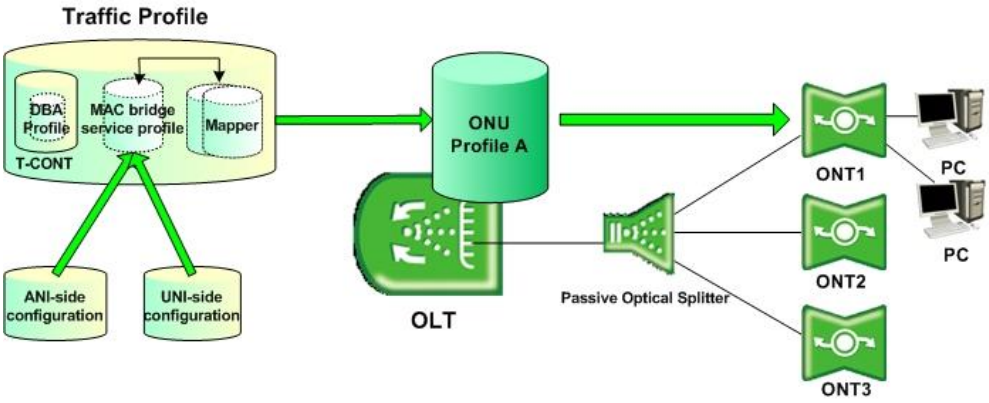


Fig. 11.5 Traffic Profile

The provides the easy and efficient management solution for various service models that are comprised of MAC bridging and 802.1p mapping functionality using the traffic profile.

There are two major layer 2 functions available: MAC bridging and 802.1p mapping. MAC bridging is described in IEEE 802.1D. The bridge has many features, and can be used to direct traffic based on MAC address or on VLAN characteristics (using the VLAN filter feature). The mapping function describes the steering of traffic from one UNI-side entity to ANI-side port-IDs. The mapper is equivalent to a MAC bridge with VLAN filters that only operate on the priority bits of the VLAN tags.

i The is supported by all G.984.4 compliant vender system based on the 1:N, N:M, 1:MP, and N:MP model. Only a single 802.1p mapper is need for 1:N, N:M model deployments. However, multiple 802.1p mappers can be used for 1:MP, N:MP model deployments.

11.4.1 Creating Traffic Profile

To create a traffic profile and open *Traffic Profile Configuration* mode, use the following command.

Command	Mode	Description
traffic-profile *NAME* **create**	GPON	Creates a traffic profile. NAME: traffic profile name

After opening *Traffic Profile Configuration* mode, the prompt changes from SWITCH(gpon)# to SWITCH(config-traffic-pf[*NAME*])#.

To delete a created traffic profile, use the following command.

Command	Mode	Description
no traffic-profile {*NAME* | **all**}	GPON	Deletes the traffic profile with its all configurations.

To modify an existing traffic profile, use the following command.

Command	Mode	Description
traffic-profile *NAME* **modify**	GPON	Modifies the existing traffic profile. NAME: traffic profile name

i The OMCI and service model of MAC bridging and 802.1p mapping functionality must be supported by the ONUs (ONTs).

11.4.2 Creating a Mapper

A mapper provides support for upstream flow routing based on 802.1p priority bits. The supports the DSCP to IEEE802.1p mapping to allow the OLT to prioritize all traffic based on the incoming DSCP value according to the DiffServ to IEEE802.1p mapping table.

To create an IEEE802.1p mapper for a specified traffic profile, use the following command.

Command	Mode	Description
mapper *MAPPER_ID*	Traffic-Profile	Creates a 802.1p mapper for a specified traffic profile. MAPPER_ID: 1 to 32, 802.1p mapper ID
no mapper *MAPPER_ID*		Removes the created mapper from the traffic profile

To configure a mapper for upstream transmission, use the following command.

Command	Mode	Description
gemport count {**1** | **2** | **4** | **8**}	Traffic-Mapper	Sets the GEM port count of mapper. The GEM port count corresponds to a total number of priority queues.
dscp-to-pbit {**enable** | **disable**}		Enables/disables the DSCP to P-bit marking for untagged frame forwarding.
default-cos <0-7>		Specifies CoS value for untagged frame forwarding.
cos-mapping cos *RANGE* **gemport** *GEM-PORT-VALUE*		Specifies the range of CoS values for mapping with GEM port. RANGE: CoS range GEM-PORT-VALUE: corresponds to the gemport count

i If a mapper is associated with ports of a bridge, the 802.1ag entities should be associated with the bridge and its port, rather than with the mapper.

To configure the rate limit for an GEM port ID, use the following command.

Command	Mode	Description
gemport *GEM-PORT-RANGE* **rate-limit** { **upstream** | **downstream** } *PIR_BANDWIDTH* [*SIR_ BANDWIDTH*]	Traffic-Mapper	Sets the downstream/upstream traffic bandwidth for GEM port ID. RANGE: GEM port range SIR_VALUE: SIR bandwidth range of 0 to 2147483584 (in steps of 64Kbps)

		PIR_VALUE: PIR bandwidth range of 0 to 2147483584
no gemport *GEM-PORT-RANGE* **rate-limit** { **upstream** | **downstream** }		Deletes the configured rate limit of GEM port ID.

i You should configure GEM port count for mapper before setting the rate limit for GEM port.

To apply the configured Rate-limit profile for GEM ports, use the following command.

Command	Mode	Description
gemport *RANGE* **rate-limit profile** *NAME*	Traffic-Mapper	Applies the configured Rate-limit profile to specified GEM port. NAME: Rate-limit profile name
no gemport *RANGE* **rate-limit profile**		Removes the Rate-limit profile from the GEM port.

i For the details of how to create and configure the Rate-limit profile, see 11.12 Rate-limit Profile.

11.4.3 MAC Bridge Service Profile

A MAC bridge service profile can be configured per each UNI-side port or it can be configured for the multiple UNI-side ports.

The MAC bridge service profile is comprised of ANI-side port for the upstream traffic management and UNI-side port for the downstream traffic management. The system creates both ANI-side and UNI-side MAC bridge port config data ME.

To create a bridge ID and open a *MAC Bridge Service Profile Configuration* mode, use the following command.

Command	Mode	Description
bridge *BRIDGE_ID*	Traffic-Profile	Creates a bridge ID in traffic profile. BRIDGE_ID: 1 to 32, MAC Bridge ID

After opening *MAC Bridge Service Profile Configuration* mode, the prompt changes from SWITCH(gpon)# to SWITCH(config-traffic-pf[*NAME*]-bridge[*BRIDGE_ID*])#.

To remove the configured bridge ID from a traffic profile, use the following command.

Command	Mode	Description
no bridge *BRIDGE_ID*	Traffic-Profile	Removes the configured bridge ID from a traffic profile

11.4.3.1 Max Host

To configure the max host for a MAC bridge service profile, use the following command.

Command	Mode	Description
max-hosts <0-255>	Traffic-Bridge Traffic Bridge-UNI	Sets the maximum number of hosts. 0-255: maximum MAC number (0: unlimited)
no max-hosts		Deletes the configured max host.

11.4.3.2 MAC Learning

To enable/disable the ONU's MAC learning, use the following command.

Command	Mode	Description
mac-learning {**enable** | **disable**}	Traffic-Bridge	Enables/disables the MAC learning for this bridge service profile. (default: enable)

11.4.3.3 Port Bridge

The L2 port bridge feature allows the port to forward the packets that the outgoing interface in the MAC address entry is the same as the incoming interface where the packet arrived. To enable/disable the L2 port bridge feature, use the following command.

Command	Mode	Description
port-bridge enable	Traffic-Bridge	Enables L2 port bridge feature.
port-bridge disable		Disables L2 port bridge feature.

11.4.3.4 Multicast Interworking Termination Point

The multicast GEM port is represented by a GEM network Connection Termination Point Managed Entity (CTP ME) and a multicast GEM interworking TP ME. The multicast GEM interworking TP is then connected into the ONU through a MAC Bridge Config Data ME.

To enable/disable the MAC bridge port configuration of MAC bridge service profile for multicast Interworking Termination Point (IW TP), use the following command.

Command	Mode	Description
multicast link-mac-bridge enable	Traffic-Bridge	Connects the multicast GEM port network CTP ME to a MAC bridge service profile ME. (default)
multicast link-mac-bridge disable		Disables the connections between the multicast GEM port network CTP ME to the MAC bridge service profile.

11.4.3.5 ANI Port Configuration

To enable/disable a connection between MAC bridge service profile and a mapper ID, use the following command.

Command	Mode	Description
ani mapper *MAPPER_ID*	Traffic-Bridge	Connects a MAC bridge service profile with a mapper ID. MAPPER_ID: 1 to 32, IEEE802.1p mapper ID
no ani mapper *MAPPER_ID*		Disconnects a mapper ID from the MAC bridge service profile.

To enable/disable a connection between MAC bridge service profile and the GEM Port ID Network TCP, use the following command.

Command	Mode	Description
ani gem *GEM_NUM*	Traffic-Bridge	Connects a MAC bridge service profile with a GEM Port ID. GEM_NUM: GEM port ID (1 to 32)
no ani gem *GEM_NUM*		Disconnects a GEM Port ID from the MAC bridge service profile.

If there are more than one mapper connected to a MAC bridge service profile, you need to configure a VLAN tagging filtering for VLAN ID-based traffic forwarding. To enable/disable VLAN tagging filtering function on ANI interface, use the following command.

Command	Mode	Description
vlan-filter [**vid** <1-4094>] **untagged** {**allow** | **discard**}	Traffic Bridge-ANI	Enables a VLAN tagging filtering function of ANI-side port. allow: forwards the untagged frames to the ANI-side port discard: blocks the untagged frames to the ANI-side port 1-4094: VLAN ID(s)
vlan-filter vid {**add** | **del**} *VID*		Adds or deletes the VLAN ID on the VLAN list configured by **vlan-filter vid** command above.
no vlan-filter		Disables the VLAN tagging filtering function.

The provides an alternate approach to address filtering from that supported through MAC bridge port filter table data. This alternate approach is useful when all groups of addresses are stored beforehand in the ONU, and it designates which groups are valid or invalid for filtering. On a circuit pack in which all groups of addresses are pre-assigned and stored locally, the ONU creates or deletes an instance of this managed entity automatically upon creation or deletion of a MAC bridge port configuration data ME.

To enable/disable MAC filtering function on ANI interface, use the following command.

Command	Mode	Description

mac-filter {**ip4-mcast** | **ip6-mcast**| **ip4-bcast** | **rarp** | **ipx** | **net-beui** | **apple-talk** | **bridge-manage** | **arp** | **pppoe**}	Traffic Bridge-ANI	Enables the MAC filtering function according to the protocol type for ANI-side bridge port.
no mac-filter {**ip4-mcast** | **ip6-mcast**| **ip4-bcast** | **rarp** | **ipx** | **net-beui** | **apple-talk** | **bridge-manage** | **arp** | **pppoe**}		Disables the MAC filtering function according to the protocol type for ANI-side bridge port.

The following table shows ten attributes that permit the OLT to specify whether MAC address or Ethertypes of the given type are forwarded or filtered. In each case, the initial value of the attribute is 0.

Protocol	MAC Address	Ethertype
IPv4 multicast	01.00.5E.00.00.00 – 01.00.5E.7F.FF.FF	–
IPv6 multicast	33.33.00.00.00.00 –33.33.FF.FF.FF.FF	–
IPv4 broadcast	FF.FF.FF.FF.FF.FF	0x0800
RARP	FF.FF.FF.FF.FF.FF	0x8035
IPX	FF.FF.FF.FF.FF.FF	0x8137
	09.00.1B.FF.FF.FF, 09.00.4E.00.00.02	–
NetBEUI	03.00.00.00.00.01	–
AppleTalk	FF.FF.FF.FF.FF.FF	0x809B, 0x80F3
	09.00.07.00.00.00 – 09.00.07.00.00.FC, 09.00.07.FF.FF.FF	–
Bridge management information	01.80.C2.00.00.00 – 01.80.C2.00.00.FF	–
ARP	FF.FF.FF.FF.FF.FF	0x0806
PPPoE broadcast	FF.FF.FF.FF.FF.FF	0x8863

Tab. 11.2 Protocol Types for MAC Filtering

11.4.3.6 UNI Port Configuration

A UNI-side port is an ONU device port connected to a subscriber. To enable/disable a connection between a MAC bridge service profile and UNI-side port for the downstream traffic, use the following command.

Command	Mode	Description
uni {**eth** | **virtual-eth**} *UNI-PORT*	Traffic Bridge	Connects an UNI port of ONT to a specified MAC bridge service profile. UNI-PORT: UNI port number
no uni {**eth** | **virtual-eth**} *UNI-PORT*		Removes the UNI port of ONT from the MAC bridge service profile.

VLAN Tagging Filtering

To enable/disable VLAN tagging filtering function on the UNI-side port, use the following

command.

Command	Mode	Description
vlan-filter [**vid** <1-4094>] **untagged** {**allow** | **discard**}	Traffic Bridge-UNI	Enables a VLAN tagging filtering function of UNI-side port. allow: forwards the untagged frames to UNI-side port discard: blocks the untagged frames to UNI-side port 1-4094: VLAN ID(s)
vlan-filter vid {**add** | **del**} *VID*		Adds or deletes the VLAN ID on the VLAN list configured by **vlan-filter vid** command above.

VLAN Tagging Operating

To configure a VLAN tagging operation, use the following command.

Command	Mode	Description
vlan-operation us-oper keep	Traffic Bridge-UNI	Sets the policy of VLAN tagging for upstream frame. keep: keeps forwarding the existing tagged/untagged frame
vlan-operation us-oper {**add** | **overwrite**} <1-4094> <0-7>		Sets the policy of VLAN tagging for upstream frame. add: adds a specified VID (double tagging) with tag in case of tagged frame overwrite: replaces an existing tagged/untagged frame to a specified VID with tag. 1-4094: VLAN ID 0-7: CoS value
vlan-operation ds-oper {**keep** | **remove**}		Sets the policy of VLAN tagging for downstream frame. keep: keeps forwarding the incoming tagged frame from OLT to UNI. remove: removes a tag from the incoming tagged packet and forwards it to UNI.
no vlan-operation		Deletes the configured policy for VLAN tagging operation.

Rate Limit

To configure the rate limit for an UNI-side port of ONU, use the following command.

Command	Mode	Description
rate-limit {**upstream** | **downstream**} *PIR_BANDWIDTH SIR_BANDWIDTH*	Traffic Bridge-UNI	Sets the downstream/upstream traffic bandwidth for UNI port. SIR_BANDWIDTH: 0 to 2147483584 (in steps of 64Kbps) PIR_BANDWIDTH: 0 to 2147483584
no rate-limit {**upstream** | **downstream**}		Deletes the configured rate limit.

To apply the configured Rate-limit profile for an UNI-side port of ONU, use the following command.

Command	Mode	Description
rate-limit profile *NAME*	Traffic Bridge-UNI	Applies the configured Rate-limit profile to specified UNI port. NAME: Rate-limit profile name
no rate-limit profile		Removes the Rate-limit profile from connected UNI port.

i For the details of how to create and configure the Rate-limit profile, see 11.12 Rate-limit Profile.

To configure the rate limit for the multicast traffic, use the following command.

Command	Mode	Description
multicast rate-limit <0-1031616>	Traffic Bridge-UNI	Sets the maximum bandwidth of multicast traffic. 0-1031616: maximum bandwidth (in steps of 8kbps, 0 is disable)

Maximum Frame Size

To specify the maximum frame size to be handled by an UNI-side port, use the following command.

Command	Mode	Description
max-frame <64-2036>	Traffic Bridge-UNI	Sets the maximum frame size for an UNI port.
no max-frame		Deletes the configured maximum frame size.

Mapping between Multicast Profile and UNI port

To apply the configured multicast profile to a specified UNI-side port, use the following command.

Command	Mode	Description
multicast-profile *PROFILE*	Traffic Bridge-UNI	Applies the existing multicast profile to a specified UNI port. PROFILE: Multicast profile name
no multicast-profile		Deletes the mapping between a multicast profile and this UNI port.

IGMP Group

To specify the maximum number of IGMP groups, which are correspond to IGMP join message from the UNI-side port, use the following command.

Command	Mode	Description
igmp max-group <0-255>	Traffic Bridge-UNI	Sets the maximum number of IGMP groups for an UNI port.

Activating Administration for UNI

To enable/disable the administration of the ONU (ONT) UNI port, use the following command.

Command	Mode	Description
port-admin {**enable** | **disable**}	Traffic Bridge-UNI	Enables/disables the administration of UNI port.

i To see the admin status of the ONU (ONT) UNI, use **show onu uni-status** command. (See 11.2.25 Displaying ONU Information)

Extended VLAN Tagging Operation Profile Association

To associate the extended VLAN tagging operation profile to the current mode, use the following command.

Command	Mode	Description
extended-vlan-tagging-operation *NAME*	Traffic Bridge-UNI	Associates the extended VLAN tagging operation profile. NAME: profile name
no extended-vlan-tagging-operation		Disassociates the extended VLAN tagging operation profile.

i For the details of how to create and configure the extended VLAN tagging operation profile, see 11.6 Extended VLAN Tagging Operation Profile.

MAC Filtering Function

To configure the MAC filtering function for an UNI-side port of ONU, use the following command.

Command	Mode	Description
mac-filter { **ip4-mcast** | **ip6-mcast** | **ip4-bcast** | **rarp** | **ipx** | **net-beui** | **apple-talk** | **bridge-managed** | **arp** | **pppoe** }	Traffic Bridge-UNI	Enables the MAC filtering function according to the protocol type for UNI-side bridge port.
no mac-filter { **ip4-mcast** | **ip6-mcast** | **ip4-bcast** | **rarp** | **ipx** | **net-beui** | **apple-talk** | **bridge-managed** | **arp** | **pppoe** }		Disables the MAC filtering function according to the protocol type for UNI-side bridge port.

i For the details of how to configure the MAC filtering operation, see 0

ANI Port Configuration.

11.4.3.7 IP-host Service Link

To link an IP-host service to MAC bridge service profile, use the following command.

Command	Mode	Description
link ip-host-config *SERVICE-ID*	Traffic-Bridge	Links an IP-host service to MAC bridge service profile. SERVICE-ID: IP-host service ID (1 to 32)
no link ip-host-config *SERVICE-ID*		Disconnects the linked IP-host service.

i For the details of how to create and configure the IP-host service, see 11.4.5 IP Host Service Configuration.

11.4.3.8 TDM Service Link

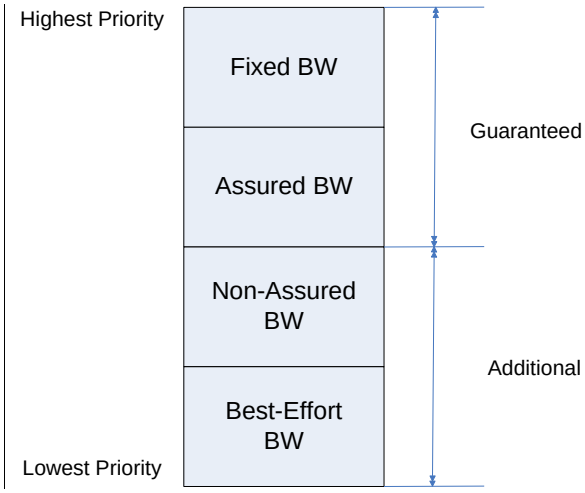
To link a TDM service to MAC bridge service profile, use the following command.

Command	Mode	Description
link tdm-service *SERVICE_ID*	Traffic-Bridge	Links a TDM service to MAC bridge service profile. SERVICE_ID: TDM service ID (1 to 8)
no link tdm-service *SERVICE_ID*		Disconnects the linked TDM service.

i For the details of how to create and configure the TDM service, see 11.4.7 TDM Service Configuration (CES UNI).

11.4.4 T-CONT Mode

Transmission containers (T-CONTs) are used for the management of upstream bandwidth in PON section of the TC layer. T-CONTs dynamically receive grants, identified by Alloc-ID, from the OLT. A single T-CONT can carry GEM traffic with various service classes. It also accommodates one or more physical queues and aggregates them into a single logical buffer so that this feature can be used for enhanced QoS implementation in upstream direction.



T-CONT type	PON Service Class	BW control
Type1	TDM-voice Traffic	Provisioned
Type2	POTS/VoIP	
Type3 & Type 4	V-RT data Best effort data traffic	Dynamic

Fig. 11.6 Priority of T-CONT types

The provides the easy and efficient management solution using T-CONT concept with the Traffic profile.

A GPON port is connected with multiple ONUs/ONTs via splitter. The GPON encapsulation mode (GEM) frames are transmitted between the OLT and the ONUs (ONTs). A GEM frame is identified by a GEM port ID. In the upstream direction, the T-CONTs carry the data stream.

The Traffic profile is a collection of configurations about dynamic bandwidth allocation and GEM port according to the service priority levels. You can configure each T-CONT to have a priority value using GEM port number.

You need to open *Traffic Profile Configuration* mode to configure a T-CONT. A T-CONT ID can include multiple T-CONTs and supports up to 8 priority queues per T-CONT.

To create a T-CONT ID in *Traffic Profile Configuration* mode, use the following command.

Command	Mode	Description
tcont *TCONT-ID*	Traffic-Profile	Creates a T-CONT ID. TCONT-ID: T-CONT ID (1 to 32)

After opening *T-CONT Configuration* mode, the prompt changes from SWITCH(config-traffic-pf[*NAME*])# to SWITCH(config-traffic-pf[*NAME*]-tcont[*TCONT-ID*])#.

To delete the T-CONT ID, use the following command.

Command	Mode	Description
no tcont *TCONT_ID*	Traffic-Profile	Deletes the configured T-CONT ID.

11.4.4.1 GEM Port Configuration

To specify the GEM ports (priority queue) per T-CONT by mapping between T-CONT and GEM port, use the following command.

Command	Mode	Description
gemport *GEM-PORTS* [**queue** <0-7>]	Traffic-TCONT	Specifies the priority queues of a GEM port. GEM-PORTS: mapper ID/GEM port ID (ex: 1/1= mapper #1:gem port 1, 1/2= mapper#1:gem port 2, 2/1-4=mapper #2:all gem ports)
no gemport *GEM-PORTS*		Deletes the configured mapping between T-CONT and the list of GEM ports.

11.4.4.2 Configuration of Weight on WRR Scheduling

To specify the weight value to queue number on WRR scheduling mode, use the following command.

Command	Mode	Description
queue <1-8> **weight** <1-255>	Traffic-TCONT	Specifies the weight value to queue number on WRR scheduling mode. 1-8: priority queue number (1 : lowest) 1-255: weight value

11.4.4.3 DBA Profile Association

You can associate a configured DBA profile with T-CONT by using the following command.

Command	Mode	Description
dba-profile *NAME*	Traffic-TCONT	Associates a configured DBA profile with T-CONT. NAME: DBA profile name

i For the details of how to create and configure a DBA profile, see 11.5 DBA Profile.

11.4.4.4 Displaying T-CONT Information

To display the information of T-CONT, use the following command.

Command	Mode	Description
show tcont-id *OLT-ID* [*ONU-ID*]	Enable Global GPON	Shows the information of T-CONT ID of OLT.
show onu tcont *OLT-ID*		
show tcont [*ONU-ID*]	GPON-OLT	Shows the information of T-CONT allocation for ONU.
show onu detail-info [*ONU-ID*]		Shows the detailed information (status, serial number, T-CONT number, T-CONT queue number) of ONU.
show current-profile	All modes of Traffic-profile	Shows the information currently configured for the profile.

11.4.5 IP Host Service Configuration

In order to configure an IP host, you need to create an IP host service ID. To create the IP host service ID and enter the configuration mode for the host, use the following command.

Command	Mode	Description
ip-host-config *SERVICE-ID*	Traffic-Profile	Creates the IP host service ID and enters the configuration mode for the host. SERVICE-ID : IP host number (1 to 32)
no ip-host-config *SERVICE-ID*		Deletes the created IP host service ID.

After opening *IP-host Configuration* mode, the prompt changes from SWITCH(config-traffic-pf[*NAME*])# to SWITCH(config-traffic-pf[*NAME*]-iphost[*ID*])#.

11.4.5.1 IP Address

To specify the IP address assignment on the host, use the following command.

Command	Mode	Description
ip address {**static** | **dhcp**}	Traffic-IP-host	Specifies the IP address assignment on the host.

11.4.5.2 DNS

To specify the DNS address assignment on the host, use the following command.

Command	Mode	Description
dns primary *A.B.C.D* [**secondary** *A.B.C.D*]	Traffic-IP-host	Specifies the primary/secondary DNS IP address on the host.

ipv6 dns primary *X:X::X:X* [**secondary** *X:X::X:X*]		Specifies the primary/secondary DNS IPv6 address on the host.
no dns		Deletes the configured DNS IP address.
no ipv6 dns		Deletes the configured DNS IPv6 address.

11.4.5.3 VLAN Tagging Operating

To configure a VLAN tagging operation on the host, use the following command.

Command	Mode	Description
vlan-operation us-oper keep	Traffic-IP-host	Sets the policy of VLAN tagging for upstream frame. keep: keeps forwarding the existing tagged/untagged frame
vlan-operation us-oper {**add** | **overwrite**} *VLAN* <0-7>		Sets the policy of VLAN tagging for upstream frame. add: adds a specified VID (double tagging) with tag in case of tagged frame overwrite: replaces an existing tagged/untagged frame to a specified VID with tag. VLAN: VLAN ID (1-4094) 0-7: CoS value
vlan-operation ds-oper {**keep** | **remove**}		Sets the policy of VLAN tagging for downstream frame. keep: keeps forwarding the incoming tagged frame from OLT to UNI. remove: removes a tag from the incoming tagged packet and forwards it to UNI.
no vlan-operation		Deletes the configured policy for VLAN tagging operation.

11.4.5.4 VLAN Tagging Filtering

If there are more than one mapper connected to VLAN tagging, you need to configure a VLAN tagging filtering for VLAN ID-based traffic forwarding. To enable/disable VLAN tagging filtering function on ANI interface, use the following command.

Command	Mode	Description
vlan-filter [**vid** <1-4094>] **untagged** {**allow** | **discard**}	Traffic-IP-host	Enables a VLAN tagging filtering function of ANI-side port. allow: forwards the untagged frames to the ANI-side port discard: blocks the untagged frames to the ANI-side port 1-4094: VLAN ID(s)
vlan-filter vid {**add** | **del**} *VID*		Adds or deletes the VLAN ID on the VLAN list configured by **vlan-filter vid** command above.
no vlan-filter		Disables the VLAN tagging filtering function.

11.4.5.5 IPv6 Configuration

To configure the IPv6 DHCP client mode, use the following command.

Command	Mode	Description
ipv6 dhcp client na	Traffic-IP-host	Sets the DHCPv6 client mode using non-temporary address.
ipv6 dhcp client stateless		Sets the DHCPv6 client mode using the stateless address.

To control transmission of IPv6 Router Solicitation(RS) messages on the host, use the following command.

Command	Mode	Description
ipv6 suppress-rs	Traffic-IP-host	Disables the sending of RS messages on the IP host.
no ipv6 suppress-rs		Sends RS messages on the IP host.

11.4.5.6 Extended VLAN Tagging Operation Profile Association

To associate the extended VLAN tagging operation profile to the host, use the following command.

Command	Mode	Description
extended-vlan-tagging-operation *NAME*	Traffic-IP-host	Associates the extended VLAN tagging operation profile. NAME: profile name
no extended-vlan-tagging-operation		Disassociates the extended VLAN tagging operation profile.

i For the details of how to create and configure the extended VLAN tagging operation profile, see 11.6 Extended VLAN Tagging Operation Profile.

11.4.5.7 VoIP Service Link

To link the VoIP service to the host, use the following command.

Command	Mode	Description
link voip-service *SERVICE_ID*	Traffic-IP-host	Links the VoIP service to the host. SERVICE_ID: VoIP service ID (1 to 32)
no link voip-service *SERVICE_ID*		Disconnects the linked VoIP service.

i For the details of how to create and configure the VoIP service, see 11.4.6 VoIP Service Configuration (POTS UNI).

11.4.5.8 TDM Service Link

To link the TDM service to the host, use the following command.

Command	Mode	Description
link tdm-service *SERVICE_ID*	Traffic-IP-host	Links the TDM service to the host. SERVICE_ID: TDM service ID (1 to 8)
no link tdm-service *SERVICE_ID*		Disconnects the linked TDM service.

i For the details of how to create and configure the TDM service, see 11.4.7 TDM Service Configuration (CES UNI).

11.4.6 VoIP Service Configuration (POTS UNI)

In order to configure VoIP service, you need to create an VoIP service ID.

To create the VoIP service ID and enter the configuration mode for the service, use the following command.

Command	Mode	Description
voip-service *SERVICE_ID*	Traffic-Profile	Creates the VoIP service ID and enters the configuration mode for the service. SERVICE_ID: 1 to 32, VoIP service number
no voip-service *SERVICE_ID*		Deletes the created VoIP service ID.

After opening *VoIP Service Configuration* mode, the prompt changes from SWITCH(config-traffic-pf[*NAME*])# to SWITCH(config-traffic-pf[*NAME*]-voip[*ID*])#.

11.4.6.1 VoIP Service Management Mode

The provides VoIP management function for the subtended ONUs. There are two VoIP management models: IP-path managed model and OMCI (ONT Management and Control Interface) managed model.

OMCI Managed Model
The full OMCI is used to control the VoIP configurations and OLT can handle these configurations for VoIP clients integrated in the ONT.

IP-path Managed Model
OMCI might still be used either to communicate the URI (FTP/HTTP server) of a configuration file to VoIP client integrated in the ONT, or to configure the VoIP client itself.

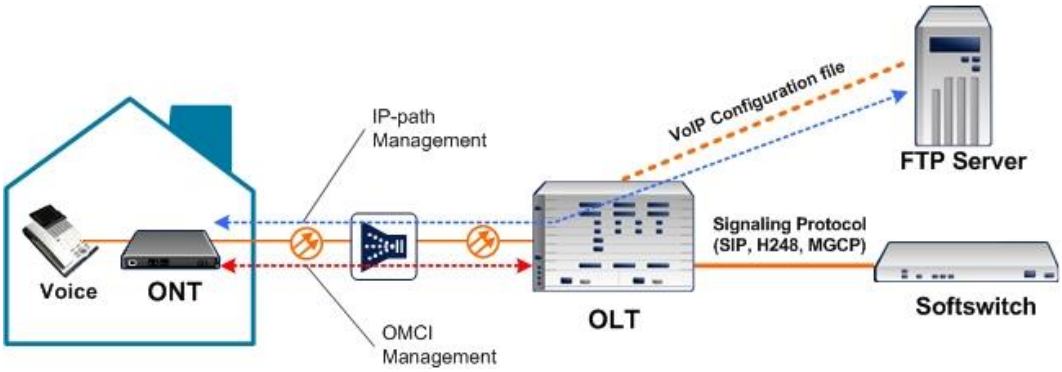


Fig. 11.7 VoIP Service Architecture

The supports the VoIP service management with two modes based on the managed models above.

To configure VoIP service management mode, use the following command.

Command	Mode	Description
manage-method {**omci** | **ip-path**}	Traffic-VoIP	Sets VoIP service management mode. omci: ONT Management and Control Interface ip-path: IP-path managed
no manage-method		Deletes the configured VoIP service management mode.

11.4.6.2 OMCI Managed VoIP

If you configure the VoIP service management mode as OMCI managed by using **voip-profile omci** command, you need to connect VoIP profile with which OLT can handle the configurations for VoIP clients. To connect VoIP profile to the current VoIP service, use the following command.

Command	Mode	Description
voip-profile *NAME*	Traffic-VoIP	Connects VoIP profile to the current VoIP service. NAME: VoIP profile name
no voip-profile		Disconnects the specified VoIP profile.

i You need to create a VoIP profile first to connect the existing VoIP profile to the current VoIP service. For the details of how to create and configure the VoIP profile, see 11.7 VoIP Profile.

11.4.6.3 IP-path Managed VoIP

If you configure the VoIP service management mode as IP-path managed by using **voip-profile ip-path** command, you need to set IP-path configuration in *VoIP IP-path Configuration* mode.

i When you use the **voip-profile ip-path** command, you enter automatically *VoIP IP-path Configuration* mode.

Whenever an ONU is deployed with the IP-path managed VoIP service, the OLT should assign the URL of a VoIP configuration file to communicate with the ONU VoIP client. The provides an authentication method for ONUs to have access to the VoIP configuration server.

To configure IP-path managed VoIP mode, use the following command.

Command	Mode	Description
ip-path uri *URI*	Traffic VoIP-IP-path	Configures a VoIP configuration server. URI: IP-path URI
ip-path auth *NAME* [*PASSWD*]		Sets the user ID and password for IP-path managed model to have access to VoIP configuration server. NAME: user name used for authentication PASSWD: password used for authentication
no ip-path { **uri** | **auth** }		Deletes the configured VoIP configuration server or authentication information.

To specify the protocol on the current VoIP service, use the following command.

Command	Mode	Description
protocol { **h248** | **sip** | **mgcp**}	Traffic VoIP-IP-path	Specifies the protocol on the current VoIP service. sip: Session Initiation Protocol h248, mgcp: Media Gateway Control protocol (= MEGACO)

11.4.6.4 POTS UNI Configuration

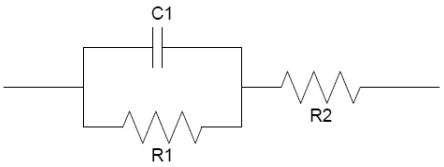
To configure the user network interface, use the following command.

Command	Mode	Description
uni {**pots** | **isdn**} *POTS_NUMBER*	Traffic-VoIP	Configures the VoIP user network interface. pots: POTS (Plain Old Telephone Service) isdn: ISDN (Integrated Services Digital Network) (future release) POTS_NUMBER: POTS port number
no uni {**pots** | **isdn**} *POTS_NUMBER*		Deletes the configuration of UNI.

If you specify UNI as the POTS by using **uni pots** command, you need to perform the configuration for the interface in *VoIP-UNI Configuration* mode as follows:

i When you use the **uni pots** command, you enter automatically *VoIP-UNI Configuration* mode, where you can configure the specified POTS interface.

To specify the impedance for the POTS UNI, use the following command.

Command	Mode	Description
impedance {**600** | **900** | **750** | **820** | **1050**}	Traffic VoIP-UNI	Specifies the impedance for the specified POTS UNI. 600: 600 Ohm (default) 900: 900 Ohm 750: C1=150 nF, R1=750 Ohm, R2=270 Ohm 820: C1=115 nF, R1=820 Ohm, R2=220 Ohm 1050: C1=230 nF, R1=1050 Ohm, R2=320 Ohm 
no impedance		Deletes the configured impedance for the POTS UNI.

To specify the on-hook transmission type, use the following command.

Command	Mode	Description
transmission-path {**full-time** | **part-time**}	Traffic VoIP-UNI	Allows setting the POTS UNI either to full-time on-hook transmission or part-time on-hook transmission. (default: full-time)
no transmission-path		Deletes the configured on-hook transmission type.

To specify Rx/Tx gain value for the receive/transmit signal, use the following command.

Command	Mode	Description
gain rx *VALUE* **tx** *VALUE*	Traffic VoIP-UNI	Specifies Rx/Tx gain value for the receive/transmit signal. VALUE: −120 (–12.0 dB) to 60 (+6.0 dB) (form: two's complement number, default: 0)

To specify POTS holdover time, use the following command.

Command	Mode	Description
pots-holdover-time <0-65535>	Traffic VoIP-UNI	Determines the time during which POTS loop voltage is held up when the ONT is not ranged on the PON. After the specified time elapses, the ONT drops loop voltage, and may thereby cause premises intrusion alarm circuits to go active. When the ONT ranges successfully on the PON, it restores POTS loop voltage immediately and resets the timer to zero. 0-65535: POTS holdover time (unit: second, default: 0(= ONT vendor's factory policy))

11.4.6.5 Protocol Type Configuration

To perform the configuration for protocol type-based service that is offered from an IP host, use the following command.

Command	Mode	Description
udp port *PORT* **tos** *TOS*	Traffic-VoIP	Specifies the port number that offers the UDP/TCP/TLSP/protocol-type service and the value of the TOS field of the IPv4 header. PORT: port number TOS: type of service per IETF RFC 1349 or a differentiated services code point (DSCP) defined by IANA (default: 0)
protocol { **udp** | **tcp** | **tlsp** | *TYPE*} **port** *PORT* **tos** *TOS*		

11.4.7 TDM Service Configuration (CES UNI)

This section describes the configuration of CES UNI in the ONT where the physical path terminates and physical level functions are performed.

In order to configure CES UNI and TDM service, you need to specify the CES port first. To specify the CES port, use the following command.

Command	Mode	Description
ces *PORT*	Traffic-Profile	Specifies the CES port. PORT: CES port number (1 to 8)
no ces *PORT*		Deletes the CES port configuration.

After opening *CES Configuration* mode, the prompt changes from SWITCH(config-traffic-pf[*NAME*])# to SWITCH(config-traffic-pf[*NAME*]-ces[*PORT*])#.

11.4.7.1 Expected Circuit Pack Type

To specify the expected circuit pack type, use the following command.

Command	Mode	Description
expected-type { **auto** | **ds1** | **e1** | **c-ds1-e1** | *VALUE* }	Traffic-CES	Specifies the expected circuit pack type. auto: Autosense ds1: DS1 e1: E1 c-ds1-e1: Configurable DS1/E1 VALUE: 1 to 254 (according to "Table 9.1.5-1 – Circuit pack types" in "ITU-T G.984.4")

11.4.7.2 Framing Structure

To specify the framing structure, use the following command.

Command	Mode	Description
framing { **extend-superframe** | **superframe** | **unframed** | **g-704** | **jt-g-704** | **basic-g-704** | **basic-crc4** | **basic-ts16** | **basic-crc4-ts16** }	Traffic-CES	Specifies the framing structure. (mandatory for DS1 interfaces)

11.4.7.3 Encoding

To specify the line coding scheme, use the following command.

Command	Mode	Description
encoding { **b8zs** | **ami** | **hdb3** | **b3zs** }	Traffic-CES	Specifies the line coding scheme. (mandatory for DS1 and DS3 interfaces) b8zs: B8ZS , ami: AMI hdb3: HDB3 b3zs: B3ZS

11.4.7.4 Line Length

To specify the cable line length with power feed, use the following command.

Command	Mode	Description
line-length power-feed ds1-non-power line-length { **110** | **220** | **330** | **440** | **550** | **660** }	Traffic-CES	Specifies the length of the twisted pair cable from a DS1 physical UNI to the DSX-1 cross-connect point. ds1-non-power: non-power feed type DS1 110~660: line length (unit: ft) (110: 0 to 110, 660: 550 to 660) ds1-power-short: power feed type DS1 (Wet T1), short haul 133~655: line length (unit: ft) (133: 0 to 133, 655: 533 to 655) ds1-power-long: power feed type DS1 (Wet T1), long haul 0/7_5/15/22_5: line length (unit: db) (7_5: 7.5, 22_5: 22.5)
line-length power-feed ds1-power-short line-length { **133** | **266** | **399** | **533** | **655** }		
line-length power-feed ds1-power-long line-length { **0** | **7_5** | **15** | **22_5** }		
line-length power-feed ds3-power line-length { **225** | **450** }		Specifies the length of coaxial cable from a DS3 physical UNI to the DSX-3 cross-connect point. ds3-power: DS3 power feed 225/450: line length (unit: ft) (225: 0 to 225, 450: 226 to 450)
no line-length		Deletes the configured line length.

11.4.7.5 DS1 Mode

To specify the mode of DS1, use the following command.

Command	Mode	Description
ds1-mode connect ds1-cpe line-length { **short** | **long** }	Traffic-CES	Specifies the mode of DS1. ds1-cpe: DS1 CPE (loopback: smart jack) ds1-niu-cpe: DS1 NIU CPE (loopback: intelligent office repeater) short: line length - short haul long: line length - long haul no-power: no power feed with-power: with power feed
ds1-mode connect ds1-niu-cpe power { **no-power** | **with-power** }		
no ds1-mode		Deletes the configured DS1 mode.

11.4.7.6 Line Type

To specify the line type used in DS3 or E3 application, use the following command.

Command	Mode	Description
line-type { **other** | **ds3-m23** | **ds3-syntran** | **ds3-cbit-parity** | **ds3-clear-channel** | **e3-framed** | **e3-plcp** }	Traffic-CES	Specifies the line type used in a DS3 or E3 application. (mandatory for DS3 and E3 interfaces, not applicable to other interfaces)

11.4.7.7 TDM Service Configuration

In order to configure TDM service, you need to create an TDM service ID. To create the TDM service ID and enter the configuration mode for the service, use the following command.

Command	Mode	Description
tdm-service *SERVICE_ID* **mode** { **pw-ip** | **pw-mef8** | **pw-mpls** }	Traffic-CES	Creates a TDM service ID and enters the configuration mode for the service. pw-ip: pseudowire IP transport (UDP/IP) pw-mef8: pseudowire MEF8 pw-mpls: pseudowire MPLS
no tdm-service *SERVICE_ID*		Deletes the created TDM service ID.

After creating a TDM service ID with **pw-ip** option, the prompt changes from SWITCH(config-traffic-pf[*NAME*]-ces[*PORT*])# to SWITCH(config-traffic-pf[*NAME*]-ces[*PORT*]-svc[*ID*]-pw-ip)#. In this mode, you can perform the following configuration.

Applying TDM Pseudowire Profile

In order to configure the TDM service, you need to connect TDM pseudowire profile.
To connect TDM pseudowire profile to the current TDM service, use the following command.

Command	Mode	Description
tdm-pw-profile *NAME*	Traffic CES-PW-IP	Connects TDM pseudowire profile. NAME: TDM pseudowire profile name
no tdm-pw-profile		Disconnects the specified TDM pseudowire profile.

i For the details of how to create and configure the TDM pseudowire profile, see 11.8 TDM Pseudowire Profile.

Far-End URI

To specify the URI of the far-end, use the following command.

Command	Mode	Description
far-end-ip *URI*	Traffic CES-PW-IP	Specifies the URI of the far-end, when the pseudowire service is transported via IP. URI: far-end URI (Both target address and port number should be specified.)
no far-end-ip		Deletes the specified far-end URI.

UDP/TOS Configuration

To perform the configuration for protocol type-based service that is offered from an IP host, use the following command.

Command	Mode	Description
udp port *PORT* **tos** *TOS*	Traffic CES-PW-IP	Specifies the port number that offers the UDP/TCP/TLSP/protocol type service and the value of the TOS field of the IPv4 header. PORT: port number TOS: type of service per IETF RFC 1349 or a differentiated services code point (DSCP) defined by IANA (default: 0)
protocol { **udp** | **tcp** | **tlsp** | *TYPE*} **port** *PORT* **tos** *TOS*		

11.4.7.8 Displaying TDM Pseudowire Information

To display the information of TDM pseudowire profiles, use the following command.

Command	Mode	Description
show tdm-pw-profile [*NAME*]	Global GPON GPON-OLT TDM-PW-Profile	Shows the information of TDM pseudowire profiles. NAME: TDM pseudowire profile name

To display the list information of source MAC addresses for TDM pseudowire of ONU, use the following command.

Command	Mode	Description
show onu tdm-pw source-mac *OLT-ID ONU-ID*	Enable/Global/GPON	Shows the list of source MAC addresses for TDM pseudowire of the specified ONU.
show onu tdm-pw source-mac *ONU-ID*	GPON-OLT	

11.4.8 Management Mode

The OLT manages the ONU through an ONU management and control interface (OMCI) path. An OMCI is a configuration transmission path defined in the GPON standard. If the OLT manages the ONU through a non-OMCI path, this ONU's UNI port is connected as a Virtual Eth and is controlled by its web/TR-69/SNMP management system.

To specify the management mode of ONU's UNI port, use the following command.

Command	Mode	Description
mgmt-mode uni { **eth** | **pots** | **ces** | **video** } *UNI_PORT* { **omci** | **non-omci link virtual-eth** *NUMBER*}	Traffic-Profile	Specifies the management mode of ONU's UNI port using OMCI or non-OMCI path. UNI_PORT: UNI port number (1-32)
no mgmt-mode uni { **eth** | **pots** | **ces** | **video** } *UNI_PORT*		Deletes the specified UNI port's management mode.

To display the configured management mode of ONU, use the following command.

Command	Mode	Description
show onu uni-mgmt *OLT-ID ONU-ID*	Enable/Global/GPON	Shows the management mode of ONU ID.
show onu uni-mgmt *ONU-ID*	GPON-OLT	

11.4.9 Configuring Rate-limit

To configure the rate limit profile, use the following command.

Command	Mode	Description
dot1-rate-limit {**ucast** | **mcast** | **bcast**} **profile** *PROF_NAME*	Traffic-TCONT / Traffic-Bridge	Sets the rate limit profile. ucast: unicast mcast: multicast bcast: broadcast PROF_NAME: profile name
dot1-rate-limit {**ucast** | **mcast** | **bcast**} **upstream** *PIR_VALUE* [*SIR_VALUE*]		Sets the upstream traffic bandwidth. PIR_VALUE: PIR bandwidth range of 0 to 2147483584 SIR_VALUE: SIR bandwidth range of 0 to 2147483584 (in steps of 64Kbps)
no dot1-rate-limit [{**ucast** | **mcast**		Deletes the configured rate limit for downstream traffic.

| **bcast**}]		

11.4.10 Video Return Path Mode

RF return path technology enables the pay-per-view and video-on-demand services that are simply offered over traditional MSO (Multiservice Operator) infrastructure. In order to configure video RF return path service, you need to create a Video return service ID.

A single traffic profile can be used to serve one single video return path service ID.

To create the VoIP service ID and enter the configuration mode for the service, use the following command.

Command	Mode	Description
video-return-path-service *SERVICE_ID*	Traffic-Profile	Creates the VoIP service ID and enters the configuration mode for the service. SERVICE_ID: 1, Video return service number
no video-return-path-service *SERVICE_ID*		Deletes the created VoIP service ID.

After opening *Video Return Path Service Configuration* mode, the prompt changes from SWITCH(config-traffic-pf[*NAME*])# to SWITCH(config-traffic-pf[*NAME*]-vrp[*ID*])#.

To configure the video return path service-related parameters, use the following command.

Command	Mode	Description
frequency *HERTZ*	Traffic-VRP	Specifies the VRP tunner frequency to use. (unit: Hertz)
vrp { **mode1** | **mode2-256k** | **mode2-1m** | **mode2-3m** }		Specifies the format to be used for the VRP service. mode1: SCTE 55-1 (256 kbit/s data rate, 62 byte PDUs, preceded by the unique word 0xCC CC CC 00) mode2-1m: SCTE 55-1 (1.544 Mbit/s data rate, 59 byte PDUs, preceded by the unique word 0xCC CC CC 0D) mode2-256k: SCTE 55-1 (256 kbit/s data rate, 59 byte PDUs, preceded by the unique word 0xCC CC CC 0D) mode2-3m: SCTE 55-1 (3.088 Mbit/s data rate, 59 byte PDUs, preceded by the unique word 0xCC CC CC 0D)
mode1-physical {**default** | **alternate**} { **stage-6** | **stage-7** | **stage-8** | **stage-9** | **stage-10** | **stage-11** | **stage-12** | **stage-13** }		Controls the physical layer configuration to be used in mode 1. default: DQPSK default mode alternate: DQPSK alternate mode stage-6: Randomizer stage 6 preload (Bit 7) stage-7: Randomizer stage 7 preload (Bit 6) stage-8: Randomizer stage 8 preload (Bit 5) stage-9: Randomizer stage 9 preload (Bit 4) stage-10: Randomizer stage 10 preload (Bit 3) stage-11: Randomizer stage 11 preload (Bit 2) stage-12: Randomizer stage 12 preload (Bit 1)

		stage-13: Randomizer stage 13 preload (Bit 0)

11.4.11 Creating a GEM Port Network CTP

The GEM port Network CTP profile manages the upstream traffic identified by the GEM Port-ID. Each GEM port is identified by a port ID uniquely. The port ID ranges from 0 to 32. A GEM port ID is unique per GPON interface and represents a specific traffic or group of flows between the OLT and the ONT. When each GEM port carries the traffic flows, traffic control is performed according to the specific service profile.

To create a GEM port network CTP for a specified traffic profile, use the following command.

Command	Mode	Description
gemport-nctp *GEM_PORT_ID*	Traffic-Profile	Creates a GEM port network CTP profile associated with GEM port ID. GEM_PORT_ID: 1 to 32, GEM port number
no gemport-nctp *GEM_PORT_ID*		Removes the created GEM port Network CTP from the traffic profile

After opening *GEM Port Network CTP Service Configuration* mode, the prompt changes from SWITCH(config-traffic-pf[*NAME*])# to SWITCH(config-traffic-pf[*NAME*]-gem[*ID*])#.

To connect a service profile (MAC bridge, IP Host config, video return path service) with a GEM Port ID, use the following command.

Command	Mode	Description
service {**bridge** | **ip-host** | **video-return-path**} *SVC_ID*	Traffic-GEM	Specifies a service profile to be mapped to the GEM port network CTP for traffic management. bridge: MAC bridge ip-host: IP Host config video-return-path: video return path service SVC_ID: service ID

11.4.12 Saving Traffic Profile

To save the traffic profile after configuring a traffic profile, use the following command.

Command	Mode	Description
apply	Traffic-Profile	Saves a traffic profile configuration.

i Whenever you modify a traffic profile, you should apply the changes again using the **apply** command. If you do not, it will not be applied.

11.4.13 Adding/Applying Traffic Profile

If you want to apply a created traffic profile to an ONU profile, open *ONU Profile Configuration* mode, where you can add the traffic profile.

```
SWITCH(config-traffic-pf[AAA])# apply
SWITCH(config-traffic-pf[AAA])# exit
SWITCH(gpon)# onu-profile BB create
SWITCH(config-onu-profile[BB])# traffic-profile AAA
SWITCH(config-onu-profile[BB])# apply
```

To add/delete the configured traffic profile to a specified ONU profile, use the following command.

Command	Mode	Description
traffic-profile *NAME*	ONU-Profile	Adds the configured traffic profile to ONU profile. NAME: traffic profile name
no traffic-profile		Removes the traffic profile from ONU profile.

i You should modify a traffic profile, you should apply the changes again using the **apply** command. If you do not, it will not be applied.

11.4.14 Displaying Traffic Profile Information

To display the information of traffic profiles, use the following command.

Command	Mode	Description
show traffic-profile [*NAME*]	GPON GPON-OLT Traffic-profile	Shows the currently applied configuration information of traffic profile. NAME: traffic profile name
show current-profile	Current-Profile	Shows the information currently configured for the profile.

To display the information of GEM port ID, use the following command.

Command	Mode	Description
show port-id [*ONU-ID*]	GPON-OLT	Shows the GEM port ID information. ONU-ID: ONU ID (1 to 128)

To display the DBA profile associated with the specific Traffic profile, use the following command.

Command	Mode	Description
show traffic-profile *NAME* **dba-profile**	Enable Global GPON GPON-OLT	Shows the DBA profile associated with the specified Traffic profile. NAME: Traffic profile name

To display the VLAN filter configured on the specific Traffic profile, use the following command.

Command	Mode	Description
show traffic-profile *NAME* **vlan-filter**	Enable Global GPON GPON-OLT	Shows the VLAN filter configured on the specified Traffic profile. NAME: Traffic profile name

11.4.15 Sample Configuration

For the sample configuration, see “Configuration Example 1” in 11.15 Sample Configuration.

11.5 DBA Profile

You need to open *DBA Profile Configuration* mode to set the bandwidth allocation and ONU status reporting mode.

11.5.1 Creating DBA Profile

To create/delete/modify a DBA profile, use the following command.

Command	Mode	Description
dba-profile *PROFILE* **create**	GPON	Creates a DBA profile. PROFILE: DBA profile name
no dba-profile {*PROFILE* | **all**}		Deletes a DBA profile.
dba-profile *PROFILE* **modify**		Modifies the configured DBA profile.

11.5.2 Configuring DBA Profile

If the bandwidth allocation method for ONU upstream transmission is dynamic (DBA), there are two methods of DBA are defined for GPON: status-reporting (SR) DBA, which is based on ONU reports via the dynamic bandwidth report upstream (DBRu) field, and non-status-reporting (NSR) DBA, which is based on OLT monitoring per T-CONT utilization.

To set the bandwidth allocation and ONU status reporting mode of DBA profile, use the following command.

Command	Mode	Description
mode fixed [**cbr**]	DBA Profile	Configure a fixed-UBR bandwidth allocation mode. fixed: fixed-ubr bandwidth (fixed-ubr BW: minimum 512 kbps) cbr: fixed-cbr bandwidth
mode { **nsr** | **sr** }		Configure an ONU status reporting mode of DBA profile. nsr: non status reporting dynamic bandwidth allocation sr: status reporting dynamic bandwidth allocation (fixed-cbr BW: minimum 512 kbps)
sla fixed <0-1031616>		Sets a bandwidth. 0-1031616: fixed bandwidth (unit: 64Kbps) 0-1031616: assured bandwidth (unit: 64Kbps) 128-1031616: maximum bandwidth (unit: 64Kbps) (default option: best-effort (=do not use **non-assured** option))
sla assured <0-1031616>		
sla maximum <128-1031616> [**non-assured**]		

The maximum bandwidth value should be same or more than the sum of a fixed bandwidth and assured bandwidth value.

Maximum B/W ≥ fixed B/W + assured B/W

i If there are a “non-assured” T-CONT and “best-effort” T-CONT, the “non-assured” T-CONT takes precedence over the other one to be allocated the remained bandwidth by OLT.

To delete the configured bandwidth allocation policy of DBA profile, use the following command.

Command	Mode	Description
no sla { **fixed** | **assured** | **maximum**}	DBA-Profile	Deletes the configured bandwidth allocation policy.

11.5.3 Saving DBA Profile

After configuring a DBA profile, you need to save the profile using the following command.

Command	Mode	Description
apply	DBA-Profile	Saves a DBA profile configuration.

i Whenever you modify a DBA profile, you should apply the changes again using the **apply** command. If you do not, it will not be saved with new changes.

i You can apply the flexible bandwidth allocation per T-CONT according to the priority of traffic. After saving the DBA profile and creating T-CONT profile, you should apply the DBA profile on a specified GEM port of T-CONT profile to specify the bandwidth of GEM port by mapping between T-CONT and DBA profile.

11.5.4 Displaying DBA Profile

To display DBA profile information, use the following command.

Command	Mode	Description
show dba-profile [*NAME*]	GPON GPON-OLT DBA-profile Traffic-TCONT	Shows the information of DBA profiles.

11.6 Extended VLAN Tagging Operation Profile

You can configure the ONU's extended VLAN tagging operation. In order to configure the operation, you need to create an extended VLAN tagging operation profile. To create the profile, use the following command.

Command	Mode	Description
extended-vlan-tagging-operation *NAME* **create**	GPON	Creates an extended VLAN tagging operation profile. NAME: profile name
no extended-vlan-tagging-operation {*NAME* | **all**}		Deletes an extended VLAN tagging operation profile.
extended-vlan-tagging-operation *NAME* **modify**		Modifies the configured extended VLAN tagging operation profile.

After opening (creating) *GPON Extended VLAN Operation Configuration* mode, the prompt changes from SWITCH(gpon)# to SWITCH(config-ext-vlan-oper[*NAME*])#.

11.6.1 Received Frame VLAN Tagging Operation Table Configuration

This configuration specifies a table that filters and tags upstream frames. Each entry represents a tagging rule, comprising a filtering part and a treatment part. Each incoming upstream packet is matched against each rule in list order. The first rule that matches the packet is selected as the active rule, and the packet is then treated according to that rule. There are three categories of rules: untag, single-tag, and double-tag rules.

Logically, these categories are separate, and apply to their respective incoming frame types. In other words, a single-tag rule should not apply to a double-tagged frame, even though the single-tag rule might match the outer tag of the double-tagged frame.

Single-tag rules have a filter outer priority field = 15 (indicating no external tag), untag rules have both filter priority fields = 15 (indicating no tags), and double-tag rules have both filter priority fields set to a value that is different from 15 (indicating two tags).

Each tagging rule is based on 'remove' and 'add' operation, where up to two tags can be removed or added. A modify operation is applied by the combination of 'remove' and 'add'.

Note that when a single tag is added, the treatments use the 'inner tag' data-fields for definiteness – this is true even for treatments where a single tag is added to a frame that already has a tag, i.e., added as a second tag. The 'outer tag' data-fields are used only when two tags are added by the same rule.

The terms 'inner' and 'outer' only have meaning with respect to the tags that are being filtered or added.

One set operation can add, modify or delete one entry. The first 8 bytes of each entry are guaranteed to be unique, and are used to identify table entries. The OLT deletes a table entry by setting its last eight bytes to all 0xFF.

When the table is created, the ONT should predefine three entries that list the default treatment (of normal forwarding) for untagged, single-tagged, and double-tagged frames. As an exception to the rule on ordered processing, these default rules are always

considered as a last resort for frames that do not match any other applicable rule. Best practice dictates that these entries not be deleted; however, they can be modified to produce the desired default behaviour.

15, x, x, 15, x, x, x, (0, 15, x, x, 15, x, x)
15, x, x, 14, x, x, x, (0, 15, x, x, 15, x, x)
14, x, x, 14, x, x, x, (0, 15, x, x, 15, x, x)

The ‘x’ is a "do not care" field and should be set to zero.

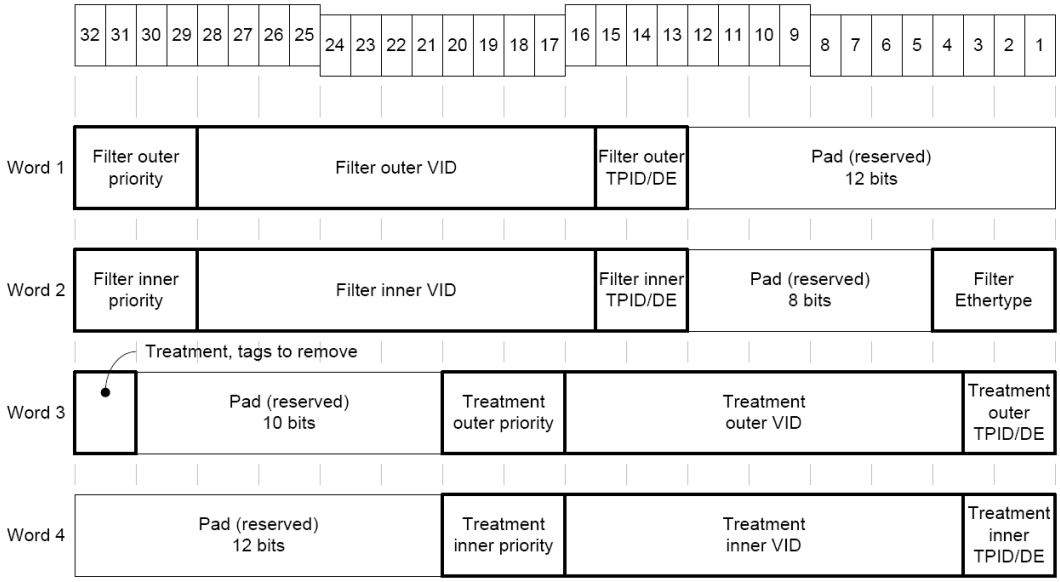


Fig. 11.8 Received Frame Layout

11.6.1.1 Configuration for Single-tagged Frame Treatment

To create the mapping table to configure the single-tagged frame treatment, use the following command.

Command	Mode	Description
single-tagged-frame *TABLE*	GPON-ext-vlan-oper	Creates the mapping table to configure the single-tagged frame treatment. TABLE: table number
no single-tagged-frame *TABLE*		Deletes the specified table.

After opening (creating) the mapping table to configure the single-tagged frame treatment, the prompt changes from SWITCH(config-ext-vlan-oper[*NAME*])# to SWITCH(config-ext-vlan-oper[*NAME*]-single-tagged-frame[*TABLE*])#.

To configure the filtering for single-tagged frames, use the following command.

Command	Mode	Description
filter inner vid {**any** | <0-4094>} **cos** {**any** | <0-7>} **tpid** {**any** | **0x8100** | **input** [**dei** {**0** | **1**}]}	Single-Tagged-Frame	Configures the received single-tagged frames to be filtered by the provided values concerning inner tag. vid any: do not filter on the inner VID. vid 0-4094: filters received frames on this value. cos any: do not filter on the inner priority. cos 0-7: filters received frames on this value. tpid any: do not filter on the inner TPID field. tpid 0x8100: filters received frames on this value. tpid input: input TPID attribute value, don't care about DE bit. tpid input dei 0: input TPID, DE=0 tpid input dei 1: input TPID, DE=1
no filter inner		Deletes the filtering configuration above.

To configure the treatment of filtered single-tagged frames, use the following command.

Command	Mode	Description
treat {**remove** {**single** | **double**} | **discard-frame**}	Single-Tagged-Frame	Configures the treatment of filtered single-tagged frames. remove single: removes one tag (the outer tag is stripped from double-tagged frames.) remove double: removes all of outer and inner tags. discard-frame: drops the frames.
treat inner vid {<0-4094> | **copy-inner** } **cos** {<0-7> | **copy-inner** | **dscp-to-pbit**} **tpid** {**output dei** {**0** | **1** | **copy-inner** } | **copy-inner** | **0x8100**}		Configures the inner tag treatment for filtered single-tagged frames. 0-4094: uses this value as the VID in the inner VLAN tag. copy-inner: copies value from inner tag of received frame. 0-7: uses this value as the priority in the inner VLAN tag.
treat outer vid {<0-4094> | **copy-inner** } **cos** {<0-7> | **copy-inner** | **dscp-to-pbit**} **tpid** {**output dei** {**0** | **1** | **copy-inner** } | **copy-inner** | **0x8100**}		Configures the outer tag treatment for filtered single-tagged frames.
no treat {**remove-discard** | **outer** | **inner**}		Deletes the treatment-related configuration above.

11.6.1.2 Configuration for Double-tagged Frame Treatment

To create the mapping table to configure the double-tagged frame treatment, use the following command.

Command	Mode	Description
double-tagged-frame *TABLE*	GPON-ext-vlan-oper	Creates the mapping table to configure the double-tagged frame treatment. TABLE: table number
no double-tagged-frame *TABLE*		Deletes the specified table.

After opening (creating) the mapping table to configure the double-tagged frame treatment, the prompt changes from SWITCH(config-ext-vlan-oper[*NAME*])# to SWITCH(config-ext-vlan-oper[*NAME*]-double-tagged-frame[*TABLE*])#.

To configure the filtering for double-tagged frames, use the following command.

Command	Mode	Description
filter inner vid {**any** | <0-4094>} **cos** {**any** | <0-7>} **tpid** {**any** | **0x8100** | **input** [**dei** {**0** | **1**}]}	Double-Tagged-Frame	Configures the received double-tagged frames to be filtered by the provided values concerning inner tag. vid any: do not filter on the inner VID. vid 0-4094: filters received frames on this value. cos any: do not filter on the inner priority. cos 0-7: filters received frames on this value. tpid any: do not filter on the inner TPID field. tpid 0x8100: filters received frames on this value. tpid input: input TPID attribute value, don't care about DE bit. tpid input dei 0: input TPID, DE=0 tpid input dei 1: input TPID, DE=1
filter outer vid {**any** | <0-4094>} **cos** {**any** | <0-7>} **tpid** {**any** | **0x8100** | **input** [**dei** {**0** | **1**}]}		Configures the received double-tagged frames to be filtered by the provided values concerning outer tag.
no filter {**inner** | **outer**}		Deletes the filtering configuration above.

To configure the treatment of filtered double-tagged frames, use the following command.

Command	Mode	Description
treat {**remove** {**single** | **double**} | **discard-frame**}	Double-Tagged-Frame	Configures the treatment of filtered double-tagged frames. remove single: removes one tag (the outer tag is stripped from double-tagged frames.) remove double: removes all of outer and inner tags. discard-frame: drops the frames.
treat inner vid {<0-4094> | **copy-inner** | **copy-outer**} **cos** {<0-7> | **copy-inner** | **copy-outer** | **dscp-to-pbit**} **tpid** {**output dei** {**0** | **1** | **copy-inner** | **copy-outer**} | **copy-inner** | **copy-outer** | **0x8100**}		Configures the inner tag treatment for filtered double-tagged frames. 0-4094: uses this value as the VID in the inner VLAN tag. copy-inner: copies value from inner tag of received frame. copy-outer: copies value from outer tag of received frame. 0-7: uses this value as the priority in the inner VLAN tag.
treat outer vid {<0-4094> | **copy-inner** | **copy-outer**} **cos** {<0-7> | **copy-inner** | **copy-outer** | **dscp-to-pbit**} **tpid** {**output dei** {**0** | **1** | **copy-inner** | **copy-outer**} | **copy-inner** | **copy-outer** | **0x8100**}		Configures the outer tag treatment for filtered double-tagged frames.
no treat {**remove-discard** | **outer** | **inner**}		Deletes the treatment-related configuration above.

11.6.1.3 Configuration for Untagged Frame Treatment

To create the mapping table to configure the untagged frame treatment, use the following command.

Command	Mode	Description
untagged-frame *TABLE*	GPON-ext-vlan-oper	Creates the mapping table to configure the untagged frame treatment. TABLE: table number
no untagged-frame *TABLE*		Deletes the specified table.

After opening (creating) the mapping table to configure the untagged frame treatment, the prompt changes from SWITCH(config-ext-vlan-oper[*NAME*])# to SWITCH(config-ext-vlan-oper[*NAME*]-untagged-frame[*TABLE*])#.

To configure the filtering for untagged frames, use the following command.

Command	Mode	Description
filter ether-type {**ipoe** | **pppoe** | **arp** | **ipv6-ipoe**}	Untagged-Frame	Configures the received untagged frames to be filtered by the provided option.
no filter ether-type		Deletes the filtering configuration above.

To configure the treatment of filtered untagged frames, use the following command.

Command	Mode	Description
treat inner vid <0-4094 **cos** {<0-7> | **dscp-to-pbit**} **tpid** {**output dei** {**0** | **1** } | **0x8100**}	Untagged-Frame	Configures the inner tag treatment for filtered untagged frames. 0-4094: uses this value as the VID in the inner VLAN tag. 0-7: uses this value as the priority in the inner VLAN tag.
treat outer vid <0-4094**> cos** {<0-7> | **dscp-to-pbit**} **tpid** {**output dei** {**0** | **1** } | **0x8100**}		Configures the outer tag treatment for filtered untagged frames.
treat discard-frame		Drops the filtered untagged frames.
no treat {**remove-discard** | **outer** | **inner**}		Deletes the treatment-related configuration above.

For untagged frames, queue information need to be specified. You can configure whether they use a default DSCP to CoS mapping table as specifying the queue (assuming that the untagged frames can use the DSCP to CoS mapping table). Unless you configure the table to be used, the untagged frames use default queue information.

To configure to use a default DSCP to CoS mapping table as specifying queue for untagged frames, use the following command.

Command	Mode	Description
dscp-to-cos-map default-map	GPON-ext-vlan-oper	Configures to use a default DSCP to CoS mapping table as specifying queue for untagged frames.
no dscp-to-cos-map		Deletes the configuration above. (= Configures to use default queue information as specifying queue for untagged frames.)

11.6.2 TPID Configuration

To configure the specific TPID value for operations on the input (filtering) side and output (tagging) side of the table, use the following command.

Command	Mode	Description
tpid { **input** *VALUE* | **output** *VALUE* }	GPON-ext-vlan-oper	Configures the specific TPID value for operations on the input (filtering) side and output (tagging) side of the table. VALUE: TPID
no tpid { **input** | **output** }		Deletes the configured TPID value.

11.6.3 Downstream Mode Configuration

Although the extended VLAN tagging operation pertains to upstream traffic, this configuration specifies the mode for downstreaming mapping.

The operation performed in the downstream direction is the inverse of that performed in the upstream direction. For one-to-one VLAN mappings, the inverse is trivially defined. Many-to-one mappings are possible, however, and these are treated as follows. If the many-to-one mapping results from multiple operation rules producing the same ANI-side tag configuration, then the first rule in the list defines the inverse operation. If the many-to-one mapping results from “do not care” fields in the filter being replaced with provisioned fields in the ANI-side tags, then the inverse is defined to set the corresponding fields on the ANI-side with their lowest value.

To enable/disable the extended VLAN tagging operation for the downstream mode, use the following command.

Command	Mode	Description
downstream-mode {**enable** | **disable**}	GPON-ext-vlan-oper	Enables/disables the extended VLAN tagging operation for the downstream mode.

11.6.4 Saving Profile

After configuring an profile, you need to save the profile with the following command.

Command	Mode	Description
apply	GPON-ext-vlan-oper	Saves an profile configuration.

i

Even if you modify a running profile, you also need to use the **apply** command to apply the changes to ONUs (ONTs).

11.6.5 Displaying Extended VLAN Tagging Operation Profile

To display a configured Extended VLAN tagging operation profile, use the following command.

Command	Mode	Description
show running-config extended-vlan-tagging-operation [*NAME*]	All	Shows the configured extended vlan tagging operation profile. NAME: Extended VLAN tagging operation profile name

To display the information of current profile, use the following command.

Command	Mode	Description
show current-profile	Current-Profile	Shows the information currently configured for the profile.

11.7 VoIP Profile

11.7.1 OMCI Management Configuration

The GPON system enables multi-vendor interoperability between OLT and ONT. The OMCI specification addresses the ONT configuration management, fault management and performance management for GPON system operation and for several services including voice services. The OMCI and the configuration server based architecture are the standard alternatives to convey the operation of the ONT for VoIP. In addition, the VoIP user agent at the ONT needs to work in conjunction with a softswitch for voice service features.

You need to open *VoIP Profile Configuration* mode to configure VoIP based on OMCI management. To implement the configurations of VoIP between OLT and ONU, an ONU profile should be included by the configured VoIP profile. You can easily manage the VoIP network parameters of ONUs using the VoIP profile.

i The ONT must be applied by VoIP profile defined in if the ONT has POTS terminations and if OLT is to be used to remotely manage and provide the VoIP service.

11.7.1.1 Creating VoIP Profile

To create a VoIP profile, use the following command.

Command	Mode	Description
voip-profile *NAME* **create**	GPON	Creates a VoIP profile. NAME: VoIP profile name

After opening *VoIP Profile Configuration* mode, the prompt changes from SWITCH(gpon)# to SWITCH(config-voip-profile[*NAME*])#.

To delete an existing VoIP profile, use the following command.

Command	Mode	Description
no voip-profile *NAME*	GPON	Deletes n VoIP profile. NAME: VoIP profile name

To modify an existing VoIP profile, use the following command.

Command	Mode	Description
voip-profile *NAME* **modify**	GPON	Modifies the exisitng VoIP profile. NAME: VoIP profile name

11.7.1.2 VoIP Media Configuration

To specify fax mode, use the following command.

Command	Mode	Description
fax-mode {**passthru** | **t-38**}	VoIP-Profile	Specifies fax mode.

To configure codec negotiation with codec type, packet period and silence suppression, use the following command.

Command	Mode	Description
codec-nego <1-4> **codec** {**pcmu** | **gsm** | **g723** | **dvi4-8k** | **dvi4-16k** | **lpc** | **pcma** | **g722** | **l16-2ch** | **l16-1ch** | **qcelp** | **cn** | **mpa** | **g728** | **dvi4-11k** | **dvi4-22k** | **g729**} **packet-period** *VALUE* **silence-suppression** *VALUE*	VoIP-Profile	Configures codec negotiation by specifying codec, packet period and silence suppression. 1-4: codec negotiation number pcmu ~ g729: codecs as defined by IETF RFC 3551 (default: pcmu) VALUE: 10~30, packet period (unit: ms, default: 10) VALUE: 0~1, whether silence suppression is on or off (0 = off, 1 = on)

To specify out-of-band DTMF carriage, use the following command.

Command	Mode	Description
oob-dtmf {**enable** | **disable**}	VoIP-Profile	Specifies out-of-band DTMF carriage. When enabled, DTMF signals are carried out of band via RTP or the associated signalling protocol. When disabled, DTMF tones are carried in the PCM stream.

11.7.1.3 Voice Service Configuration

To configure the announcement type, use the following command.

Command	Mode	Description
announcement-type { **silence** | **reorder-tone** | **fast-busy** | **voice-announcement** }	VoIP-Profile	Specifies the treatment when a subscriber goes off hook but does not attempt a call.

To configure the target value of jitter buffer, use the following command.

Command	Mode	Description
jitter-target *VALUE*	VoIP-Profile	Specifies the target value of jitter buffer. The system tries to maintain the jitter buffer at the target value. VALUE: 0-65535, target value of jitter buffer, the value 0 specifies dynamic jitter buffer sizing. (unit: ms)
no jitter-target		Deletes the configured target value of jitter buffer.

To configure the maximum depth of the jitter buffer, use the following command.

Command	Mode	Description
jitter-buffer-max *VALUE*	VoIP-Profile	Specifies the maximum depth of the jitter buffer associated with this service. VALUE: 0-65535, maximum depth of jitter buffer (unit: ms)
no jitter-buffer-max		Deletes the configured maximum depth of the jitter buffer.

To configure echo cancellation, use the following command.

Command	Mode	Description
echo-cancel {**true** | **false**}	VoIP-Profile	Specifies whether echo cancellation is on or off. (true = on, false = off)

To configure the variant of POTS signalling used on the associated UNIs, use the following command.

Command	Mode	Description
pstn-protocol-variant *E164_COUNTRY_CODE*	VoIP-Profile	Controls which variant of POTS signalling is used on the associated UNIs. Its value is equal to the E.164 country code. E164_COUNTRY_CODE: 0-65535
no pstn-protocol-variant		Deletes the configured E.164 country code.

11.7.1.4 RTP Configuration

To configure the RTP port used for voice traffic, use the following command.

Command	Mode	Description
rtp-local-port min *VALUE* {**max** *VALUE* }	VoIP-Profile	Defines the base and highest RTP port that should be used for voice traffic. VALUE: 0-65535, the base RTP port (default: 50000) VALUE: 0-65535, the highest RTP port

To configure Diffserv code point to be used for outgoing RTP packets, use the following command.

Command	Mode	Description
rtp-dscp-mark *VALUE*	VoIP-Profile	Specifies Diffserv code point to be used for outgoing RTP packets for this profile. VALUE: 0-255, Diffserv code point for outgoing RTP packets

To enable/disable RTP piggyback events, use the following command.

Command	Mode	Description
rtp-piggyback-event {**enable** | **disable**}	VoIP-Profile	Enables/disables RTP piggyback events. (default: disable)

To enable/disable handling of tones via RTP tone events, use the following command.

Command	Mode	Description
rtp-tone-event {**enable** | **disable**}	VoIP-Profile	Enables/disables handling of tones via RTP tone events per IETF RFC4733 and IETF RFC4734. (default: disable)

To enable/disable handling of DTMF via RTP DTMF events, use the following command.

Command	Mode	Description
rtp-dtmf-event {**enable** | **disable**}	VoIP-Profile	Enables/disables handling of DTMF via RTP DTMF events per IETF RFC4733 and IETF RFC 4734. (default: disable) This configuration is ignored unless out-of-band DTMF in the VoIP media configuration is enabled. (For out-of-band DTMF, see **oob-dtmf** command in 11.7.4 Saving VoIP Profile.)

To enable/disable handling of CAS via RTP CAS events, use the following command.

Command	Mode	Description
rtp-cas-event {**enable** | **disable**}	VoIP-Profile	Enables/disables handling of CAS via RTP CAS events per IETF RFC4733 and IETF RFC4734. (default: disable)

11.7.1.5 Signalling Code

To specify the POTS-side signalling, use the following command.

Command	Mode	Description
signaling-code {**loop-start** | **ground-start** | **loop-reverse-battery** | **coin-first** | **dial-tone-first** | **multi-party** }	VoIP-Profile	Specifies the POTS-side signalling.

11.7.1.6 DTMF Digit Configuration

To configure DTMF digit power levels, use the following command.

Command	Mode	Description
dtmf-digit levels *VALUE*	VoIP-Profile	Specifies the power level of DTMF digits that may be generated by the ONT toward the subscriber set. It is a 2s complement value referred to 1mW at the 0TLP (dBm0), with resolution 1dB. VALUE: DTMF digit power level
no dtmf-digit levels		Deletes the configured DTMF digit power levels.

To configure DTMF digit duration, use the following command.

Command	Mode	Description
dtmf-digit duration *VALUE*	VoIP-Profile	Specifies the duration of DTMF digits that may be generated by the ONT toward the subscriber set. VALUE: DTMF digit duration (unit: ms)
no dtmf-digit duration		Deletes the configured DTMF digit duration.

11.7.1.7 Hook Flash Time Configuration

To configure hook flash time, use the following command.

Command	Mode	Description
hook-flash-time {**max** | **min**} *VALUE*	VoIP-Profile	Defines the maximum or minimum duration recognized by the ONT as a switchhook flash. VALUE: maximum or minimum hook flash time (unit: ms)
no hook-flash-time {**max** | **min**}		Deletes the configured hook flash time.

11.7.1.8 VoIP Extended Operation Configuration

To configure the special line service, use the following command.

Command	Mode	Description
special-line-service disable	VoIP-Profile	Disables the special line service.
special-line-service hot-line *NUMBER*		Enables the hot-line feature that it immediately dials a pre-configured number as soon as the handset goes off hook.
special-line-service warm-line timeout <1-30> *NUMBER*		Enables the warm-line feature that it dials a pre-configured number if no digits were entered before the specified timer value expired when the handset went off hook. 1-30: warm-line timeout value (unit: seconds)

When a three-way call is established, the audio mixing can be perfomed by media server or client (ONT). With the media server, audio mixing is performed for all active calls at the server and it sends the audio stream using one audio channel to the client. In case of client, it mixes audio locally and thus achieves three-way calling without assistance from the media server.

To handle the three-way call audio mixing by server or client, use the following command.

Command	Mode	Description
three-way-ssw-mixing server	VoIP-Profile	Enables the server to control the transfer and perform audio mixing for the three-way call conferencing.
three-way-ssw-mixing client		Enables the client (ONT) to control the transfer and perform audio mixing for the three-way call conferencing.

To display the configure paramters for VoIP extended opration, use the following command.

Command	Mode	Description
show onu voip voip-ext-oper *OLT-ID ONU-ID*	Enable Global GPON	Shows the VoIP extended operation parameters. ONU-ID: 1-128 or ONU serial number
show onu voip voip-ext-oper *ONU-ID*	GPON-OLT	

11.7.2 OMCI-based SIP Configuration

If the ONUs are fully provisioned and managed from the using OMCI, you can configure POTS interface, call features and SIP agents of these ONUs.

You need to enter SIP mode to perform the SIP-related detail configuration such as VoIP application service, SIP agent, etc. To enter the SIP mode, use the following command.

Command	Mode	Description
protocol sip	VoIP-Profile	Enters the SIP mode.

11.7.2.1 SIP Agent Configuration

This defines the configuration necessary to establish communication for signalling between the SIP user agent and SIP servers.

To specify an SIP proxy server, use the following command.

Command	Mode	Description
proxy-server *ADDRESS*	VoIP-SIP	Configures IP address or URI of SIP proxy server for SIP signalling messages.

		ADDRESS: SIP proxy server IP address or URI
no proxy-server		Deletes the configured address of SIP proxy server.

To specify an outbound SIP proxy server, use the following command.

Command	Mode	Description
outbound-proxy-server *ADDRESS*	VoIP-SIP	Configures IP address or URI of outbound SIP proxy server for SIP signalling messages. ADDRESS: outbound SIP proxy server IP address or URI
no outbound-proxy-server		Deletes the configured address of outbound SIP proxy server.

To specify an SIP DNS, use the following command.

Command	Mode	Description
dns primary *A.B.C.D* [**secondary** *A.B.C.D*]	VoIP-SIP	Specifies the primary/secondary SIP DNS IP address. A.B.C.D: primary/secondary DNS server address (default: 0 (= no primary/secondary SIP DNS is defined))
no dns		Deletes the configured address of SIP DNS server.

To specify a register server, use the following command.

Command	Mode	Description
register-server *ADDRESS*	VoIP-SIP	Specifies the register server IP address or resolved name. ADDRESS: register server address
no register-server		Deletes the configured address of register server.

To identify an SIP gateway softswitch vendor, use the following command.

Command	Mode	Description
soft-switch *NAME*	VoIP-SIP	Identifies the SIP gateway softswitch vendor. NAME: vendor name
no soft-switch		Deletes the configured SIP gateway softswitch vendor name.

i The format of vendor name is four ASCII coded alphabetic characters (A..Z) as defined in ATIS-0322000. A value of four null characters indicates no particular vendor.

To configure the SIP registration expiration time, use the following command.

Command	Mode	Description
reg-exp-time <0-65535>	VoIP-SIP	Specifies the SIP registration expiration time. If the value is 0, the SIP agent does not add an expiration time to the registration requests and does not perform re-registration.

		0-65535: SIP registration expiration time (unit: second, default: 3600)

To configure the SIP re-registration head start time, use the following command.

Command	Mode	Description
rereg-head-start-time <0-65535>	VoIP-SIP	Specifies the time prior to timeout that causes the SIP agent to start the re-registration process. (unit: second, default: 360)

To specify a host part , use the following command.

Command	Mode	Description
host-part-server *URI*	VoIP-SIP	Specifies the host or domain part of the SIP address of record for users connected to the ONT. URI: host part URI
no host-part-server		Deletes the configured host part URI.

To enable/disable ONT to transmit SIP options, use the following command.

Command	Mode	Description
sip-option-transmit-control {**enable** | **disable**}	VoIP-SIP	Enables/disables ONT to transmit SIP options. (default: disable)
no sip-option-transmit-control		Sets no transmit-control value.

To configure the URI format in outgoing SIP messages, use the following command.

Command	Mode	Description
sip-uri-format {**tel-uri** | **sip-uri**}	VoIP-SIP	Specifies the format of the URI in outgoing SIP messages. (default: TEL URI)
no sip-uri-format		Deletes the configured format of URI in outgoing SIP messages.

11.7.2.2 SIP Detailed Feature Operation

If you specify the SIP server doamin, SIP server supports DNS for resolving the IP address of a proxy required to send a SIP message. This information is stored in DNS cache to prevent sending every DNS Query packets.

To set a SIP stack DNS cache update policy, use the following command.

Command	Mode	Description
dns-cache-policy ttl	VoIP-SIP	Specifies the expired time of DNS cache by TTL value in DNS response message. ttl: SIP stack DNS Cache is updated by TTL Value
dns-cache-policy permanent		Retains the DNS resolved IP address without the

		expired time of DNS cache. permanent: SIP Stack DNS Cache is updated when VoIP configurations are changed

SIP timers define the transaction expiration timers, retransmission intervals when UDP is used as a transport, and the lifetime of dynamic TCP connection. The retransmission and expiration timers correspond to the timers defined in RFC 3261.

To specify various timers that SIP uses, use the following command.

Command	Mode	Description
sip-timer t1 <0-2500> **t2** <0-5000> **td** <5000-65535>	VoIP-SIP	Specifies the SIP timers. t1: Round-trip time (RTT) estimate (default: 500 ms) t2: maximum retransmission interval for non-INVITE requests and INVITE responses td: wait time for response retransmissions

The supports SIP session timer which allows a periodic refreshing of SIP sessions using the register message to prevent the termination of SIP session. When using NAT with SIP service, NAT terminates the SIP session in case there is no SIP message transmission for a certain time period. To specify a session timeout to maintain the connection of SIP session, use the following command.

Command	Mode	Description
session-timer timeout <1-65535>	VoIP-SIP	Defines the time for waiting to maintain the connection of SIP session by force.
no session-timer		Deletes the configured SIP session timer.

When the user dials digits that do not match the digit map, it's possible to keep dialing by pressing "#" button. It is called the end-of-digit. To enable/disable the use of an end-of-digit, use the following command.

Command	Mode	Description
end-of-digit {**enable** | **disable**}	VoIP-SIP	Enables/disables the use of an end-of-digit.
end-sharp-token {**hex** | **ascii**}		Translates the characters to the hexadecimal value or ASCII character code and sends them. For example, the hash (#) symbol has a hexadecimal value of 0x23, so it is encoded as %23.

To display the parameters of SIP detailed feature operation, use the following command.

Command	Mode	Description
show onu voip sip-detail-oper *OLT-ID ONU-ID*	Enable Global GPON	Shows the configured parameters of SIP detailed feature operation. ONU-ID: 1-128 or ONU serial number

show onu voip sip-detail-oper *ONU-ID*	GPON-OLT	

11.7.2.3 VoIP Application Service

The configuration of VoIP application service defines the attributes of calling features used in conjunction with a VoIP line service, such as CID, call waiting, call transfer, call presentation, direct connect, and etc. To configure the CID features, use the following command.

Command	Mode	Description
caller-id {**call-number** | **call-name** | **cid-blocking** | **cid-number** | **cid-name** | **acr**}	VoIP-SIP	Enables each feature for caller ID. (default: disabled) call-number: calling number call-name: calling name cid-blocking: CID blocking (both number and name) cid-number: permanent presentation status for number cid-name: permanent presentation status for name acr: anonymous CID blocking. It may not be possible to support this feature in the ONT.
no caller-id		Disables all the features for caller ID.

To configure the call waiting features, use the following command.

Command	Mode	Description
call-waiting {**call-wait** | **cid-announce**}	VoIP-SIP	Enables each feature for call waiting. (default: disabled) call-wait: call waiting cid-announce: caller ID announcement
no call-waiting		Disables the call waiting feature.

To configure the call processing (transfer) features, use the following command.

Command	Mode	Description
call-progress-transfer {**3way** | **call-transfer** | **call-hold** | **call-park** | **not-disturb** | **flash-emerg-call** | **emerg-originating-hold** | **6way**}	VoIP-SIP	Enables each feature for call processing. (default: disabled) 3way: 3way call call-transfer: call transfer call-hold: call hold call-park: call park not-disturb: do not disturb flash-emerg-call: flash on emergency service call (flash is to be processed during an emergency service call) emerg-originating-hold: emergency service originating hold (determines whether call clearing is to be performed on on-hook during an emergency service call) 6way: 6way call

no call-progress-transfer		Disables all the features for call processing.

To configure the call presentation features, use the following command.

Command	Mode	Description
call-present {**splash-ring** | **dial-tone** | **visual-indicate** | **call-forward**}	VoIP-SIP	Enables each feature for call presentation. (default: disabled) splash-ring: message waiting indication splash ring dial-tone: message waiting indication special dial tone visual-indicate: message waiting indication visual indication call-forward: call forwarding indication
no call-present		Disables all the features for call presentation.

To configure the direct connect feature, use the following command.

Command	Mode	Description
direct-connect enable	VoIP-SIP	Enables the direct connect feature. (default: disabled)
direct-connect delay-option		Enables the dial tone feature delay option.
direct-connect disable		Disables the direct connect feature.

To specify a direct connect target, use the following command.

Command	Mode	Description
direct-connect-uri *URI*	VoIP-SIP	Configures the URI of direct connect. URI: direct connect URI
no direct-connect-uri		Deletes the configured URI of direct connect.

To specify a bridged line agent, use the following command.

Command	Mode	Description
bridged-line-agent-uri *URI*	VoIP-SIP	Configures the URI of bridged line agent. URI: bridged line agent URI
no bridged-line-agent-uri		Deletes the configured URI of bridged line agent.

To specify a conference factory, use the following command.

Command	Mode	Description
conference-factory-uri *URI*	VoIP-SIP	Configures the URI of conference factory. URI: conference factory URI
no conference-factory-uri		Deletes the configured URI of conference factory.

11.7.2.4 VoIP Feature Access Codes

The configuration of VoIP feature access codes defines administrable feature access codes for the VoIP subscriber.

To configure VoIP feature access codes, use the following command.

Command	Mode	Description
feature cancel-call-wait *VALUE*	VoIP-SIP	Specifies the access code for each feature. VALUE: a string of characters from the set (0..9, *, #) with trailing nulls in any unused bytes
feature call-hold *VALUE*		
feature call-park *VALUE*		
feature caller-id-act *VALUE*		
feature caller-id-deact *VALUE*		
feature do-not-disturb-act *VALUE*		
feature do-not-disturb-deact *VALUE*		
feature do-not-disturb-pin-change *VALUE*		
feature emerg-service-number *VALUE*		
feature intercom-service *VALUE*		
no feature cancel-call-wait		Deletes the specified access code for each feature.
no feature call-hold		
no feature call-park		
no feature caller-id-act		
no feature caller-id-deact		
no feature do-not-disturb-act		
no feature do-not-disturb-deact		
no feature do-not-disturb-pin-change		
no feature emerg-service-number		
no feature intercom-service		

11.7.2.5 SIP User Data

The configuration of SIP user data defines the user-specific attributes associated with a specific VoIP CTP.

To specify an SIP voicemail server, use the following command.

Command	Mode	Description
voicemail-server-uri *ADDRESS*	VoIP-SIP	Configures IP address or URI of SIP voicemail server. ADDRESS: voicemail server IP address or URI

To specify the voicemail subscription expiration time, use the following command.

Command	Mode	Description
voicemail-subscript-expire-time *VALUE*	VoIP-SIP	Defines the voicemail subscription expiration time. If this value is 0, the SIP agent uses an implementation-specific value. (unit: second, default: 3600)

To configure a release timer, use the following command.

Command	Mode	Description
release-timer <0-255>	VoIP-SIP	Configures a release timer. The value 0 specifies that the ONT is to use its internal default. (unit: second, default: 10)

To configure a ROH timer, use the following command.

Command	Mode	Description
roh-timer <0-255>	VoIP-SIP	Defines the time for the receiver off hook condition before ROH tone is applied. The value 0 disables ROH timing. (unit: second, default: 15)

11.7.2.6 Network Dial Plan

To configure the critical dial timeout, use the following command.

Command	Mode	Description
dial-plan crit-timeout *TIMEOUT*	VoIP-SIP	Defines the critical dial timeout for digit map processing. TIMEOUT: critical dial timeout (unit: ms, default: 4000)

To configure the partial dial timeout, use the following command.

Command	Mode	Description
dial-plan part-timeout *TIMEOUT*	VoIP-SIP	Defines the partial dial timeout for digit map processing. TIMEOUT: partial dial timeout (unit: ms, default: 16000)

To configure the dial plan format, use the following command.

Command	Mode	Description
dial-plan format {**h248** | **nsc** | **vendor**}	VoIP-SIP	Defines the dial plan format standard that is supported in the ONT for VoIP. h248: H.248 format with specific plan (table entries define the dialling plan) nsc: NSC format vendor: vendor-specific format

To configure the dial plan table, use the following command.

Command	Mode	Description
dial-plan table *TABLE_ID TABLE_TOKEN*	VoIP-SIP	Adds a dial plan with the configured token. TABLE_ID: A unique identifier of a dial plan within the dial plan table

		TABLE_TOKEN: the token used by the VoIP service to process dial plans (This ASCII string is typically delimited by ":".)
no dial-plan table *TABLE_ID*		Deletes the created dial plan table.

i The dial plan created by **dial-plan table** command can be applied only if you configure the dial plan format as H.248 by using **dial-plan format h248** command.

i In order to see the configured dial plan, use **show voip-profile** command.

11.7.3 OMCI-based MGC Configuration

MGCP (Media Gateway Control Protocol) is a signalling and call control protocol used within VoIP systems that typically interoperate with the public switched telephone network (PSTN).

If the ONUs are fully provisioned and managed from the using OMCI, you can configure the MGC-related settings of these ONUs. The MGC entity defines the media gateway controller configuration associated with an MG subscriber. It is conditionally required for ONUs (ONTs) that support MGCP (H.248, Megaco) VoIP service.

You need to enter MGC mode to perform the MGC-related detail configuration. To enter the MGC mode, use the following command.

Command	Mode	Description
protocol {**mgcp** | **h248**}	VoIP-Profile	Enters the MGC mode.

To configure the IP address of primary and secondary MGC server that controls the signalling messages, use the following command.

Command	Mode	Description
mgc {**primary** | **secondary**} *A.B.C.D*	VoIP-MGC	Configures the IP address of primary and secondary MGC server.
no mgc {**primary** | **secondary**}		Deletes the configured IP address.

To configure the version of MGCP to be used, use the following command.

Command	Mode	Description
mgc version *VALUE*	VoIP-MGC	Configures the version of MGCP.

To define the message format, use the following command.

Command	Mode	Description
mgc msg-format {**text-long** | **text-short** | **binary**}	VoIP-MGC	Configures the message format. (default: text-long)

To specify the maximum retry time for MGC transactions, use the following command.

Command	Mode	Description
mgc max-retry-time <0-65534>	VoIP-MGC	Configures the maximum retry time for MGC transactions. 0-65534: maximum retry time (unit: second)
no mgc max-retry-time		Deletes the configured maximum retry time.

To specify the maximum number of times that a message is retransmitted to the MGC, use the following command.

Command	Mode	Description
mgc max-retry-attempts <0-65534>	VoIP-MGC	Configures the maximum number of times that a message is retransmitted to the MGC. 0-65534: maximum number of times
no mgc max-retry-attempts		Deletes the configured maximum number of times.

To specify the service status delay time for changes in line service status, use the following command.

Command	Mode	Description
mgc service-change-delay <0-65534>	VoIP-MGC	Configures the service status delay time for changes in line service status. 0-65534: service status delay time
no mgc service-change-delay		Deletes the configured delay time.

To specify the gateway softswitch name, use the following command.

Command	Mode	Description
mgc soft-switch *NAME*	VoIP-MGC	Specifies the gateway softswitch name. NAME: gateway softswitch (format: four ASCII coded alphabetic characters [A-Z])
no mgc soft-switch		Deletes the gateway softswitch name configuration.

11.7.4 Saving VoIP Profile

After configuring a VoIP profile, you need to save the profile with the following command.

Command	Mode	Description
apply	VoIP-Profile	Saves a VoIP profile configuration.

i

Whenever you modify a VoIP profile, you should apply the changes again using the **apply** command. If not, the changes will not be applied.

11.7.5 Displaying VoIP Information

To display the information of VoIP profiles, use the following command.

Command	Mode	Description
show voip-profile [*NAME*]	Global GPON GPON-OLT VoIP-profile	Shows the information of VoIP profiles. NAME: VoIP profile name

To display VoIP service and VoIP line status information, use the following command.

Command	Mode	Description
show onu voip line *OLT-ID ONU-ID*	Enable Global GPON	Shows the information of VoIP service and line status. ONU-ID: 1-128 or ONU serial number
show onu voip line *ONU-ID*	GPON-OLT	

To display the information of current profile, use the following command.

Command	Mode	Description
show current-profile	Current-Profile	Shows the information currently configured for the profile.

11.7.6 Sample Configuration

For the sample configuration, see “Configuration Example 1” in 11.15 Sample Configuration.

11.8 TDM Pseudowire Profile

Pseudowire emulation is a method for transmitting any Layer 2 protocol over PSNs (Packet Switched Networks). It allows a seamless connection between two network elements by creating logical links, or virtual tunnels, across the packet network. In TDM pseudowires, the transmitted E1, T1, E3, or T3 streams are encapsulated in packets upon entering the network and then reconstructed at the pseudowire egress, where clocking information is also regenerated. As a result, real-time traffic is delivered transparently without distortion, avoiding the complexities of translating signaling data, while ensuring that synchronization criteria are met.

In order to perform the TDM pseudowire related configuration, you should create/enter the TDM pseudowire profile. For the creation and configuration of the profile, see the following sections.

11.8.1 Creating TDM Pseudowire Profile

To create a TDM pseudowire profile, use the following command.

Command	Mode	Description
tdm-pw-profile *NAME* **create**	GPON	Creates a TDM pseudowire profile. NAME: TDM pseudowire profile name

After opening *TDM Pseudowire Profile Configuration* mode, the prompt changes from SWITCH(gpon)# to SWITCH(config-tdm-pw-profile[*NAME*])#.

To delete an existing TDM pseudowire profile, use the following command.

Command	Mode	Description
no tdm-pw-profile {*NAME* | **all**}	GPON	Deletes the TDM pseudowire profile. NAME: TDM pseudowire profile name

To modify an existing TDM pseudowire profile, use the following command.

Command	Mode	Description
tdm-pw-profile *NAME* **modify**	GPON	Modifies the exisitng TDM pseudowire profile. NAME: TDM pseudowire profile name

11.8.2 Basic Service Type

To specify the basic service type, use the following command.

Command	Mode	Description
service-type {**unstructured** | **octet-aligned-unstructured** | **structured**}	TDM-PW-Profile	Specifies the basic service type, either a transparent bit pipe or an encapsulation that recognizes the underlying structure of the payload. unstructured: Basic unstructured (also known as structure agnostic) octet-aligned-unstructured: Octet-aligned unstructured, structure agnostic. Applicable only to DS1, a mode in which each frame of 193 bits is encapsulated in 25 bytes with 7 padding bits structured: Structured (structure-locked)

11.8.3 Signalling

To configure the signalling, use the following command.

Command	Mode	Description
signalling { **no-signalling** | **cas-carry-packet** | **cas-carry-channel** }	TDM-PW-Profile	Specifies the signalling attribute. no-signalling: No signalling visible at this layer cas-carry-packet: CAS, to be carried in the same packet stream as the payload cas-carry-channel: CAS, to be carried in a separate signalling channel

11.8.4 Payload Size

To specify the payload size per packet, use the following command.

Command	Mode	Description
payload-size {**192** | **200** | **256** | **1024**}	TDM-PW-Profile	Defines the number of payload bytes per packet. Valid only if service type = unstructured or unstructured octet-aligned. Valid choices depend on the TDM service as follows. 192: DS1 200: DS1, required only if unstructured octet-aligned service is supported 256: E1 1024: DS3 / E3
no payload-size		Deletes the configured payload size.

11.8.5 Payload Encapsulation Delay

To configure the payload encapsulation delay (only for structured service), use the following command.

Command	Mode	Description
payload-encapsulation-delay { **1** | **2** | **3** | **4** | **5** | **8** }	TDM-PW-Profile	Defines the delay time (which corresponds to number of 125 microsecond frames) to be encapsulated in each pseudowire packet. Valid only if service type = structured. The minimum set of choices for various TDM services is listed below, and is affected by the possible presence of in-band signalling. 8: 8 ms (that corresponds to 64 frames), no signalling, N = 1, required 5: 5 ms (that corresponds to 40 frames), no signalling, N = 1, desired 4: 4 ms (that corresponds to 32 frames), no signalling, N = 2~4 3: 3 ms (that corresponds to 24 frames), with DS1 CAS 2: 2 ms (that corresponds to 16 frames), with E1 CAS 1: 1 ms (that corresponds to 8 frames), no signalling, N > 4
no payload-encapsulation-delay		Deletes the configured payload encapsulation delay time.

11.8.6 Timing Mode

To configure the timing mode of the TDM service, use the following command.

Command	Mode	Description
timing-mode {**network** | **differential** | **adaptive** | **loop**}	TDM-PW-Profile	Selects the timing mode of the TDM service. If RTP is used, this configuration must be set to be consistent with the value of the RTP time stamp mode configuration in the RTP parameters setting at the far end. network: Network timing (default) differential: Differential timing adaptive: Adaptive timing loop: Loop timing. local TDM transmit clock derived from local TDM receive stream

11.8.7 RTP Pseudowire Parameter

If a pseudowire service uses RTP, the RTP pseudowire parameters provide configuration for the RTP layer. You can configure the RTP pseudowire parameters by referring to the following sections.

11.8.7.1 Clock Reference

To specify the frequency of the common timing reference, use the following command.

Command	Mode	Description
rtp-clock-reference *VALUE*	TDM-PW-Profile	Specifies the frequency of the common timing reference. VALUE: in multiples of 8 kHz (for example, input 1 means 8 kHz) (default: 1)

11.8.7.2 RTP Time Stamp Mode

To specify the RTP time stamp mode, use the following command.

Command	Mode	Description
rtp-time-stamp-mode {**unknown** | **absolute** | **differential**}	TDM-PW-Profile	Determines the mode in which RTP timestamps are generated in the TDM to PSN direction. unknown: Unknown or not applicable (default) absolute: Absolute. Timestamps are based on the timing of the incoming TDM signal differential: Differential. Timestamps are based on the ONT's reference clock, which is understood to be stratum-traceable along with the reference clock at the far end

11.8.7.3 RTP Payload Type

To configure the RTP payload type, use the following command.

Command	Mode	Description
rtp-payload-type payload *VALUE* **signalling** *VALUE*	TDM-PW-Profile	Specifies the RTP payload type in the TDM to PSN direction. payload VALUE: for the payload channel signalling VALUE: 96 to 127, for the optional separate signalling channel. If signalling is not transported in its own channel, this value should be set to 0.
rtp-expect-payload-type payload *VALUE* **signalling** *VALUE*		Specifies the RTP payload type in the PSN to TDM direction. The received payload type may be used to detect malformed packets. payload VALUE: for the payload channel signalling VALUE: for the optional separate signalling channel
no rtp-expect-payload-type		Deletes the configured RTP payload type in the PSN to TDM direction.

11.8.7.4 RTP Synchronization Source

To configure the RTP synchronization source, use the following command.

Command	Mode	Description
rtp-sync-source payload *VALUE* **signalling** *VALUE*	TDM-PW-Profile	Specifies the RTP synchronization source in the TDM to PSN direction. payload VALUE: for the payload channel signalling VALUE: for the optional separate signalling channel. If signalling is not transported in its own channel, this value should be set to 0.
rtp-expect-sync-source payload *VALUE* **signalling** *VALUE*		Specifies the RTP synchronization source in the PSN to TDM direction. The received synchronization source may be used to detect misconnection (stray packets). payload VALUE: for the payload channel signalling VALUE: for the optional separate signalling channel
no rtp-expect-sync-source		Deletes the configured RTP synchronization source in the PSN to TDM direction.

11.8.8 Pseudowire Maintenance Configuration

If you need the configuration for pseudowire service exception handling, you should connect a pseudowire maintenance profile to the current profile.

To connect the pseudowire maintenance profile to the current profile, use the following command.

Command	Mode	Description
pw-maintenance-profile *NAME*	TDM-PW-Profile	Connects a pseudowire maintenance profile to the current TDM pseudowire profile.
no pw-maintenance-profile		Disconnects the specified pseudowire maintenance profile.

i For the details of how to create and configure the pseudowire maintenance profile, see 11.9 Pseudowire Maintenance Profile.

11.8.9 Saving TDM Pseudowire Profile

After configuring a TDM pseudowire profile, you need to save the profile with the following command.

Command	Mode	Description
apply	TDM-PW-Profile	Saves a TDM pseudowire profile configuration.

i Whenever you modify a TDM pseudowire profile, you should apply the changes again using the **apply** command. If not, the changes will not be applied.

11.8.10 Displaying TDM Pseudowire Information

To display the information of TDM pseudowire profiles, use the following command.

Command	Mode	Description
show tdm-pw-profile [*NAME*]	Global GPON GPON-OLT TDM-PW-Profile	Shows the information of TDM pseudowire profiles. NAME: TDM pseudowire profile name

To display the list information of source MAC addresses for TDM pseudowire of ONU, use the following command.

Command	Mode	Description
show onu tdm-pw source-mac *OLT-ID ONU-ID*	Enable Global GPON	Shows the list of source MAC addresses for TDM pseudowire of the specified ONU.
show onu tdm-pw source-mac *ONU-ID*	GPON-OLT	

11.9 Pseudowire Maintenance Profile

The pseudowire maintenance profile permits the configuration of pseudowire service exception handling. The pseudowire maintenance profile primarily affects the alarms declared by the subscribing pseudowire termination. And also, the settings of a pseudowire maintenance profile affect the pseudowire performance monitoring history.

11.9.1 Creating Pseudowire Maintenance Profile

To create a pseudowire maintenance profile, use the following command.

Command	Mode	Description
pw-maintenance-profile *NAME* **create**	GPON	Creates a pseudowire maintenance profile. NAME: pseudowire maintenance profile name

After opening *PW Maintenance Profile Configuration* mode, the prompt changes from SWITCH(gpon)# to SWITCH(config-pw-maintenance-profile[*NAME*])#.

To delete an existing pseudowire maintenance profile, use the following command.

Command	Mode	Description
no pw-maintenance-profile {*NAME* | **all**}	GPON	Deletes the pseudowire maintenance profile. NAME: pseudowire maintenance profile name

To modify an existing pseudowire maintenance profile, use the following command.

Command	Mode	Description
pw-maintenance-profile *NAME* **modify**	GPON	Modifies the exisitng pseudowire maintenance profile. NAME: pseudowire maintenance profile name

11.9.2 Jitter Buffer Maximum Depth

To specify the maximum depth of the playout buffer in the PSN to TDM direction, use the following command.

Command	Mode	Description
jitter-buffer-max-depth *VALUE*	PW-Maintenance-Profile	Specifies the desired maximum depth of the playout buffer in the PSN to TDM direction. VALUE: expressed as a multiple of the 125 μs frame rate
no jitter-buffer-max-depth		Deletes the configured maximum depth of the playout buffer.

11.9.3 Jitter Buffer Desired Depth

To specify the desired nominal fill depth of the playout buffer in the PSN to TDM direction, use the following command.

Command	Mode	Description
jitter-buffer-desired-depth *VALUE*	PW-Maintenance-Profile	Specifies the desired nominal fill depth of the playout buffer in the PSN to TDM direction. VALUE: expressed as a multiple of the 125 μs frame rate
no jitter-buffer-desired-depth		Deletes the configured nominal fill depth of the playout buffer.

11.9.4 Fill Policy

To specify the payload bit pattern to be applied toward the TDM service, if no payload packet is available to play out, use the following command.

Command	Mode	Description
fill-policy {**vendor-specific** | **play-out-ais** | **play-out-all-1s** | **play-out-all-0s** | **repeat-prev-data** | **play-out-ds1-idle**}	PW-Maintenance-Profile	Defines the payload bit pattern to be applied toward the TDM service if no payload packet is available to play out. vendor-specific: ONT default, vendor-specific (recommended: AIS for unstructured service, all 1s for structured service) play-out-ais: Play out AIS according to the service definition (for example, DS3 AIS) play-out-all-1s: Play out all 1s play-out-all-0s: Play out all 0s repeat-prev-data: Repeat the previous data play-out-ds1-idle: Play out DS1 idle (Appendix C of "b-ATIS T1.403")
no fill-policy		Deletes the configured payload bit pattern.

11.9.5 Alarm-related Policy

The supports four pairs of alarm-related policies configuration which causes the corresponding alarm to be declared or cleared. To configure the policy (anomaly rate) that causes the alarm to be declared or cleared, use the following command.

Command	Mode	Description
buffer-over-underrun-declaration-policy <1-100>	PW-Maintenance-Profile	Defines the anomaly rate that causes the corresponding alarm to be declared. If this density of anomalies occurs during the alarm onset soak interval, the alarm is declared. buffer-over-underrun: buffer overrun/underrun loss-packet: loss packet
loss-packet-declaration-policy <1-100>		
malformed-packet-declaration-policy <1-100>		

misconnect-packet-declaration-policy <1-100>		malformed-packet: malformed packet misconnect-packet: misconnect packet 1-100: anomaly rate (unit: integer percentage)
buffer-over-underrun-clear-policy <0-99>		Defines the anomaly rate that causes the corresponding alarm to be cleared. If no more than this density of anomalies occurs during the alarm clear soak interval, the alarm is cleared. buffer-over-underrun: buffer overrun/underrun loss-packet: loss packet malformed-packet: malformed packet misconnect-packet: misconnect packet 1-99: anomaly rate (unit: integer percentage)
loss-packet-clear-policy <0-99>		
malformed-packet-clear-policy <0-99>		
misconnect-packet-clear-policy <0-99>		

To delete the configured anomaly rate, use the following command.

Command	Mode	Description
no buffer-over-underrun-declaration-policy	PW-Maintenance-Profile	Deletes the configured anomaly rate that causes the corresponding alarm to be declared or cleared.
no loss-packet-declaration-policy		
no malformed-packet-declaration-policy		
no misconnect-packet-declaration-policy		
no buffer-over-underrun-clear-policy		
no loss-packet-clear-policy		
no malformed-packet-clear-policy		
no misconnect-packet-clear-policy		

11.9.6 L-bit/R-bit Receive/Transmit Policy

To configure the L-bit receive policy, use the following command.

Command	Mode	Description
l-bit-receive-policy {**play-out** | **repeat-last-packet** | **send-idle**}	PW-Maintenance-Profile	Defines the action toward the TDM interface when far end TDM failure is indicated on packets received from the PSN (L-bit set). play-out: Play out service-specific AIS (default) repeat-last-packet: Repeat last received packet send-idle: Send channel idle signalling and idle channel payload to all DS0s comprising the service
no l-bit-receive-policy		Deletes the configured L-bit receive policy.

To configure the R-bit transmit set policy, use the following command.

Command	Mode	Description
r-bit-transmit-set-policy *VALUE*	PW-Maintenance-Profile	Defines the number of consecutive lost packets that causes the transmitted R-bit to be set in the TDM to PSN direction, indicating lost packets to the far end. VALUE: number of consecutive lost packets
no r-bit-transmit-set-policy		Deletes the configured R-bit transmit set policy.

To configure the R-bit receive policy, use the following command.

Command	Mode	Description
r-bit-receive-policy {**none** | **play-out** | **send-idle**}	PW-Maintenance-Profile	Defines the action toward the N x 64 TDM interface when remote failure is indicated on packets received from the PSN (R-bit set = 0b10 while the L-bit is cleared). none: Do nothing (default) play-out: Play out service-specific RAI/REI/RDI code send-idle: Send channel idle signalling and idle channel payload to all DS0s comprising the service

11.9.7 SES Threshold

To configure the SES threshold, use the following command.

Command	Mode	Description
ses-threshold *VALUE*	PW-Maintenance-Profile	Defines the number of lost, malformed or otherwise unusable packets expected in the PSN to TDM direction within a one-second interval that causes a severely errored second to be counted. Stray packets do not count toward a severely errored second, nor do packets whose L-bit is set at the far end. VALUE: Number of lost, malformed or otherwise unusable packets (default: 3)
no ses-threshold		Deletes the configured SES threshold.

11.9.8 Saving Pseudowire Maintenance Profile

After configuring a pseudowire maintenance profile, you need to save the profile with the following command.

Command	Mode	Description
apply	PW-Maintenance-Profile	Saves a pseudowire maintenance profile configuration.

i Whenever you modify a pseudowire maintenance profile, you should apply the changes again using the **apply** command. If not, the changes will not be applied.

11.9.9 Displaying Pseudowire Maintenance Information

To display the information of pseudowire maintenance profiles, use the following command.

Command	Mode	Description
show pw-maintenance-profile [*NAME*]	Global GPON GPON-OLT PW-Maintenance-Profile	Shows the information of pseudowire maintenance profiles. NAME: pseudowire maintenance profile name

To display the information of current profile, use the following command.

Command	Mode	Description
show current-profile	Current-Profile	Shows the information currently configured for the profile.

11.10 Performance Monitoring (PM) Profile

Performance Monitoring (PM) profile is used for the traffic statistics of all ONUs (ONTs) collected by an OLT. The ONT conceptually has only two storage bins: a current accumulator and a history bin. The current accumulator is used to store data collected for the current 15-minute interval. The history bin is used to store data for the previous 15-minute interval. At the end of the current 15-minute interval, they switch roles: the previous accumulator bin becomes the new history bin, while the content of the history bin is discarded and the bin itself is initialized as the new accumulator.The ONT performs no calculations upon the collected data nor does it keep an archive of collected data beyond the previous 15-minute interval. All calculations based on collected data and archiving of past intervals is performed by the OLT.

11.10.1 Creating PM Profile

To create a PM profile, use the following command.

Command	Mode	Description
pm-profile *NAME* **create**	GPON	Creates a PM profile. NAME: PM profile name

To delete a created PM profile, use the following command.

Command	Mode	Description
no pm-profile {*NAME* | **all**}	GPON	Deletes a created PM profile. NAME: PM profile name

To modify an existing PM profile, use the following command.

Command	Mode	Description
pm-profile *NAME* **modify**	GPON	Modifies the existing PM profile. NAME: PM profile name

i To collect the traffic statistics of ONUs via PM profile, the ONU must be applied with a Traffic Profile.

11.10.2 Collecting ONU Traffic Statistics

To enable/disable the performance monitoring (PM) function to collect the traffic statistics of the configured GEM port, use the following command.

Command	Mode	Description
pm gemport	PM-Profile	Enables the PM function to collect the GEM port-related counters.
no pm gemport		Disables the PM function to collect the GEM port-related counters.

To enable/disable the performance monitoring (PM) function to collect the traffic statistics of the configured ANI port, use the following command.

Command	Mode	Description
pm aniport	PM-Profile	Enables PM function to collect the data of ANI port's counters that are FCS error and the downstream GEM frame discarded due to buffer overflow or etc.
no pm aniport		Disables PM function to collect the data of ANI port's counters.

To enable/disable the performance monitoring (PM) function to collect the traffic statistics of the configured pseudowire, use the following command.

Command	Mode	Description
pm pseudowire	PM-Profile	Enables the PM function to collect the pseudowire-related counters.
no pm pseudowire		Disables the PM function to collect the pseudowire-related counters.

To enable/disable the performance monitoring (PM) function to collect the traffic statistics of the configured UNI port as Ethernet type 3, use the following command.

Command	Mode	Description
pm uni-eth3	PM-Profile	Enables the PM function to collect the counters of the configured UNI port as Ethernet type 3.
no pm uni-eth3		Disables the PM function to collect the counters of the configured UNI port as Ethernet type 3.

To enable/disable the performance monitoring (PM) function to collect the traffic statistics of the Ethernet frame over the configured UNI port, use the following command.

Command	Mode	Description
pm uni-eth-frame { **us** | **ds** }	PM-Profile	Enables the PM function to collect the Ethernet frame related conuters of UNI port. us: upstream ds: downstream
no pm uni-eth-frame		Disables the PM function to collect the Ethernet frame related conuters of UNI port.

To enable/disable the performance monitoring (PM) function to collect the traffic statistics of the configured CES UNI port, use the following command.

Command	Mode	Description
pm uni-ces	PM-Profile	Enables the PM function to collect the counters of the configured CES UNI port.
no pm uni-ces		Disables the PM function to collect the counters of the configured CES UNI port.

To enable/disable the performance monitoring (PM) function to collect the traffic statistics of the configured GEM NCTP ports, use the following command.

Command	Mode	Description
pm gem-nctp	PM-Profile	Enables the PM function to collect the counters of the configured GEM port network CTP for a specified traffic profile.
no pm gem-nctp		Disables the PM function to collect the counters of the configured GEM port network CTP.

11.10.3 Saving PM Profile

After configuring a PM profile, you need to save the profile with the following command.

Command	Mode	Description
apply	PM-Profile	Saves a PM profile configuration.

i Even if you modify a running profile, you also need to use the **apply** command to apply the changes to ONUs (ONTs).

11.10.4 Displaying PM Profile Information

To display the information of PM profiles, use the following command.

Command	Mode	Description
show pm-profile [*NAME*]	GPON GPON-OLT PM-Profile	Shows the information of PM profiles. NAME: PM profile name

To display the information of current profile, use the following command.

Command	Mode	Description
show current-profile	Current-Profile	Shows the information currently configured for the profile.

11.10.5 Displaying ONU Traffic Statistics

To display the traffic statistics of an ONU applied by PM profile, use the following command.

Command	Mode	Description
show onu statistics *OLT-ID* [*ONU-ID*]	Enable Global GPON	Shows the information of ONU counters collected via PM profile. (15 Min, Prev_15 Min, total)
show onu statistics [*ONU-ID*]	GPON-OLT	
show onu statistics detail *OLT-ID*	Enable Global GPON	Shows the information of GEM port counters collected via PM profile. (15 Min, Prev_15 Min, total)
show onu statistics detail [*ONU-ID*]	GPON-OLT	
show onu statistics {**current** | **current-detail**} *OLT-ID ONU-ID*	Enable Global GPON	Shows the information of current ONU counters collected via PM profile. (current counter, total + current counter)
show onu statistics {**current** | **current-detail**} *ONU-ID*	GPON-OLT	
show onu statistics avg-pkt *OLT-ID ONU-ID* [**uni-eth-frame** *UNI_ID*]	Enable Global GPON	Shows the information of ONU counter (average packets) collected via PM profile.
show onu statistics avg-pkt *ONU-ID* [**uni-eth-frame** *UNI_ID*]	GPON-OLT	
show onu statistics {**pre_15** | **hour** | **day** | **total**} *OLT-ID ONU-ID* {**eth** *PORT* {**us** | **ds**} | **pots** *PORT* | **tdm** *PORT* | **pw** *NUMBER* | **gem** *PORT* | **gem-nctp** *PORT* | **ani** *PORT* }	Enable Global GPON	Shows the information of ONU counters collected via PM profile based on Ethernet, POTS, TDM, GEM, ANI port or pseudowire number. pre_15/hour/day/total: time duration (previous 15min / hour / day / total) us/ds: upstream/downstream PORT: port number NUMBER: pseudowire number
show onu statistics {**pre_15** | **hour** | **day** | **total**} *ONU-ID* {**eth** *PORT* {**us** | **ds**} | **pots** *PORT* | **tdm** *PORT* | **pw** *NUMBER* | **gem** *PORT* **gem-nctp** *PORT* | **ani** *PORT* }	GPON-OLT	

To clear the collected traffic statistics, use the following command.

Command	Mode	Description
clear onu statistics	GPON	Clears collected traffic statistics of an ONU.
clear onu statistics *OLT-ID* [*ONU-ID*]		
clear onu statistics [*ONU-ID*]	GPON-OLT	Clears collected traffic statistics of an ONU.

11.10.6 Sample Configuration

For the sample configuration, see “Configuration Example 2” in 11.15 Sample Configuration.

11.11 Multicast Profile

The multicast profile is used for ONU (ONT) to handle the multicast traffic using a IGMP-related commands. Multicast profile managed entity organizes data associated with multicast management at subscriber ports of 802.1 bridges, including 802.1p mappers when the provisioning model is mapper-based rather than bridge-based. Instances of this managed entity are created and deleted by the OLT. It is the responsibility of the OLT to manage the members of a multicast group and control the multicast connection in ONTs

11.11.1 Creating Multicast Profile

To create a multicast profile, use the following command.

Command	Mode	Description
multicast-profile *NAME* **create**	GPON	Creates a multicast profile. NAME: multicast profile name

After opening *Multicast Profile Configuration* mode, the prompt changes from SWITCH(gpon)# to SWITCH(config-mcast-profile[*NAME*])#.

To delete a created multicast profile, use the following command.

Command	Mode	Description
no multicast-profile {*NAME* | **all**}	GPON	Deletes a created multicast profile. NAME: multicast profile name

To modify an existing multicast profile, use the following command.

Command	Mode	Description
multicast-profile *NAME* **modify**	GPON	Modifies the existing multicast profile. NAME: multicast profile name

11.11.2 IGMP Configurations

To configure the multicast profile, use the following command.

Command	Mode	Description
igmp version <1-3>	Multicast-Profile	Sets an IGMP version on a current interface. 1-3: IGMP version (default: 2)
igmp function snooping		Enables the IGMP snooping.
igmp function suppression		Enables the IGMP snooping with proxy reporting (SRP).
igmp function proxy		Enables the IGMP proxy.
igmp immediate-leave enable		Enables the IGMP immediate leave. (Default: enable)

igmp querier address *A.B.C.D*		Specifies a querier address. A.B.C.D: querier address
igmp querier query-interval <0-3600>		Specifies a general query interval. 0-3600: query interval (default: 125 seconds)
igmp querier max-response-time <0-25>		Specifies a maximum query response time. 0-25: maximum response time (default: 10 seconds)
igmp robustness-variable <1-7>		Configures the Querier's Robustness Variable (QRV) value on an interface. (default: 2)
igmp access-list vid {**untagged** | *VLAN*} **dst-ip start** *A.B.C.D* **end** *A.B.C.D* [**bw** *VALUE* | **src-ip** *A.B.C.D* | **gem** *PORT* | **cos** <0-7>]		Configures the dynamic/static access control list table. It discards the IGMP join message from ONTs based on the access list. VLAN: 1 to 4095, VLAN ID for specific tagged downstream flow dst-ip: destination IP address A.B.C.D: start/end IP address of the multicast group range VALUE: imputed group bandwidth (unit: bytes/sec) src-ip: source IP address PORT: multicast GEM port ID
igmp static-access-list vid {**untagged** | *VLAN*} **dst-ip start** *A.B.C.D* **end** *A.B.C.D* [**bw** *VALUE* | **src-ip** *A.B.C.D* | **gem** *PORT* | **cos** <0-7>]		
igmp tag-control {**bypass** | **add vid** *VLANS* **cos** *VALUE* | **replace vid** *VLANS* [**cos** *VALUE*]}		Configures IGMP tag control attribute and the policy to define a VLAN ID and P-bits to add to upstream IGMP messages. bypass: pass upstream IGMP traffic transparently add: adds a VLAN tag (including P-bits) to upstream IGMP traffic replace: replaces the TCI (VLAN ID + P-bits or VLAN ID) VLANS: VLAN ID(s) (1-4095) VALUE: CoS (0-7)
igmp ds-tag-control {**remove** | **bypass** | **add vid** *VLANS* **cos** *VALUE* | **replace vid** *VLANS* [**cos** *VALUE*]}		Configures IGMP downstream tag control attribute and the policy to define a VLAN ID and COS value to add to IGMP messages. bypass: pass downstream IGMP traffic transparently add: adds a VLAN tag (including P-bits) to downstream IGMP traffic replace: replaces the TCI (VLAN ID + P-bits or VLAN ID) VLANS: VLAN ID(s) (1-4095) VALUE: CoS (0-7)
igmp upstream rate-limit <1-65535>		Configures the rate limit of upstream IGMP traffic 1-65535: IGMP message count (message/second)
igmp unauthorized-join-request allow		ONU will forward the IGMP join request or an IGMPv3 membership report for groups that is not authorized in the dynamic address control list table.
igmp unauthorized-join-request discard		ONU will silently discard an unauthorized IGMP join request.

To delete a specified IGMP configuration for multicast profile, use the following command.

Command	Mode	Description
igmp immediate-leave disable	Multicast-Profile	Deletes a specified IGMP configuration
no igmp robustness-variable		
no igmp querier address		
no igmp querier query-interval		
no igmp querier max-response-time		
no igmp {**access-list** | **static-access-list**} **all**		
no igmp access-list vid {**untagged** | *VLANS*} **dst-ip start** *A.B.C.D* **end** *A.B.C.D* [**bw** *VALUE* | **src-ip** *A.B.C.D* | **gem** *PORTS*]		
no igmp static-access-list vid {**untagged** | *VLANS*} **dst-ip start** *A.B.C.D* **end** *A.B.C.D* [**bw** *VALUE* | **src-ip** *A.B.C.D* | **gem** *PORTS*]		
no igmp tag-control		
no igmp ds-tag-control		
no igmp upstream rate-limit		

11.11.3 Saving Multicast Profile

After configuring a multicast profile, you need to save the profile with the following command.

Command	Mode	Description
apply	Multicast-Profile	Saves a multicast profile configuration.

i

Whenever you modify a multicast profile, you should apply the changes again using the **apply** command. If you do not, it will not be applied.

11.11.4 Applying Multicast Profile

If you want to apply a created multicast profile to a MAC bridge service profile, open *Traffic Profile Configuration* mode first, then you have to apply the multicast profile to MAC bridge service profile and its UNI-side port.

```
SWITCH(config-mcast-profile[TEST])# apply
SWITCH(config-mcast-profile[TEST])# exit
SWITCH(gpon)# traffic-profile 1 create
SWITCH(config-traffic-pf[1])# bridge 1
SWITCH(config-traffic-pf[1]-bridge[1])# uni eth 1
SWITCH(config-traffic-pf[1]-bridge[1]-uni[eth:1])# multicast-profile TEST
```

To apply the configured multicast profile to a specified UNI-side port of a traffic profile, use the following command.

Command	Mode	Description
multicast-profile *NAME*	Traffic Bridge-UNI	Applies the configured Multicast profile to a specified UNI port. NAME: Multicast profile name
no multicast-profile		Deletes the connections between a multicast profile and this UNI port.

11.11.5 Displaying Multicast Information

To display the information of Multicast profiles, use the following command.

Command	Mode	Description
show multicast-profile [*PROFILE*]	GPON GPON-OLT Multicast-Profile	Shows the information of Multicast profiles PROFILE: Multicast profile name

11.11.6 Multicast Access List

The multicast access list is used for ONU (ONT) to handle the multicast traffic using the dynamic/static IGMP access list commands. For each dedicated multicast access list, it can permit/discard the IGMP message and multicast traffic of the specified IP multicast groups and ranges. It is the responsibility of the OLT to manage the members of a multicast group and control the multicast connection in ONTs. To implement this multicast access list per ONT, the specified multicast profile should be already configured on these ONTs.

11.11.6.1 Creating Multicast ACL

To create a multicast access list, use the following command.

Command	Mode	Description
multicast-access-list *NAME* **create**	GPON	Creates a multicast access list. NAME: multicast access list name

i The maximum number of access list tables can be configurable up to 5 within a multicast access list.

After opening *Multicast Access Control List Configuration* mode, the prompt changes from SWITCH(gpon)# to SWITCH(config-mcast-acl-profile[*NAME*])#.

To delete a created multicast access list, use the following command.

Command	Mode	Description
no multicast-access-list {*NAME* | **all**}	GPON	Deletes a created multicast access list. NAME: multicast access list name

To modify an existing multicast access list, use the following command.

Command	Mode	Description
multicast-access-list *NAME* **modify**	GPON	Modifies the existing multicast access list. NAME: multicast access list name

11.11.6.2 IGMP Access List Configuration

To configure the multicast access list, use the following command.

Command	Mode	Description
igmp access-list vid {**untagged** | *VLAN*} **dst-ip start** *A.B.C.D* **end** *A.B.C.D* [**bw** *VALUE* | **src-ip** *A.B.C.D* | **gem** *PORT* | **cos** <0-7>]	Multicast-ACL	Configures the dynamic/static access control list table. It discards the IGMP join message from ONTs based on the access list. VLAN: 1 to 4095, VLAN ID for specific tagged downstream flow dst-ip: destination IP address A.B.C.D: start/end IP address of the multicast group range VALUE: imputed group bandwidth (unit: bytes/sec) src-ip: source IP address PORT: multicast GEM port ID
igmp static-access-list vid {**untagged** | *VLAN*} **dst-ip start** *A.B.C.D* **end** *A.B.C.D* [**bw** *VALUE* | **src-ip** *A.B.C.D* | **gem** *PORT* | **cos** <0-7>]		

To remove the dynamic/static access control list configuration from the multicast access list, use the following command.

Command	Mode	Description
no igmp {**access-list** | **static-access-list**} **all**	Multicast-ACL	Removes the dynamic/static access control list configuration from the multicast access list.
no igmp access-list vid {**untagged** | *VLANS*} **dst-ip start** *A.B.C.D* **end** *A.B.C.D* [**bw** *VALUE* | **src-ip** *A.B.C.D* | **gem** *PORTS*]		
no igmp static-access-list vid {**untagged** | *VLANS*} **dst-ip start** *A.B.C.D* **end** *A.B.C.D* [**bw** *VALUE* | **src-ip** *A.B.C.D* | **gem** *PORTS*]		

11.11.6.3 Saving Multicast ACL

After configuring a multicast ACL, you need to save the profile with the following command.

Command	Mode	Description
apply	Multicast-ACL	Saves a multicast ACL configuration.

i Whenever you modify a multicast ACL, you should apply the changes again using the **apply** command. If you do not, it will not be applied.

11.11.6.4 Applying Multicast Access List

To apply the configured multicast access list to a specified ONU ID, use the following command.

Command	Mode	Description
onu multicast-access-list *ONU-ID NAME* [**multicast-profile** *NAME*]	GPON-OLT	Applies the dynamic/static multicast access control list table to ONU ID. It discards the IGMP join message from ONTs based on the access list. ONU_ID: ONU ID or ONU serial number NAME: multicast access list name multicast-profile: applies the multicast ACL to the specified ONUs on the Multicast profile. NAME: multicast profile name
no onu multicast-access-list *ONU-ID NAME* [**multicast-profile** *NAME*]		Removes the specified multicast access list configuration from ONU ID.

i Up to 8 multicast access lists can be configured per ONU ID.

11.11.6.5 Displaying Multicast Access List

To display the information of multicast access list, use the following command.

Command	Mode	Description
show multicast-access-list [*NAME*]	Enable Global GPON GPON-OLT Multicast-ACL	Shows the information of multicast access lists. NAME: Multicast access list name

To display the information of IGMP access control list per ONU, use the following command.

Command	Mode	Description
show onu multicast-access-list *OLT-ID*	Enable Global GPON	Shows the information of multicast access control lists per ONU.
show onu multicast-access-list [*ONU-ID*]	GPON-OLT	

11.12 Rate-limit Profile

Basically the rate-limit configuration can be set in ‘Traffic Profile’. And the ‘Traffic Profile’ is assigned to ONT through 'ONU Profile'. When the service rate should be changed, you don’t need to modify all the 'Traffic Profiles' in the OLT. If an OLT has so many 'Traffic Profiles', you can create 'Rate-limit profile' and all Traffic Profiles can share this 'Rate-limit profile'. So when the service rate needs to be changed, you simply can modify the 'Rate-limit profile'.

11.12.1 Creating Rate-limit Profile

To create an Rate-limit profile, use the following command.

Command	Mode	Description
rate-limit-profile *NAME* **create**	GPON	Creates an Rate-limit profile. NAME: Rate-limit profile name

After opening *Rate-limit Profile Configuration* mode, the prompt changes from SWITCH(gpon)# to SWITCH(config-rate-limit-profile[*NAME*])#.

To delete the created Rate-limit profile, use the following command.

Command	Mode	Description
no rate-limit-profile {*NAME* | **all**}	GPON	Deletes the created Rate-limit profile. NAME: Rate-limit profile name

To modify an existing Rate-limit profile, use the following command.

Command	Mode	Description
rate-limit-profile *NAME* **modify**	GPON	Modifies the existing Rate-limit profile. NAME: Rate-limit profile name

11.12.2 Configuring Rate-limit Profile

To configure the rate limit profile, use the following command.

Command	Mode	Description
downstream *PIR_VALUE* [*SIR_VALUE*]	Rate-limit Profile	Sets the downstream traffic bandwidth. SIR_VALUE: SIR bandwidth range of 0 to 2147483584 (in steps of 64Kbps) PIR_VALUE: PIR bandwidth range of 0 to 2147483584
upstream *PIR_VALUE* [*SIR_VALUE*]		Sets the upstream traffic bandwidth. SIR_VALUE: SIR bandwidth range of 0 to 2147483584 (in steps of 64Kbps) PIR_VALUE: PIR bandwidth range of 0 to 2147483584
no downstream		Deletes the configured rate limit for downstream traffic.
no upstream		Deletes the configured rate limit for upstream traffic.

11.12.3 Saving Rate-limit Profile

After configuring an Rate-limit profile, you need to save the profile with the following command.

Command	Mode	Description
apply	Rate-limit Profile	Saves an Rate-limit profile configuration.

i Whenever you modify an rate-limit profile, you should apply the changes again using the **apply** command. If you do not, it will not be applied.

11.12.4 Applying Rate-limit Profile

To apply the configured Rate-limit profile for GEM ports, use the following command.

Command	Mode	Description
gemport *RANGE* **rate-limit profile** *NAME*	Traffic-Mapper	Applies the configured Rate-limit profile to specified GEM port. NAME: Rate-limit profile name
no gemport *RANGE* **rate-limit profile**		Removes the Rate-limit profile from the GEM port.

i For the details of how to create and configure the Rate-limit profile, see 11.4.2 Creating a Mapper.

To apply the configured Rate-limit profile for an UNI-side port of ONU, use the following command.

Command	Mode	Description
rate-limit profile *NAME*	Traffic Bridge-UNI	Applies the configured Rate-limit profile to specified UNI port. NAME: Rate-limit profile name
no rate-limit profile		Removes the Rate-limit profile from connected UNI port.

i For the details of how to create and configure the Rate-limit profile, see 11.4.3.6 UNI Port Configuration.

11.12.5 Displaying Rate-limit Profile

To display the information of Rate-limit profile, use the following command.

Command	Mode	Description
show rate-limit-profile [*NAME*]	Enable Global GPON GPON-OLT Rate-limit-profile	Shows the information of Rate-limit profile. NAME: Rate-limit profile name

11.13 ONU Service Profile

The provides numerous functions to customize a GPON network with many CLI commands and parameters. Each ONU profile can be designed with several profiles such as T-CONT, DBA and VoIP to meet the requirement of data bandwidth, VoIP access and the advanced security issues. The also provides the service ONU profile for customer convenience. You can apply one of ONU profiles as the default profile to all ONUs or apply an ONU profile to specified ONUs with a given model name.

To apply a default ONU profile to all ONUs(ONTs), use the following command.

Command	Mode	Description
olt service-profile default *PROFILE*	GPON	Applies a default ONU profile to all ONUs. PROFILE: existing ONU profile name

To apply an ONU profile to specified ONUs(ONTs) with a given model name, use the following command.

Command	Mode	Description
olt service-profile model-name *NAME PROFILE*	GPON GPON-OLT	Applies an ONU profile to specified ONUs with a given model name. NAME: ONU model name PROFILE: existing ONU profile name

i

If you try to configure a default profile for all ONUs when a specified service ONU profile is already applied to ONUs with a given model name, the default ONU profile will be applied only to the ONUs that do not have specific profiles.

To release the default ONU profile from all ONUs(ONTs), use the following command.

Command	Mode	Description
no olt service-profile	GPON	Releases a default/service ONU profile from all ONUs.
no olt service-profile default		
no olt service-profile model-name *NAME*	GPON GPON-OLT	

To display the service ONU profile from all ONUs(ONTs), use the following command.

Command	Mode	Description
show olt service-profile	Enable Global GPON	Shows the configured service ONU profiles.

11.14 GPON Debug

To enable debugging of all GPON or a specific feature of GPON, use the following command.

Command	Mode	Description
debug gpon { **all** | **func** | **db** | **comm** | **ugrd** | **profile** | **queue** | **statistics** | **rauth**}	Enable GPON	Enables GPON debugging. all: all GPON features func: GPON function db: GPON database comm.: GPON communication ugrd: GPON auto-upgrade profile: GPON profile queue: GPON queue statistics: GPON statistics rauth: GPON radius-authentication
no debug gpon {**all** | **func** | **db** | **comm** | **ugrd** | **profile** | **queue** | **statistics** | **rauth**}		Disables GPON debugging.

To enable debugging of OMCI message between OLT and ONT, use the following command.

Command	Mode	Description
debug gpon omci {**console** | **syslog**}	GPON	Enables GPON OMCI debugging. console: log output to console syslog: log output to syslog
no debug gpon omci		Disables GPON OMCI debugging.

To display the debugging status of GPON, use the following command.

Command	Mode	Description
show debugging gpon	Enable Global GPON	Shows the debugging status of GPON.

11.15 Sample Configuration

Configuration Example 1

```
SWITCH(config)# gpon
SWITCH(gpon)# voip-profile voip create
SWITCH(config-voip-profile[voip])# codec-nego 1 codec pcma packet-period 10
silence-suppression 1
SWITCH(config-voip-profile[voip])# codec-nego 2 codec pcmu packet-period 10
silence-suppression 1
SWITCH(config-voip-profile[voip])# codec-nego 3 codec g729 packet-period 10
silence-suppression 1
SWITCH(config-voip-profile[voip])# codec-nego 4 codec g723 packet-period 10
silence-suppression 1
SWITCH(config-voip-profile[voip])# pstn-protocol-variant 616
SWITCH(config-voip-profile[voip])# protocol sip
SWITCH(config-voip-profile[voip]-sip)# proxy-server proxy.xxxxx.com
SWITCH(config-voip-profile[voip]-sip)# outbound-proxy-server proxy.xxxxx.com
SWITCH(config-voip-profile[voip]-sip)# register-server proxy.xxxxx.com
SWITCH(config-voip-profile[voip]-sip)# host-part-server proxy.xxxxx.com
SWITCH(config-voip-profile[voip]-sip)# dns primary 168.126.63.1
SWITCH(config-voip-profile[voip]-sip)# exit
SWITCH(config-voip-profile[voip])# apply
SWITCH(config-voip-profile[voip])# exit

SWITCH(gpon)# pm-profile pm_ces create
SWITCH(config-pm-profile[pm_ces])# pm uni-ces
SWITCH(config-pm-profile[pm_ces])# pm pseudowire
SWITCH(config-pm-profile[pm_ces])# apply
SWITCH(config-pm-profile[pm_ces])# exit

SWITCH(gpon)# dba-profile sr_100m create
SWITCH(config-dba-profile[sr_100m])# mode sr
SWITCH(config-dba-profile[sr_100m])# sla fixed 128
SWITCH(config-dba-profile[sr_100m])# sla maximum 102400
SWITCH(config-dba-profile[sr_100m])# apply
SWITCH(config-dba-profile[sr_100m])# exit

SWITCH(gpon)# pw-maintenance-profile pw_m create
SWITCH(config-pw-maintenance-profile[pw_m])# apply
SWITCH(config-pw-maintenance-profile[pw_m])# exit

SWITCH(gpon)# tdm-pw-profile tdm create
SWITCH(config-tdm-pw-profile[tdm])# payload-size 256
SWITCH(config-tdm-pw-profile[tdm])# timing-mode adaptive
SWITCH(config-tdm-pw-profile[tdm])# apply
SWITCH(config-tdm-pw-profile[tdm])# exit
```

```
SWITCH(gpon)# traffic-profile g-60a create
SWITCH(config-traffic-pf[g-60a])# tcont 1
SWITCH(config-traffic-pf[g-60a]-tcont[1])# gemport 1/1-1/4
SWITCH(config-traffic-pf[g-60a]-tcont[1])# dba-profile sr_100m
SWITCH(config-traffic-pf[g-60a]-tcont[1])# exit

SWITCH(config-traffic-pf[g-60a])# tcont 2
SWITCH(config-traffic-pf[g-60a]-tcont[2])# gemport 2/1-2/4
SWITCH(config-traffic-pf[g-60a]-tcont[2])# dba-profile sr_100m
SWITCH(config-traffic-pf[g-60a]-tcont[2])# exit

SWITCH(config-traffic-pf[g-60a])# tcont 3
SWITCH(config-traffic-pf[g-60a]-tcont[3])# gemport 4/1-4/4
SWITCH(config-traffic-pf[g-60a]-tcont[3])# dba-profile sr_100m
SWITCH(config-traffic-pf[g-60a]-tcont[3])# exit

SWITCH(config-traffic-pf[g-60a])# mapper 1
SWITCH(config-traffic-pf[g-60a]-mapper[1])# gemport count 4
SWITCH(config-traffic-pf[g-60a]-mapper[1])# exit

SWITCH(config-traffic-pf[g-60a])# mapper 2
SWITCH(config-traffic-pf[g-60a]-mapper[2])# gemport count 4
SWITCH(config-traffic-pf[g-60a]-mapper[2])# exit

SWITCH(config-traffic-pf[g-60a])# mapper 3
SWITCH(config-traffic-pf[g-60a]-mapper[3])# gemport count 4
SWITCH(config-traffic-pf[g-60a]-mapper[3])# exit

SWITCH(config-traffic-pf[g-60a])# bridge 1
SWITCH(config-traffic-pf[g-60a]-bridge[1])# ani mapper 1
SWITCH(config-traffic-pf[g-60a]-bridge[1])# uni eth 1
SWITCH(config-traffic-pf[g-60a]-bridge[1]-uni[eth:1])# exit
SWITCH(config-traffic-pf[g-60a]-bridge[1])# uni eth 2
SWITCH(config-traffic-pf[g-60a]-bridge[1]-uni[eth:2])# exit
SWITCH(config-traffic-pf[g-60a]-bridge[1])# uni eth 3
SWITCH(config-traffic-pf[g-60a]-bridge[1]-uni[eth:3])# exit
SWITCH(config-traffic-pf[g-60a]-bridge[1])# uni eth 4
SWITCH(config-traffic-pf[g-60a]-bridge[1]-uni[eth:4])# exit
SWITCH(config-traffic-pf[g-60a]-bridge[1])# exit

SWITCH(config-traffic-pf[g-60a])# bridge 2
SWITCH(config-traffic-pf[g-60a]-bridge[2])# ani mapper 2
SWITCH(config-traffic-pf[g-60a]-bridge[2]-ani[mapper:2])# exit
SWITCH(config-traffic-pf[g-60a]-bridge[2])# link ip-host-config 1
SWITCH(config-traffic-pf[g-60a]-bridge[2])# exit

SWITCH(config-traffic-pf[g-60a])# bridge 3
SWITCH(config-traffic-pf[g-60a]-bridge[3])# ani mapper 3
SWITCH(config-traffic-pf[g-60a]-bridge[3]-ani[mapper:3])# exit
SWITCH(config-traffic-pf[g-60a]-bridge[3])# link ip-host-config 2
SWITCH(config-traffic-pf[g-60a]-bridge[3])# exit
```

```
SWITCH(config-traffic-pf[g-60a])# ip-host-config 1
SWITCH(config-traffic-pf[g-60a]-iphost[1])# ip address dhcp
SWITCH(config-traffic-pf[g-60a]-iphost[1])# vlan-operation us-oper overwrite
100 0
SWITCH(config-traffic-pf[g-60a]-iphost[1])# vlan-operation ds-oper remove
SWITCH(config-traffic-pf[g-60a]-iphost[1])# link voip-service 1
SWITCH(config-traffic-pf[g-60a]-iphost[1])# exit

SWITCH(config-traffic-pf[g-60a])# ip-host-config 2
SWITCH(config-traffic-pf[g-60a]-iphost[2])# ip address static
SWITCH(config-traffic-pf[g-60a]-iphost[2])# dns primary 168.123.0.1 secondary
168.123.0.2
SWITCH(config-traffic-pf[g-60a]-iphost[2])# vlan-operation us-oper overwrite
200 0
SWITCH(config-traffic-pf[g-60a]-iphost[2])# vlan-operation ds-oper remove
SWITCH(config-traffic-pf[g-60a]-iphost[2])# link tdm-service 1
SWITCH(config-traffic-pf[g-60a]-iphost[2])# exit

SWITCH(config-traffic-pf[g-60a])# voip-service 1
SWITCH(config-traffic-pf[g-60a]-voip[1])# manage-method omci
SWITCH(config-traffic-pf[g-60a]-voip[1])# voip-profile voip
SWITCH(config-traffic-pf[g-60a]-voip[1])# uni pots 1
SWITCH(config-traffic-pf[g-60a]-voip[1]-uni[1])# exit
SWITCH(config-traffic-pf[g-60a]-voip[1])# exit

SWITCH(config-traffic-pf[g-60a])# ces 1
SWITCH(config-traffic-pf[g-60a]-ces[1])# tdm-service 1 mode pw-ip
SWITCH(config-traffic-pf[g-60a]-ces[1]-svc[1]-pw-ip)# tdm-profile tdm
SWITCH(config-traffic-pf[g-60a]-ces[1]-svc[1]-pw-ip)# udp port 10 tos 20
SWITCH(config-traffic-pf[g-60a]-ces[1]-svc[1]-pw-ip)# exit
SWITCH(config-traffic-pf[g-60a]-ces[1])# exit
SWITCH(config-traffic-pf[g-60a])# apply
SWITCH(config-traffic-pf[g-60a])# exit

SWITCH(gpon)# onu-profile g-60a create
SWITCH(config-onu-profile[g-60a])# traffic-profile g-60a
SWITCH(config-onu-profile[g-60a])# pm-profile pm_ces
SWITCH(config-onu-profile[g-60a])# circuit-pack card-config c-ds1-e1 e1
SWITCH(config-onu-profile[g-60a])# apply
SWITCH(config-onu-profile[g-60a])# exit
SWITCH(gpon)#
```

Configuration Example 2

```
SWTICH(config)# gpon
SWTICH(gpon)# pm-profile PM_PROFILE create
SWTICH(config-pm-profile[PM_PROFILE])# pm gemport
SWTICH(config-pm-profile[PM_PROFILE])# pm aniport
```

```
SWTICH(config-pm-profile[PM_PROFILE])# apply
SWTICH(config-pm-profile[PM_PROFILE])# exit
SWITCH(gpon)# onu-profile ONU_PROFILE create
SWITCH(config-onu-profile[ONU_PROFILE])# traffic-profile TRAFFIC_PROFILE
SWITCH(config-onu-profile[ONU_PROFILE])# pm-profile PM_PROFILE
SWITCH(config-onu-profile[ONU_PROFILE])# apply
SWITCH(config-onu-profile[ONU_PROFILE])# exit
SWITCH(gpon)#

SWITCH(gpon)# gpon-olt 2
SWITCH(config-gpon-olt[2])# show onu statistics
-------------------------------------------------------------------------------
OLT : 2 ONU : 1
-------------------------------------------------------------------------------
Enabled PM : gemport aniport
Elapsed time after clear : 0d 1h 32m 33s
Elapsed time after update : 0d 0h 5m 3s
-------------------------------------------------------------------------------
GEM port PM counter | 15Min | Prev-15Min | Total
-------------------------------------------------------------------------------
Lost Packets         |   0     |     0     |   0
Misinserted Packets  |   0     |     0     |   0
Received Packets     |  131    |    126    |  642
Received Blocks      |  366    |    356    | 1799
Transmitted Blocks   |  578    |    567    | 2836
Impaired Blocks      |   0     |     0     |   0
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
ANI port PM counter | 15Min | Prev-15Min | Total
-------------------------------------------------------------------------------
Discarded Frames     |   0     |     0     |   0
-------------------------------------------------------------------------------
SWITCH(config-gpon-olt[2])# show onu statistics current 1
-------------------------------------------------------------
OLT : 2 ONU : 1
-------------------------------------------------------------
Enabled PM : gemport aniport
Elapsed time after clear : 0d 1h 33m 4s
Elapsed time after update : 0d 0h 5m 34s
-------------------------------------------------------------
GEM port PM counter | Current | Total + Current
-------------------------------------------------------------
Lost Packets         |   0     | 0
Misinserted Packets  |   0     | 0
Received Packets     |   26    | 668
Received Blocks      |   73    | 1872
Transmitted Blocks   |   106   | 2942
Impaired Blocks      |   0     | 0
-------------------------------------------------------------------------------
-------------------------------------------------------------
ANI port PM counter | Current | Total + Current
-------------------------------------------------------------
Discarded Frames     |    0    | 0
-------------------------------------------------------------
SWITCH(config-gpon-olt[2])#
```

12 System Software Upgrade

For the system enhancement and stability, new system software may be released. Using this software, the can be upgraded without any hardware change. You can simply upgrade your system software with the provided upgrade functionality via the CLI.

12.1 General Upgrade

The supports the dual system software functionality, which you can select applicable system software stored in the system according to various reasons such as the system compatibility or stability.

To upgrade the system software of the switch, use the following command.

Command	Mode	Description
copy {**ftp** | **tftp**} **os download** {**os1** | **os2**}	Enable	Upgrades the system software of the switch via FTP or TFTP. os1 | os2: the area where the system software is stored

⚠ To upgrade the system software, FTP or TFTP server must be set up first! Using the **copy** command, the system will download the new system software from the server.

⚠ To reflect the downloaded system software, the system must restart using the **reload** command!

The following is an example of upgrading the system software stored in **os1**.

```
SWITCH# copy ftp os download os1
 To exit : press Ctrl+D
-------------------------------------
IP address or name of remote host (FTP): 10.100.158.144
Download File Name : .1.05.x
User Name : admin
Password:
Hash mark printing on (1024 bytes/hash mark).
Downloading NOS ....
##############################################################################
##############################################################################
##############################################################################
##############################################################################
##############################################################################
##############################################################################

(Omitted)

##############################################################################
##############################################################################
##############################################################################
##############################################################################
##############################################################################
##############################################################################
##############################################################################
##########################################################
13661792 bytes download OK.
```

```
SWITCH# default-os os1
SWITCH# write memory
SWITCH# reload
Do you want to save the system configuration? [y/n]y
Do you want to reload the system? [y/n]y

Broadcast message from admin (ttyp0) (Fri Aug 18 15:15:41 2006 +0000):

The system is going down for reboot NOW!

SWITCH login: admin
Password:
SWITCH>enable
SWITCH# show flash

Flash Information(Bytes)

 Area                          total          used          free
 ---------------------------------------------------------------
 OS1(default)(running)      16777216      13661822       3115394     1.05
 OS2                        16777216      13661428       3115788     1.03
 CONFIG                      4194304        663552       3530752
 ---------------------------------------------------------------
 Total                      37748736      27986802       9761934
```

12.2 Boot Mode Upgrade

In case that you cannot upgrade the system software with the general upgrade procedure, you can upgrade it with the boot mode upgrade procedure. Before the boot mode upgrade, please keep in mind the following restrictions.

- A terminal must be connected to the system via the console interface. To open the boot mode, you should press <**S**> key when the boot logo is shown up.
- The boot mode upgrade supports TFTP only. You must set up TFTP server before upgrading the system software in the boot mode.
- In the boot mode, the only interface you can use is MGMT interface. So the system must be connected to the network via the MGMT interface.
- All you configures in the boot mode is limited to the boot mode only!

To upgrade the system software in the boot mode, perform the following step-by-step instruction:

Step 1 To open the boot mode, press <**S**> key when the boot logo is shown up.

```
************************************************************
*                                                          *
*                Boot Loader Version x.xx                  *
*                     FURUKAWA ELECTRIC                    *
*                                                          *
************************************************************
Press 's' key to go to Boot Mode:  0
Boot>
```

Step 2 To enable the MGMT interface to communicate with TFTP server, you need to configure a proper IP address, subnet mask and gateway on the interface.

To configure an IP address, use the following command.

Command	Mode	Description
ip *A.B.C.D*	Boot	Configures an IP address.
ip		Shows a currently configured IP address.

To configure a subnet mask, use the following command.

Command	Mode	Description
netmask *A.B.C.D*	Boot	Configures a subnet mask. (e.g. 255.255.255.0)
netmask		Shows a currently configured subnet mask.

To configure a default gateway, use the following command.

Command	Mode	Description
gateway *A.B.C.D*	Boot	Configures a default gateway.
gateway		Shows a currently configured default gateway.

To display a configured IP address, subnet mask and gateway, use the following command.

Command	Mode	Description
show	Boot	Shows a currently configured IP address, subnet mask and gateway.

The configured IP address, subnet mask and gateway on the MGMT interface are limited to the boot mode only!

The following is an example of configuring an IP address, subnet mask and gateway on the MGMT interface in the boot mode.

```
Boot> ip 10.27.41.83
Boot> netmask 255.255.255.0
Boot> gateway 10.27.41.254
Boot> show
IP          = 10.27.41.83
GATEWAY     = 10.27.41.254
NETMASK     = 255.255.255.0
MAC         = b8:26:d4:00:0d:83
MAC1        = ff:ff:ff:ff:ff:ff
Boot>
```

Step 3 Download the new system software via TFTP using the following command.

Command	Mode	Description
load {**os1** | **os2**} *A.B.C.D FILENAME*	Boot	Downloads the system software. os1 | os2: the area where the system software is stored A.B.C.D: TFTP server address FILENAME: system software file name

To verify the system software in the system, use the following command.

Command	Mode	Description
flashinfo	Boot	Shows the system software in the system.

To upgrade the system software in the boot mode, TFTP server must be set up first! Using the **load** command, the system will download the new system software from the server.

The following is an example of upgrading the system software stored in **os1** in the boot mode.

```
Boot> load os1 10.27.41.82  1.05.x
TFTP from server 10.27.41.82; our IP address is 10.27.41.83
Filename '.1.05.x'.
Load address: 0xffffe0
Loading: ######################################################################
         ######################################################################
         ######################################################################
         ######################################################################
         ######################################################################

         (Omitted)

         ######################################################################
         ######################################################################
         ######################################################################
         ######################################################################
         ######################################################################
         ####
done
Bytes transferred = 13661822 (d0767e hex)

Update flash: Are you sure (y/n)? y
 Erasing      : 0x01D00000 - 0x01D1FFFF
 Programming  : 0x01D00000 - 0x01D1FFFF
 Verifying    : 0x01D00000 - 0x01D1FFFF
Boot> flashinfo
Flash Information(Bytes)
Area     OS size      Default-OS    Standby-OS     OS Version
-------------------------------------------------------------
os1       13661806        *             *         1.05
os2       13661412                                1.03

Boot>
```

Step 4 Reboot the system with the new system software using the following command.

Command	Mode	Description
reboot [**os1** | **os2**]	Boot	Reboots the system with specified system software. os1 | os2: the area where the system software is stored

If the new system software is a current standby OS, just exit the boot mode, then the interrupted system boot will be continued again with the new system software.

To exit the boot mode, use the following command.

Command	Mode	Description
exit	Boot	Exits the boot mode.

12.3 FTP Upgrade

The system software of the can be upgraded using FTP. This will allow network or system administrators to remotely upgrade the system with the familiar interface.

To upgrade the system software using FTP, perform the following step-by-step instruction:

Step 1 Connect to the with your FTP client software. To login the system, you can use the system user ID and password.

Note that you must use the command line-based interface FTP client software when upgrading the . If you use the graphic-based interface FTP client software, the system cannot recognize the upgraded software.

Step 2 Set the file transfer mode to the binary mode using the following command.

Command	Mode	Description
bin	FTP	Sets the file transfer mode to the binary mode.

Step 3 Enable to print out the hash marks as transferring a file using the following command.

Command	Mode	Description
hash	FTP	Prints out the hash marks as transferring a file.

Step 4 Uploads the new system software using the following command.

Command	Mode	Description
put *FILENAME* {**os1** | **os2**}	FTP	Uploads the system software. FILENAME: system software file name os1 | os2: the area where the system software is stored

Step 5 Exit the FTP client using the following command.

Command	Mode	Description
bye	FTP	Exits the FTP client.

To reflect the downloaded system software, the system must restart using the **reload** command!

The following is an example of upgrading the system software of the using the FTP provided by Microsoft Windows XP in the remote place.

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>ftp 10.27.41.91
Connected to 10.27.41.91.
220 FTP Server 1.2.4 (FTPD)
User (10.27.41.91:(none)): admin
331 Password required for admin.
Password:
230 User root logged in.
ftp> bin
200 Type set to I.
ftp> hash
Hash mark printing On  ftp: (2048 bytes/hash mark) .
ftp> put .1.05.x os1
200 PORT command successful.
150 Opening BINARY mode data connection for os1.
################################################################################
################################################################################
################################################################################
################################################################################
################################################################################
################################################################################

(Omitted)

################################################################################
################################################################################
################################################################################
################################################################################
################################################################################
#########################################
226 Transfer complete.
ftp: 13661428 bytes sent in 223.26Seconds 61.19Kbytes/sec.
ftp> bye
221 Goodbye.

C:\>
```

To upgrade the system software via the FTP server, the FTP server should be enabled on the system.

12.4 ONU Upgrade

The provides the remote ONU (ONT) upgradeability. This feature allows the system administrators not to offer the local service for a single ONU (ONT) at the customer premise. To upgrade an ONU successfully, you need to download a new ONU firmware in the system.

12.4.1 Manual Upgrade

To upgrade the ONU, perform the following step-by-step instruction:

Step 1 Download ONU firmware using the following command.

Command	Mode	Description
copy {**ftp** | **tftp**} **onu download**	Enable	Downloads ONU firmware via FTP or TFTP.

i ONU firmware can be downloaded by the above command. You can recognize ONU firmware by the **show onu firmware-list** command.

Step 2 Verify the downloaded ONU firmware in the system using the following command.

Command	Mode	Description
show onu firmware-list	Enable Global GPON GPON-OLT	Shows the ONU firmware list in the system.

Step 3 Upgrade an ONU with the downloaded firmware using the following command.

Command	Mode	Description
onu upgrade *ONU-ID FILENAME* {**ftp** *A.B.C.D USER PASSWD* | **tftp** *A.B.C.D*}	GPON-OLT	Upgrades an ONU (ONT) with a specified firmware. ONU-ID: ONU ID (1-128) or ONU serial number FILENAME: firmware file name A.B.C.D: FTP/TFTP server IP address USER: FTP server user name PASSWD: FTP server password

! After finishing the ONU upgrade, the ONU will restart automatically!

Step 4 Activate the upgraded ONT firmware's version using the following command.

Command	Mode	Description
onu firmware active-change {**all** | *ONU-IDs*}	GPON-OLT	Activate an firmware version of specified ONU or all ONTs. ONU-ID: 1-128

Step 5 Verify the upgraded ONU firmware's information using the following command.

Command	Mode	Description
show onu firmware-list	Enable Global GPON GPON-OLT	Shows the ONU firmware list in the system.
show onu firmware version [*ONU-IDs*]	GPON-OLT	Shows an ONU firmware version.

12.4.2 Auto Upgrade

For efficient system maintenance, the provides the auto upgrade functionality for ONU firmware in the operational environment. You can simply upgrade the ONU firmware without an effort for every single ONU.

To automatically upgrade the ONU, perform the following step-by-step instruction:

Step 1 Download GPON ONU firmware using the following command.

Command	Mode	Description
onu auto-upgrade firmware *NAME FW_NAME* {**ftp** | **tftp**} *A.B.C.D USER PASSWD*	Enable	Downloads ONU (ONT) firmware via FTP or TFTP. NAME: ONU model name FW_NAME: firmware name A.B.C.D: FTP/TFTP server IP address USER: FTP/TFTP server user name PASSWD: FTP/TFTP server password

Step 2 Verify the downloaded ONU firmware in the system using the following command.

Command	Mode	Description
show onu auto-upgrade firmware [**info**]	GPON	Shows the ONU firmware list in the system.

Step 3 Upgrade ONUs by enabling ONU auto upgrade using the following command.

Command	Mode	Description
onu auto-upgrade {**enable** | **disable**}	GPON-OLT	Enables/disables ONU auto upgrade function.

When ONU auto upgrade function is enabled, the compares the downloaded ONU firmware in the system with the firmware currently loaded in the connected ONUs. If the version of the firmware from ONU side is lower than that of the firmware from the OLT side, then the firmware upgrade will automatically start.

Step 4 To perform the auto upgrade of OLT firmware when the version of two firmware is different, regardless of the lastest firmware version, use the following command.

Command	Mode	Description
onu auto-upgrade version-match all { **enable** | **disable**}	GPON-OLT	Enables/disables the ONU auto upgrade function without verification of the firmware version.
onu auto-upgrade invalid-version-match all { **enable** | **disable**}		Enables/disables the ONU auto upgrade function without verification of the firmware version format.

Step 5 Reflect the upgraded ONU firmware by restarting ONUs using the following command.

Command	Mode	Description
onu auto-upgrade reboot-time {<0-23> | **disable**}	GPON	Specifies/deletes the time that upgrade-completed ONUs restart. 0-23: restart time (unit: o'clock)

Step 6 Verify a progress of ONU auto upgrade using the following command.

Command	Mode	Description
show onu auto-upgrade info	GPON GPON-OLT	Shows a progress of ONU auto upgrade. OLT-ID: PON port number
show onu auto-upgrade status	GPON-OLT	

Step 7 Verify the upgraded ONU firmware's version using the following command.

Command	Mode	Description
show onu auto-upgrade firmware [**info**]	GPON	Shows an ONU firmware version.
show onu auto-upgrade current-fw	GPON-OLT	Shows a current ONU firmware.

12.4.3 Upgrade Time-out Configuration

It is possible to set the total upgrade time for ONU firmware update. If ONU firmware has not been lownloaded from server during the specified time, it is regarded as a upgrade failure.

To set the time out for ONU upgrade, use the following command.

Command	Mode	Description
onu upgrade download-timeout [<60-6000>]	GPON	Set the total time for ONU firmware download. (defuat: 300 seconds)
onu upgrade commit-timeout [<60-6000>]		Set the total time for ONU upgrade commit. (default: 300 seconds)

To display the configured upgrade timeout and related information, use the following command.

Command	Mode	Description
show onu upgrade config	Enable Global GPON	Shows the number of upgrade and the configured total time for ONU firmware download.

12.4.4 Upgrade Maximum Count Configuration

It is possible to set the upgrade maximum count for ONU firmware update. If ONU firmware has not been lownloaded from server during the specified time, it is regarded as a upgrade failure.

To set the count for ONU upgrade, use the following command.

Command	Mode	Description
onu upgrade max-count <1-16>	GPON	Set the max count for ONU firmware download. 1-16: concurrent upgrade count (defuat:4)

To display the number of upgrade and related information, use the following command.

Command	Mode	Description
show onu upgrade config	Enable Global GPON	Shows the number of upgrade and the configured total time for ONU firmware download.

13 Abbreviations

ACL	Access Control List
ARP	Address Resolution Protocol
ASM	Any Source Multicast
BSR	Bootstrap Router
CE	Communauté Européenne
CIDR	Classless Inter Domain Routing
CLI	Command Line Interface
CLNS	Connectionless Network Service
CoS	Class of Service
CSNP	Complete Sequence Number PDU
DA	Destination Address
DBA	Dynamic Bandwidth Allocation
DHCP	Dynamic Host Configuration Protocol
DIS	Designated IS
DR	Designated Router
DSCP	Differentiated Service Code Point
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
EGP	Exterior Gateway Protocol
EMC	Electro-Magnetic Compatibility
EN	Europäische Norm (European Standard)
FDB	Forwarding Data Base
FE	Fast Ethernet
FSM	Finite State Machine
FTP	File Transfer Protocol
GB	Gigabyte
GE	Gigabit Ethernet
GenID	Generation ID
HW	Hardware
ID	Identifier
IEC	International Electrotechnical Commission

IEEE 802	Standards for Local and Metropolitan Area Networks
IEEE 802.1	Glossary, Network Management, MAC Bridges, and Internetworking
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IFSM	Interface Finite State Machine
IGMPv1	Internet Group Management Protocol Version 1
IGMPv2	Internet Group Management Protocol Version 2
IGMPv3	Internet Group Management Protocol Version 3
IGP	Interior Gateway Protocol
IP	Internet Protocol
ISP	Internet Service Provider
ITU	International Telecommunication Union
ITU-T	International Telecommunication Union - Telecommunications standardization sector
IU	Interface Unit
KAT	Keep Alive Time
L2	Layer 2
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
LCT	Local Craft Terminal
LLDP	Link Layer Discover Protocol
LLID	Logical Link ID
LS	Link-State
LSP	Link-State PDU
MAC	Medium Access Control
McFDB	Multicast Forwarding Database
MFC	Multicast Forwarding Cache
MPCP	Multi-point Control Protocol
MRIB	Multicast Routing Information Base
MTU	Maximum Transmission Unit
MVR	Multicast VLAN Registration
NBMA	Non-Broadcast Multi-Access
NE	Network Element

NET	Network Entity Title
NFSM	Neighbor Finite State Machine
NTP	Network Time Protocol
OIF	Outgoing Interface
OLT	Optical Line Termination
ONT	Optical Network Terminal
OS	Operating System
PC	Personal Computer
PDU	Protocol Data Unit
PON	Passive Optical Network
PSNP	Partial Sequence Number PDU
PVID	Port VLAN ID
QoS	Quality of Service
QRV	Querier's Robustness Variable
RFC	Request for Comments
RMON	Remote Monitoring
RP	Rendezvous Point
RPF	Reverse Path Forwarding
RPT	Rendezvous Point Tree
RSTP	Rapid Spanning Tree Protocol
RTC	Real Time Clock
SA	Source Address
SFP	Small Form Factor Pluggable
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SNPA	Sub-Network Point of Attachment
SNTP	Simple Network Time Protocol
SPT	Shortest Path Tree
SSH	Secure Shell
SSM	Source-Specific Multicast
STP	Spanning Tree Protocol
SW	Software
TCN	Topology Change Notification

TCP	Transmission Control Protocol
TIB	Tree Information Base
TFTP	Trivial FTP
ToS	Type of Service
TTL	Time-To-Live
UDP	User Datagram Protocol
UMN	User Manual
VID	VLAN ID
VIF	Virtual Interface
VLAN	Virtual Local Area Network
VoD	Video on Demand
VPN	Virtual Private Network
xDSL	Any form of DSL

Issue History

Revision	Date	Update
00	03/2019	Initial release

FURUKAWA ELECTRIC

CENTROS DE PRODUÇÃO

BRASIL

CURITIBA – PR
R. Hasdrubal Bellegard, 820
Cidade Industrial
CEP: 81460-120
Tel.: (41) 3341-4200
E-mail: fisa@furukawa.com.br

SOROCABA – SP
Av. Pirelli, nº 1.100, bloco D
Éden
CEP: 18103-085
Tel.: (15) 3141-4530

SANTA RITA DO SAPUCAÍ – MG
Av. Sapucaí, 450 – Boa Vista
CEP: 37540-000
Tel.: (35) 3473-8300

ARGENTINA

PROVINCIA DE BUENOS AIRES
Ruta Nacional 2, km 37,5
Centro Industrial Ruta 2 – Berazategui
CP.: B1884AGA
Tel.: (54 22) 2949-1930

COLÔMBIA

PALMIRA, VALLE DEL CAUCA
Kilómetro 6 via Yumbo-Aeropuerto,
Zona Franca del Pacifico
Lotes 1-2-3 Manzana J, Bodega 2
Tel.: (572) 280-0000

ESCRITÓRIOS COMERCIAIS & REGIONAIS

BRASIL

SÃO PAULO – SP
Av. das Nações Unidas, 11.633
10º andar – Ed. Brasilinterpart
CEP: 04578-901
Tel.: (11) 5501-5711
Fax: (11) 5501-5757
E-mail: saopaulo@furukawa.com.br

PAULÍNIA – SP
Av. Dr. Roberto Moreira, km 4
Recanto dos Pássaros
CEP: 13148-900
Tel.: (19) 2116-2000

BELO HORIZONTE – MG
Cel.: (31) 99126-7066
E-mail: belohorizonte@furukawa.com.br

BRASÍLIA – DF
(DF, GO, TO)
Cel.: (61) 98102-1919
E-mail: brasilia@furukawa.com.br

CURITIBA – PR
Tel.: (41) 3341-4275
E-mail: curitiba@furukawa.com.br

CUIABÁ – MT
(MT/MS/RO/AC)
Cel.: (65) 99981-1767

MANAUS – AM
(AM, AP, MA, PA, RR)
Cel.: (92) 98122-0381
E-mail: manaus@furukawa.com.br

PORTO ALEGRE – RS
(RS, SC)
Cel.: (51) 98116-0435
E-mail: portoalegre2@furukawa.com.br

RECIFE – PE
(PE, PI, CE, RN, PB)
Cel.: (71) 99205-9877
E-mail: recife@furukawa.com.br

RIO DE JANEIRO – RJ
(RJ, ES)
Cel.: (21) 98128-2915
E-mail: riodejaneiro@furukawa.com.br

SALVADOR – BA
(BA, SE, AL)
Cel.: (71) 99205-9877
E-mail: salvador@furukawa.com.br

ARGENTINA

CIUDAD AUTÓNOMA DE BUENOS AIRES
Maipú 255 – Piso 11B
CP: C1084ABE
Tel.: (54 11) 4326-4440
E-mail: argentina@furukawa.com.br

COLÔMBIA

BOGOTÁ
Av. Calle 100 No.9A - 45
Torre 1 – Piso 6 – Oficina 603
Tel.: (571) 5162367

ESPANHA

MADRID
Calle López de Hoyos, 35 – 1º
CP: 28002
Tel.: (34 91) 745 74 29
espana@furukawa.com.br

MÉXICO

NAUCALPAN DE JUÁREZ
Federico T. de la Chica, 2, Int. 302
Ciudad Satélite – Estado de México
CP: 53100
Tel.: (52 55) 5393-4596
E-mail: mexico@furukawa.com.br

CENTROS DE DISTRIBUIÇÃO

BRASIL

CURITIBA – PR
R. Hasdrubal Bellegard, 820
Cidade Industrial – CEP: 81460-120

CABO DE SANTO AGOSTINHO – PE
Rodovia BR 101 Sul, 5225
Anexo A – Ponte dos Carvalhos
CEP: 54510-000

ARGENTINA

PROVINCIA DE BUENOS AIRES
Ruta Nacional 2, km 37,5
Centro Industrial Ruta 2 – Berazategui
CP: B1884AGA

COLÔMBIA

PALMIRA, VALLE DEL CAUCA
Kilómetro 6 via Yumbo-Aeropuerto,
Zona Franca del Pacifico
Lotes 1-2-3 Manzana J, Bodega 2

MÉXICO

ESTADO DE MÉXICO
Av. Gustavo Baz Prada km 12,5
Parque Industrial CPA B-2 Logistics Center
Col. San Pedro Barrientos
Tlalnepantla de Baz - CP: 54010

ESPANHA

MADRID
Carretera M-300 km 28,500
Alcalá de Henares – CP: 28802
Tel.: (34 91) 110 95 90

www.furukawalatam.com / 0800 412100