

ARTISAN®
TECHNOLOGY GROUP

Your **definitive** source for quality pre-owned equipment.

Artisan Technology Group
(217) 352-9330 | sales@artisantg.com | artisantg.com

Full-service, independent repair center
with experienced engineers and technicians on staff.

We buy your excess, underutilized, and idle equipment
along with credit for buybacks and trade-ins.

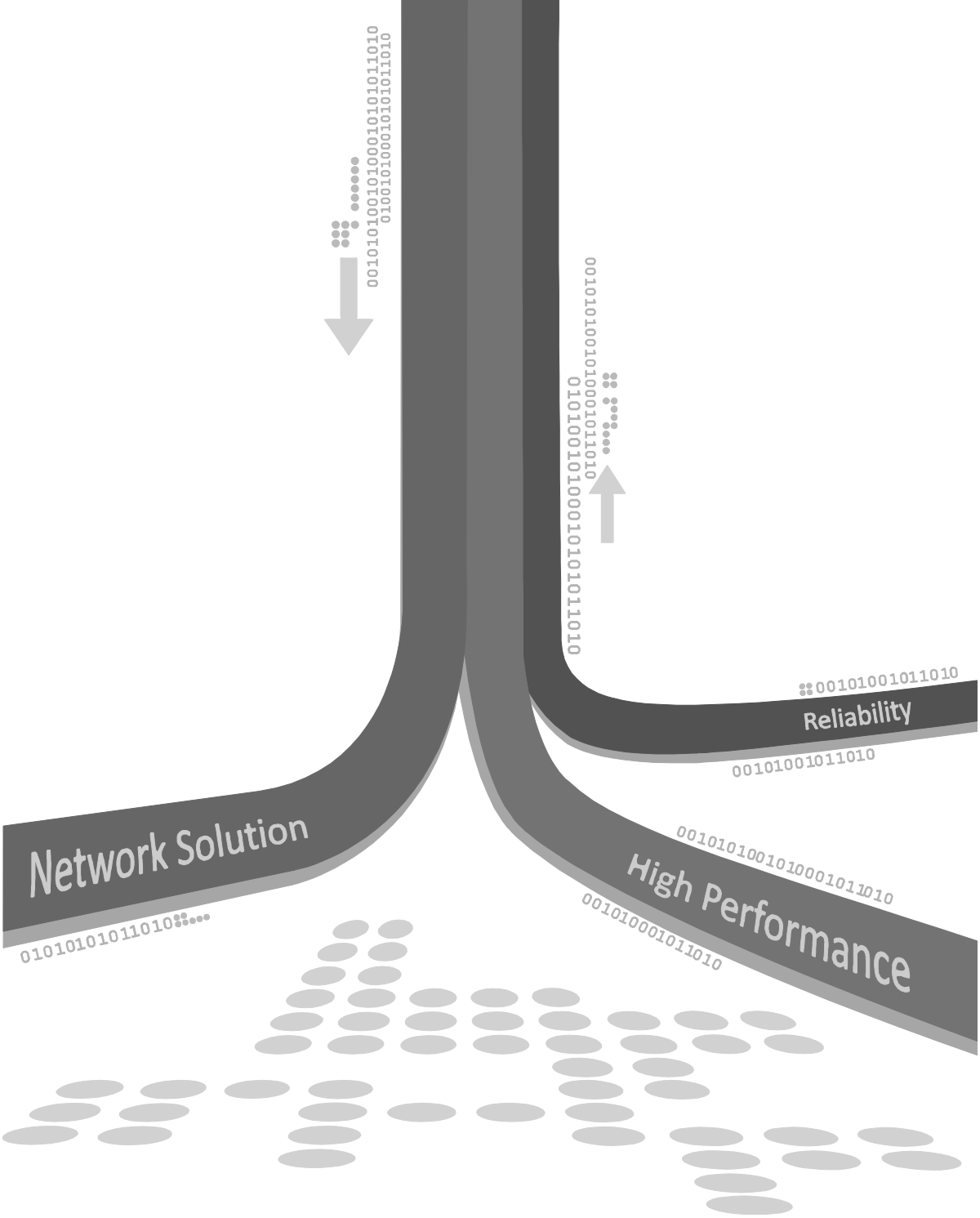
Custom engineering
so your equipment works exactly as you specify.

- Critical and expedited services
- In stock / Ready-to-ship
- Leasing / Rentals / Demos
- ITAR-certified secure asset solutions

Expert team | Trust guarantee | 100% satisfaction

All trademarks, brand names, and brands appearing herein are the property of their respective owners.

Visit our website - *Click HERE*



V5812G

GPON OLT system

User Manual

※ Copyright 2011 ⓒ DASAN Networks, Inc.

Issued by Technical Documentation Team
Korea

Technical modifications possible.
Technical specifications and features are binding only insofar as
they are specifically and expressly agreed upon in a written contract.

Contents of Update

Issue No. 1

Chapter/Section	Contents
All	Initial release

Issue History

Issue Number	Date	Update
01	May. 2011	Initial release (NOS version 4.80)

Contents

1 Introduction 25
1.1 Audience 25
1.2 Document Structure 25
1.3 Document Convention 26
1.4 Document Notation 26
1.5 Virus Protection 27
1.6 GPL/LGPL Warranty and Liability Exclusion 27

2 System Overview 29
2.1 System Features 30

3 Command Line Interface (CLI) 33
3.1 Configuration Mode 33
3.1.1 Privileged EXEC View Mode 34
3.1.2 Privileged EXEC Enable Mode 34
3.1.3 Global Configuration Mode 35
3.1.4 Bridge Configuration Mode 35
3.1.5 DHCP Pool Configuration Mode 36
3.1.6 DHCP Option Configuration Mode 36
3.1.7 DHCP Option 82 Configuration Mode 37
3.1.8 Interface Configuration Mode 37
3.1.9 Rule Configuration Mode 38
3.1.10 RMON Configuration Mode 38
3.1.11 Router Configuration Mode 39
3.1.12 Route-Map Configuration Mode 39
3.1.13 GPON Configuration Mode 40
3.1.13.1 GPON-OLT Configuration Mode 40
3.1.13.2 ONU Profile Configuration Mode 40
3.2 Configuration Mode Overview 41
3.3 Useful Tips 42
3.3.1 Listing Available Command 42
3.3.2 Calling Command History 44
3.3.3 Using Abbreviation 45
3.3.4 Using Command of Privileged EXEC Enable Mode 46
3.3.5 Exit Current Command Mode 46

4 System Connection and IP Address 47
4.1 System Connection 47
4.1.1 System Login 47
4.1.2 Password for Privileged EXEC Enable Mode 48
4.1.3 Changing Login Password 49
4.1.4 Management for System Account 49
4.1.4.1 Creating System Account 49
4.1.4.2 Security Level 50
4.1.5 Limiting Number of Users 54
4.1.6 Auto Log-out 54
4.1.7 Telnet Access 54
4.1.8 System Rebooting 55

4.1.8.1 Manual System Rebooting 55
4.1.9 Auto Reset Configuration 56
4.1.9.1 CPU Load 56
4.1.9.2 Memory 56
4.1.9.3 Network Connection 57
4.2 System Authentication 59
4.2.1 Authentication Method 59
4.2.2 Authentication Interface 59
4.2.3 Primary Authentication Method 60
4.2.4 RADIUS Server 60
4.2.4.1 RADIUS Server for System Authentication 60
4.2.4.2 RADIUS Server Priority 60
4.2.4.3 Timeout of Authentication Request 61
4.2.4.4 Frequency of Retransmit 61
4.2.5 TACACS+ Server 61
4.2.5.1 TACACS+ Server for System Authentication 61
4.2.5.2 TACACS+ Server Priority 61
4.2.5.3 Timeout of Authentication Request 62
4.2.5.4 Additional TACACS+ Configuration 62
4.2.6 Accounting Mode 63
4.2.7 Displaying System Authentication 63
4.3 Configuring Interface 64
4.3.1 Enabling Interface 64
4.3.2 Assigning IP Address to Network Interface 65
4.3.3 Static Route and Default Gateway 65
4.3.4 Interface Description 66
4.3.5 Displaying Interface 67
4.4 Secure Shell (SSH) 68
4.4.1 SSH Server 68
4.4.1.1 Enabling SSH Server 68
4.4.1.2 Displaying On-line SSH Client 68
4.4.1.3 Disconnecting SSH Client 68
4.4.1.4 Assigning Specific Authentication Key 69
4.4.1.5 Displaying Connection History of SSH Client 69
4.4.2 SSH Client 69
4.4.2.1 Login to SSH Server 69
4.4.2.2 Secured File Copy 69
4.4.2.3 Authentication Key 70
4.5 802.1x Authentication 71
4.5.1 802.1x Authentication 72
4.5.1.1 Enabling 802.1x 72
4.5.1.2 RADIUS Server 72
4.5.1.3 Authentication Mode 73
4.5.1.4 Authentication Port 74
4.5.1.5 Force Authorization 74
4.5.1.6 Interval for Retransmitting Request/Identity Packet 74
4.5.1.7 Number of Requests to RADIUS Server 74
4.5.1.8 Interval of Request to RADIUS Server 75
4.5.2 802.1x Re-Authentication 75
4.5.2.1 Enabling 802.1x Re-Authentication 75

4.5.2.2 Interval of Re-Authentication 76
4.5.2.3 Interval of Requesting Re-Authentication 76
4.5.2.4 802.1x Re-Authentication 76
4.5.3 Initializing Authentication Status 77
4.5.4 Restoring Default Value 77
4.5.5 Displaying 802.1x Configuration 77
4.5.6 802.1x User Authentication Statistics 77
4.5.7 Sample Configuration 78

5 Port Configuration 79
5.1 Port Basic 79
5.1.1 Selecting Port Type 79
5.2 Ethernet Port Configuration 79
5.2.1 Enabling Ethernet Port 79
5.2.2 Auto-Negotiation 80
5.2.3 Transmit Rate 80
5.2.4 Duplex Mode 81
5.2.5 Flow Control 81
5.2.6 Port Description 81
5.2.7 Traffic Statistics 82
5.2.7.1 Packet Statistics 82
5.2.7.2 CPU Statistics 82
5.2.7.3 Protocol Statistics 84
5.2.8 Port Information 84
5.3 Port Mirroring 85

6 System Environment 87
6.1 Environment Configuration 87
6.1.1 Host Name 87
6.1.2 Time and Date 87
6.1.3 Time Zone 88
6.1.4 Network Time Protocol (NTP) 89
6.1.5 Simple Network Time Protocol (SNTP) 89
6.1.6 Terminal Configuration 91
6.1.7 Login Banner 91
6.1.8 DNS Server 91
6.1.9 Fan Operation 92
6.1.10 Disabling Daemon Operation 92
6.1.11 FTP Server 93
6.1.12 FTP Bind Address 93
6.1.13 System Threshold 94
6.1.13.1 CPU Load 94
6.1.13.2 Port Traffic 94
6.1.13.3 Fan Operation 95
6.1.13.4 System Temperature 96
6.1.13.5 System Memory 96
6.1.13.6 System/SFP Module Operation 96
6.1.14 Enabling DDM 97
6.2 Configuration Management 98
6.2.1 Displaying System Configuration 98

6.2.2 Writing System Configuration 98
6.2.3 Auto-Saving....99
6.2.4 System Configuration File....99
6.2.5 Restoring Default Configuration....100
6.2.6 Core Dump File....101
6.3 System Management....102
6.3.1 Network Connection....102
6.3.2 IP ICMP Source Routing....104
6.3.3 Tracing Packet Route....105
6.3.4 Displaying User Connecting to System....106
6.3.5 MAC Table....107
6.3.6 System Running Time....107
6.3.7 System Information....107
6.3.8 System Memory Information....108
6.3.9 CPU Packet Limit....108
6.3.10 Running Process....108
6.3.11 Displaying System Software....109
6.3.12 Displaying Installed OS....109
6.3.13 Default OS....109
6.3.14 Switch Status....110
6.3.15 Tech Support Information....110
6.3.16 System Boot Information....110
6.3.17 Network Service Module (NSM) Daemon Debugging....111

7 Network Management....112
7.1 Simple Network Management Protocol (SNMP)....112
7.1.1 SNMP Community....112
7.1.2 Information of SNMP Agent....113
7.1.3 SNMP Com2sec....114
7.1.4 SNMP Group....114
7.1.5 SNMP View Record....115
7.1.6 Permission to Access SNMP View Record....115
7.1.7 SNMP Version 3 User....116
7.1.8 SNMP Trap....116
7.1.8.1 SNMP Trap Mode....116
7.1.8.2 SNMP Trap Host....117
7.1.8.3 Enabling SNMP Trap....117
7.1.8.4 Disabling SNMP Trap....119
7.1.8.5 Displaying SNMP Trap....119
7.1.9 SNMP Alarm....120
7.1.9.1 Alarm Notify Activity....120
7.1.9.2 Alarm Severity Criterion....120
7.1.9.3 Default Alarm Severity....121
7.1.9.4 Generic Alarm Severity....121
7.1.9.5 ADVA Alarm Severity....123
7.1.9.6 STP Guard Alarm Severity....124
7.1.9.7 Displaying SNMP Alarm....124
7.1.10 Displaying SNMP Configuration....124
7.1.11 Disabling SNMP....125
7.2 Operation, Administration and Maintenance (OAM)....125

7.2.1 Enabling OAM 126
7.2.2 OAM Link Monitoring 127
7.2.3 EFM OAM Mode 128
7.2.4 OAM Loopback 128
7.2.5 OAM Unidirection 129
7.2.6 Displaying EFM OAM Configuration 129
7.3 Link Layer Discovery Protocol (LLDP) 130
7.3.1 LLDP Operation 130
7.3.2 Enabling LLDP 130
7.3.3 LLDP Operation Type 130
7.3.4 Basic TLV 130
7.3.5 LLDP Message 131
7.3.6 Reinitiating Delay 131
7.3.7 Displaying LLDP Configuration 132
7.4 Remote Monitoring (RMON) 133
7.4.1 RMON History 133
7.4.1.1 Source Port of Statistical Data 134
7.4.1.2 Subject of RMON History 134
7.4.1.3 Number of Sample Data 134
7.4.1.4 Interval of Sample Inquiry 134
7.4.1.5 Activating RMON History 134
7.4.1.6 Deleting Configuration of RMON History 135
7.4.1.7 Displaying RMON History 135
7.4.2 RMON Alarm 135
7.4.2.1 Subject of RMON Alarm 136
7.4.2.2 Object of Sample Inquiry 136
7.4.2.3 Absolute and Delta Comparison 136
7.4.2.4 Upper Bound of Threshold 136
7.4.2.5 Lower Bound of Threshold 137
7.4.2.6 Standard of the First Alarm 137
7.4.2.7 Interval of Sample Inquiry 138
7.4.2.8 Activating RMON Alarm 138
7.4.2.9 Deleting Configuration of RMON Alarm 138
7.4.3 RMON Event 138
7.4.3.1 Event Community 139
7.4.3.2 Event Description 139
7.4.3.3 Subject of RMON Event 139
7.4.3.4 Event Type 139
7.4.3.5 Activating RMON Event 140
7.4.3.6 Deleting Configuration of RMON Event 140
7.5 Syslog 141
7.5.1 Syslog Output Level 141
7.5.2 Facility Code 143
7.5.3 Syslog Bind Address 144
7.5.4 Debug Message for Remote Terminal 144
7.5.5 Disabling Syslog 144
7.5.6 Displaying Syslog Message 145
7.5.7 Displaying Syslog Configuration 145
7.6 Rule and QoS 146
7.6.1 How to Operate QoS 147

7.6.2 Packet Classification 148
7.6.2.1 Flow Mode 149
7.6.2.2 Flow Creation 149
7.6.2.3 Configuring Flow 150
7.6.2.4 Applying and modifying Flow 152
7.6.2.5 Class Creation 152
7.6.3 Packet Conditioning 153
7.6.3.1 Policer Creation 153
7.6.3.2 Packet Counter 154
7.6.3.3 Rate-limit 154
7.6.3.4 Applying and modifying Policer 154
7.6.4 Rule Action 155
7.6.4.1 Policy Creation 155
7.6.4.2 Metering 156
7.6.4.3 Policy Priority 162
7.6.4.4 Policy Action 162
7.6.4.5 Setting CoS and ToS values 163
7.6.4.6 Attaching a Policy to an interface 163
7.6.4.7 Applying and Modifying Policy 164
7.6.5 Displaying Rule 164
7.6.6 Admin Rule 165
7.6.6.1 Creating Admin Flow for packet classification 165
7.6.6.2 Configuring Admin Flow 166
7.6.6.3 Applying and modifying Admin Flow 167
7.6.6.4 Class Creation 167
7.6.7 Admin Rule Action 168
7.6.7.1 Admin Policy Creation 168
7.6.7.2 Admin Policy Priority 169
7.6.7.3 Admin Policy Action 169
7.6.7.4 Applying and Modifying Admin Policy 170
7.6.8 Displaying Admin Rule 170
7.6.9 Scheduling 171
7.6.9.1 Scheduling mode 173
7.6.9.2 Weight and Quantum 173
7.6.9.3 Maximum and Minimum Bandwidth 174
7.6.9.4 Limiting traffic and buffer 174
7.6.9.5 The Traffic of Queue 175
7.6.9.6 Displaying QoS 175
7.7 NetBIOS Filtering 176
7.8 Martian Filtering 177
7.9 Max Host 178
7.10 Port Security 179
7.10.1 Port Security on Port 179
7.10.2 Port Security Aging 180
7.10.3 Displaying Port Security 181
7.11 Outband Management Port Security 181
7.12 MAC Table 181
7.13 MAC Filtering 183
7.13.1 Default MAC Filter Policy 183

7.13.2 Configuring MAC Filter Policy 183
7.13.3 Listing MAC Filter Policy 184
7.13.4 Displaying MAC Filter Policy 184
7.14 Address Resolution Protocol (ARP) 185
7.14.1 ARP Table 185
7.14.1.1 Registering ARP Table 185
7.14.1.2 ARP Log Interval 186
7.14.1.3 Displaying ARP Table 186
7.14.2 ARP Alias 186
7.14.3 ARP Inspection 187
7.14.3.1 ARP Access List 188
7.14.3.2 Enabling ARP Inspection Filtering 190
7.14.3.3 ARP Address Validation 190
7.14.3.4 ARP Inspection on Trust Port 191
7.14.3.5 ARP Inspection Log-buffer 191
7.14.3.6 Displaying ARP Inspection 192
7.14.4 Gratuitous ARP 193
7.14.5 Proxy ARP 193
7.15 ICMP Message Control 195
7.15.1 Blocking Echo Reply Message 195
7.15.2 Interval for Transmit ICMP Message 196
7.16 TCP Flag Control 197
7.16.1 RST Configuration 197
7.16.2 SYN Configuration 198
7.17 Packet Dump 198
7.17.1 Packet Dump by Protocol 198
7.17.2 Packet Dump with Option 199
7.17.3 Debug Packet Dump 200
7.17.4 Displaying Dump Packets 200
7.17.5 Dump File 200
7.18 Access List 202
7.18.1 Standard Access List 203
7.18.2 Extended Access List 204
7.18.3 Named Access List 206
7.18.4 Access List Range 207
7.18.5 Displaying Access List Entries 208

8 System Main Functions 209

8.1 Virtual Local Area Network (VLAN) 209
8.1.1 Port-based VLAN 210
8.1.1.1 Creating VLAN 211
8.1.1.2 Specifying PVID 211
8.1.1.3 Adding Port to VLAN 211
8.1.1.4 Deleting VLAN 211
8.1.2 Protocol-based VLAN 212
8.1.3 MAC-based VLAN 212
8.1.4 Subnet-based VLAN 213
8.1.5 Tagged VLAN 213
8.1.6 VLAN Description 214
8.1.7 VLAN Precedence 215

8.1.8 Displaying VLAN Information 215
8.1.9 QinQ 215
8.1.9.1 Double Tagging Operation 216
8.1.9.2 Double Tagging Configuration 217
8.1.9.3 TPID Configuration 217
8.1.10 Layer 2 Isolation 218
8.1.10.1 Port Isolation 218
8.1.10.2 Shared VLAN 219
8.1.11 VLAN Translation 221
8.1.12 Sample Configuration 221
8.2 Link Aggregation (LAG) 224
8.2.1 Port Trunk 224
8.2.1.1 Configuring Port Trunk 224
8.2.1.2 Disabling Port Trunk 225
8.2.1.3 Displaying Port Trunk 225
8.2.2 Link Aggregation Control Protocol (LACP) 225
8.2.2.1 Configuring LACP 226
8.2.2.2 Distribution Mode 226
8.2.2.3 Operation Mode 227
8.2.2.4 Priority of Switch 228
8.2.2.5 Manual Aggregation 228
8.2.2.6 BPDU Transmission Rate 229
8.2.2.7 Administrational Key 229
8.2.2.8 Port Priority 229
8.2.2.9 Displaying LACP Configuration 230
8.3 Spanning-Tree Protocol (STP) 231
8.3.1 STP Operation 232
8.3.2 RSTP Operation 235
8.3.3 MSTP Operation 240
8.3.4 Configuring STP/RSTP/MSTP/PVSTP/PVRSTP Mode (Required) 242
8.3.5 Configuring STP/RSTP/MSTP 242
8.3.5.1 Activating STP/RSTP/MSTP 242
8.3.5.2 Root Switch 242
8.3.5.3 Path-cost 243
8.3.5.4 Port-priority 244
8.3.5.5 MST Region 244
8.3.5.6 MSTP Protocol 245
8.3.5.7 Point-to-point MAC Parameters 245
8.3.5.8 Edge Ports 246
8.3.5.9 Displaying Configuration 246
8.3.6 Configuring PVSTP/PVRSTP 247
8.3.6.1 Activating PVSTP/PVRSTP 248
8.3.6.2 Root Switch 249
8.3.6.3 Path-cost 249
8.3.6.4 Port-priority 249
8.3.7 Root Guard 249
8.3.8 Restarting Protocol Migration 250
8.3.9 BPDU Configuration 251
8.3.9.1 Hello Time 251
8.3.9.2 Forward Delay 252

8.3.9.3 Max Age 252
8.3.9.4 BPDU Hop 252
8.3.9.5 BPDU Filter 253
8.3.9.6 BPDU Guard 253
8.3.9.7 Displaying BPDU Configuration 254
8.3.10 Sample Configuration 254
8.4 Ethernet Ring Protection (ERP) 257
8.4.1 ERP Mechanism 257
8.4.2 Loss of Test Packet (LOTP) 261
8.4.3 ERP Shared Link 261
8.4.4 Configuring ERP Domian 262
8.4.4.1 ERP Domain 262
8.4.4.2 ERP Domain Description 262
8.4.4.3 Node Mode 262
8.4.4.4 Primary and Secondary Port 262
8.4.5 Protected Activation 263
8.4.6 Primary/Secondary Port State 263
8.4.7 Learning Disable Time 263
8.4.8 Wait-to-Restore Time 264
8.4.9 Test Packet Interval 264
8.4.10 ERP Ring Priority 265
8.4.11 LOTP Hold Off Time 265
8.4.12 ERP Trap 266
8.4.13 Registering ERP MAC 266
8.4.14 Private VLAN with ERP 266
8.4.15 Displaying ERP Configuration 267
8.5 Loop Detection 268
8.6 Dynamic Host Configuration Protocol (DHCP) 270
8.6.1 DHCP Server 271
8.6.1.1 DHCP Pool Creation 272
8.6.1.2 DHCP Subnet 272
8.6.1.3 Range of IP Address 272
8.6.1.4 Default Gateway 273
8.6.1.5 IP Lease Time 273
8.6.1.6 DNS Server 274
8.6.1.7 Manual Binding 274
8.6.1.8 Domain Name 275
8.6.1.9 DHCP Server Option 275
8.6.1.10 Static Mapping 275
8.6.1.11 Recognition of DHCP Client 276
8.6.1.12 IP Address Validation 276
8.6.1.13 Authorized ARP 276
8.6.1.14 Prohibition of 1:N IP Address Assignment 277
8.6.1.15 Ignoring BOOTP Request 278
8.6.1.16 DHCP Packet Statistics 278
8.6.1.17 Setting DHCP Pool Size 279
8.6.1.18 Displaying DHCP Pool Configuration 279
8.6.2 DHCP Address Allocation with Option 82 280
8.6.2.1 DHCP Class Capability 280
8.6.2.2 DHCP Class Creation 280

8.6.2.3 Relay Agent Information Pattern 280
8.6.2.4 Associating DHCP Class 281
8.6.2.5 Range of IP Address for DHCP Class 281
8.6.3 DHCP Lease Database 282
8.6.3.1 DHCP Database Agent 282
8.6.3.2 Displaying DHCP Lease Status 282
8.6.3.3 Deleting DHCP Lease Database 283
8.6.4 DHCP Relay Agent 283
8.6.4.1 DHCP Helper Address 284
8.6.4.2 Smart Relay Agent Forwarding 284
8.6.4.3 DHCP Server ID Option 285
8.6.4.4 DHCP Relay Statistics 285
8.6.5 DHCP Option 286
8.6.5.1 Entering DHCP Option Mode 286
8.6.5.2 Configuring DHCP Option Format 287
8.6.5.3 Deleting DHCP Option Format 287
8.6.5.4 Displaying DHCP option 287
8.6.6 DHCP Option 82 288
8.6.6.1 Enabling DHCP Option 82 289
8.6.6.2 Option 82 Sub-Option 289
8.6.6.3 Option 82 Reforwarding Policy 290
8.6.6.4 Option 82 Trust Policy 291
8.6.7 DHCP Snooping 291
8.6.7.1 Enabling DHCP Snooping 292
8.6.7.2 DHCP Trust State 292
8.6.7.3 DHCP Filter on Trust Port 293
8.6.7.4 DHCP Rate Limit 293
8.6.7.5 DHCP Lease Limit 294
8.6.7.6 Source MAC Address Verification 295
8.6.7.7 Static DHCP Snooping Binding 295
8.6.7.8 DHCP Snooping Database Agent 295
8.6.7.9 ARP Inspection Start Time 296
8.6.7.10 DHCP Snooping with Option82 296
8.6.7.11 DHCP Snooping Option 297
8.6.7.12 Displaying DHCP Snooping Configuration 298
8.6.8 IP Source Guard 298
8.6.8.1 Enabling IP Source Guard 299
8.6.8.2 Static IP Source Binding 300
8.6.8.3 Displaying IP Source Guard Configuration 300
8.6.9 DHCP Client 300
8.6.9.1 Enabling DHCP Client 300
8.6.9.2 DHCP Client ID 300
8.6.9.3 DHCP Class ID 301
8.6.9.4 Host Name 301
8.6.9.5 IP Lease Time 301
8.6.9.6 Requesting Option 301
8.6.9.7 Forcing Release or Renewal of DHCP Lease 301
8.6.9.8 Displaying DHCP Client Configuration 302
8.6.10 DHCP Filtering 302
8.6.10.1 DHCP Packet Filtering 302
8.6.10.2 DHCP Server Packet Filtering 303

8.6.11 Debugging DHCP 304
8.7 Virtual Router Redundancy Protocol (VRRP) 305
8.7.1 Configuring VRRP 306
8.7.1.1 Associated IP Address 306
8.7.1.2 Access to Associated IP Address 306
8.7.1.3 Master Router and Backup Router 306
8.7.1.4 VRRP Track Function 309
8.7.1.5 Authentication Password 311
8.7.1.6 Preempt 311
8.7.2 VRRP Monitoring and Management 312
8.7.2.1 Displaying VRRP Protocol Information 312
8.7.2.2 VRRP Statistics 312
8.7.2.3 VRRP Debug 313
8.8 Single IP Management 314
8.8.1 Switch Group 314
8.8.2 Designating Master and Slave Switch 315
8.8.3 Disabling Cascading 315
8.8.4 Displaying Cascading Status 315
8.8.5 Accessing to Slave Switch from Master Switch 316
8.8.6 Sample Configuration 316
8.9 Rate Limit 318
8.10 Flood Guard 319
8.10.1 MAC Flood Guard 319
8.10.2 CPU Flood Guard 320
8.10.3 System Flood Guard 320
8.11 PPS Control 322
8.12 Storm Control 323
8.13 Jumbo Frame Capacity 323
8.14 Bandwidth 324
8.15 Maximum Transmission Unit (MTU) 324
8.16 Blocking Packet Forwarding 324

9 IP Multicast 325

9.1 Multicast Group Membership 327
9.1.1 IGMP Basic 327
9.1.1.1 IGMP Version 328
9.1.1.2 Querier's Robustness Variable 328
9.1.1.3 Clearing IGMP Entry 328
9.1.1.4 IGMP Debug 329
9.1.2 IGMP Version 2 329
9.1.2.1 IGMP Static Join 330
9.1.2.2 IGMP Access Control 332
9.1.2.3 IGMP Querier Configuration 332
9.1.2.4 IGMP Immediate Leave 334
9.1.3 IGMP Version 3 335
9.1.4 Displaying IGMP Information 336
9.2 Multicast Functions 337
9.2.1 Multicast Forwarding Database 337
9.2.1.1 Blocking Unknown Multicast Traffic 337

9.2.1.2 Forwarding Entry Aging 338
9.2.1.3 Displaying McFDB Information 338
9.2.2 IGMP Snooping Basic 339
9.2.2.1 Enabling IGMP Snooping 340
9.2.2.2 IGMP Snooping Version 340
9.2.2.3 IGMP Snooping Robustness Value 341
9.2.3 IGMPv2 Snooping 341
9.2.3.1 IGMP Snooping Querier Configuration 341
9.2.3.2 IGMP Snooping Last Member Query Interval 343
9.2.3.3 IGMP Snooping Immediate Leave 344
9.2.3.4 IGMP Snooping Report Suppression 345
9.2.3.5 IGMP Snooping S-Query Report Agency 345
9.2.3.6 Explicit Host Tracking 346
9.2.3.7 Multicast Router Port Configuration 347
9.2.3.8 TCN Multicast Flooding 349
9.2.4 IGMPv3 Snooping 351
9.2.5 Displaying IGMP Snooping Information 351
9.2.6 Multicast VLAN Registration (MVR) 353
9.2.6.1 Enabling MVR 353
9.2.6.2 MVR Group 353
9.2.6.3 Source/Receiver Port 354
9.2.6.4 MVR Helper Address 354
9.2.6.5 Displaying MVR Configuration 354
9.2.7 IGMP Filtering and Throttling 355
9.2.7.1 IGMP Filtering 355
9.2.7.2 IGMP Throttling 357
9.2.7.3 Displaying IGMP Filtering and Throttling 357
9.2.8 IGMP Proxy 358
9.2.8.1 Designating Downstream Interface 358
9.2.8.2 Designating Upstream Interface 358
9.2.8.3 Configuring Upstream Interface Mode 359
9.2.8.4 IGMP-Proxy IF Flap Discredit 359
9.2.8.5 Disabling Verification of Source IP of IGMP Packets 361
9.2.8.6 Specifying IGMP Report/Leave's Source IP Address 361
9.2.8.7 Querying with Real Querirer's Source IP Address 362
9.2.8.8 Displaying IGMP Proxy Information 362
9.2.9 IGMP State Limit 362
9.2.10 Multicast-Source Trust Port 363
9.3 Multicast Routing 364
9.3.1 Multicast Routing 364
9.3.1.1 Enabling Multicast Routing 364
9.3.1.2 TTL Threshold 364
9.3.1.3 ECMP Load Splitting 365
9.3.1.4 MRIB Entry Limit 365
9.3.1.5 Displaying MRIB Entry 366
9.3.1.6 Displaying MRIB Statistics 367
9.3.1.7 Displaying MFIB Information 367
9.3.1.8 MRIB Debug 368
9.3.2 PIM Basic 368
9.3.2.1 PIM Mode 369
9.3.2.2 DR Priority 369

9.3.2.3 Neighbor Filtering 370
9.3.2.4 PIM Join/Prune Message Group Filtering 371
9.3.2.5 PIM Hello Message 371
9.3.2.6 PIM Join/Prune Interval 372
9.3.2.7 PIM VIF Flap Discredit 372
9.3.2.8 PIM Static Join 373
9.3.2.9 Displaying PIM Information 373
9.3.3 PIM-SM 374
9.3.3.1 Rendezvous Point 376
9.3.3.2 Bootstrap Router 378
9.3.3.3 Source Registration 379
9.3.3.4 SPT Switchover 381
9.3.3.5 Cisco's Router Interoperability 382
9.3.3.6 PIM Debug 383
9.3.4 Source Specific Multicast (SSM) 384
9.3.4.1 PIM-SSM 384
9.3.4.2 Static SSM Mapping 385

10 IP Routing Protocol 387
10.1 Border Gateway Protocol (BGP) 387
10.1.1 Basic Configuration 388
10.1.1.1 Configuration Type of BGP 388
10.1.1.2 Enabling BGP Routing 388
10.1.1.3 Disabling BGP Routing 389
10.1.2 Advanced Configuration 389
10.1.2.1 Summary of Path 389
10.1.2.2 Automatic Summarization of Path 390
10.1.2.3 BGP Next-Hop Address Tracking 390
10.1.2.4 Local Preference 391
10.1.2.5 Multi-Exit Discriminator (MED) 391
10.1.2.6 Choosing Best Path 392
10.1.2.7 Graceful Restart 393
10.1.3 Administrative Distance for BGP 394
10.1.4 IP Address Family 395
10.1.5 BGP Neighbor 395
10.1.5.1 Default Route 395
10.1.5.2 Peer Group 396
10.1.5.3 Route Map 397
10.1.5.4 Force Shutdown 397
10.1.5.5 Changing the Nexthop Information 397
10.1.5.6 Neighbor Password 398
10.1.5.7 Neighbor Description 398
10.1.5.8 Source of Routing Updates 398
10.1.5.9 Updates for Inbound Soft Reconfiguration 399
10.1.6 BGP Timers 399
10.1.7 Route Flap Dampening 399
10.1.8 BGP Session Reset 401
10.1.8.1 Session Reset of All Peers 401
10.1.8.2 Session Reset of Peers within Particular AS 402
10.1.8.3 Session Reset of Specific Route 403
10.1.8.4 Session Reset of External Peer 403

10.1.8.5 Session Reset of Peer Group....404
10.1.9 Displaying and Managing BGP....405
10.1.9.1 BGP Neighbor....405
10.1.9.2 Logging Neighbor Changes....406
10.1.9.3 Checking the BGP Network Route....406
10.1.9.4 Sending SNMP Trap....406
10.1.10 BGP Debug....407
10.2 Open Shortest Path First (OSPF)....408
10.2.1 Enabling OSPF....408
10.2.2 ABR Type Configuration....410
10.2.3 Compatibility Support....410
10.2.4 OSPF Interface....410
10.2.4.1 Authentication Type....410
10.2.4.2 Authentication Key....411
10.2.4.3 Interface Cost....412
10.2.4.4 Blocking Transmission of Route Information Database....412
10.2.4.5 Routing Protocol Interval....413
10.2.4.6 OSPF Maximum Transmission Unit (MTU)....414
10.2.4.7 OSPF Priority....415
10.2.4.8 OSPF Network Type....415
10.2.5 Non-Broadcast Network....416
10.2.6 OSPF Area....417
10.2.6.1 Area Authentication....417
10.2.6.2 Default Cost of Area....417
10.2.6.3 Blocking the Transmission of Routing Information Between Area....418
10.2.6.4 Not So Stubby Area (NSSA)....419
10.2.6.5 Area Range....422
10.2.6.6 Shortcut Area....422
10.2.6.7 Stub Area....423
10.2.6.8 Maximum Area....423
10.2.6.9 Virtual Link....423
10.2.7 Default Metric....426
10.2.8 Graceful Restart Support....426
10.2.9 Opaque-LSA Support....427
10.2.10 Default Route....428
10.2.11 Finding Period....429
10.2.12 External Routes to OSPF Network....429
10.2.13 OSPF Distance....431
10.2.14 Host Route....431
10.2.15 Passive Interface....432
10.2.16 Blocking Routing Information....432
10.2.17 Summary Routing Information....433
10.2.18 OSPF Monitoring and Management....433
10.2.18.1 Displaying OSPF Protocol Information....433
10.2.18.2 Sending SNMP Trap....435
10.2.18.3 Logging Neighbor Changes....435
10.2.18.4 Limiting Number of Database....436
10.2.18.5 Maximum Process of LSA....436
10.2.19 OSPF Debug....437
10.3 Routing Information Protocol (RIP)....439

10.3.1 Enabling RIP 439
10.3.2 RIP Neighbor Router 440
10.3.3 RIP Version 441
10.3.4 Creating available Static Route only for RIP 442
10.3.5 Redistributing Routing Information 442
10.3.6 Metrics for Redistributed Routes 444
10.3.7 Administrative Distance 444
10.3.8 Originating Default Information 445
10.3.9 Routing Information Filtering 445
10.3.9.1 Filtering Access List and Prefix List 445
10.3.9.2 Disabling the transmission to Interface 446
10.3.9.3 Offset List 446
10.3.10 Maximum Number of RIP Routes 447
10.3.11 RIP Network Timer 447
10.3.12 Split Horizon 447
10.3.13 Authentication Key 448
10.3.14 Restarting RIP 449
10.3.15 UDP Buffer Size of RIP 449
10.3.16 Monitoring and Managing RIP 449
10.3.16.1 Displaying RIP Protocol Information 450
10.3.16.2 Displaying Debugging Information 450

11 GPON Configuration 452
11.1 OLT Management 454
11.1.1 Opening OLT Mode 454
11.1.1.1 OLT Description 455
11.1.1.2 Activating OLT 455
11.1.2 Downstream Encryption 455
11.1.3 OLT Bandwidth 456
11.1.3.1 Upstream Bandwidth 456
11.1.3.2 Bandwidth Scheduler 456
11.1.4 OLT Optical Transceiver Parameter 457
11.1.5 Auto ONU Fault Detection 457
11.1.6 Maximal Distance between OLT and ONU (ONT) 458
11.1.7 Forward Error Correction (FEC) Mode 458
11.1.8 MAC Aging Time 459
11.1.9 OLT Link Down Detection 459
11.1.10 Maximum Number of ONU 460
11.1.11 OLT Anti-Spoofing 460
11.1.12 Displaying OLT Information 461
11.1.12.1 OLT Traffic Statistics 461
11.1.12.2 MAC Address 463
11.1.12.3 OLT Slot Information 463
11.1.12.4 GPON Daemon Memory Usage 463
11.1.12.5 OLT Rx Power 464
11.2 ONU Management 465
11.2.1 ONU Registration 465
11.2.1.1 Activating/deactivating ONU 465
11.2.1.2 Serial Number-based ONU (ONT) Registration 465
11.2.1.3 Manual ONU (ONT) Registration Mode 466
11.2.1.4 ONU Registration Mode 466

11.2.1.5 Changing ONU Registration Mode 467
11.2.1.6 ONU Description 467
11.2.2 Assigning IP address 467
11.2.3 Activating Administration for UNI 468
11.2.4 ONU Reset 468
11.2.5 Forward Error Correction (FEC) Mode 468
11.2.6 Loopback 469
11.2.7 ONU Laser Down 469
11.2.8 Source MAC address Monitoring 470
11.2.9 POTS Interface Configuration 471
11.2.10 ONU Firmware Upgrade 472
11.2.10.1 Manual Upgrade (1) 472
11.2.10.2 Manual Upgrade (2) 474
11.2.10.3 Auto Upgrade 476
11.2.11 Displaying ONU Information 482
11.3 ONU Profile 485
11.3.1 Creating ONU Profile 485
11.3.2 Configuring ONU Profile 486
11.3.2.1 RX Optical Power Threshold 486
11.3.2.2 Rogue ONU 486
11.3.2.3 Card Type Configuration 487
11.3.2.4 Applying Traffic & PM Profile 488
11.3.3 Overwriting Traffic Profile Configuration 488
11.3.3.1 VLAN Configurations 489
11.3.3.2 Max Host 489
11.3.3.3 Rate Limit 489
11.3.3.4 IGMP Group List 490
11.3.3.5 Activating Administration for Ethernet UNI 490
11.3.3.6 Mapping between T-CONT ID and DBA profile 490
11.3.4 Saving Profile 490
11.3.5 Applying ONU Profile 491
11.3.6 Checking ONU Profile Configuration 491
11.3.7 Displaying ONU profile 491
11.4 DBA Profile 493
11.4.1 Creating DBA Profile 493
11.4.2 Configuring DBA Profile 493
11.4.3 Saving DBA Profile 494
11.4.4 Displaying DBA Profile 494
11.5 Traffic Profile 495
11.5.1 Creating Traffic Profile 495
11.5.2 Creating a Mapper 496
11.5.3 MAC Bridge Service Profile 497
11.5.3.1 Max Host 497
11.5.3.2 MAC Learning 497
11.5.3.3 Multicast Interworking Termination Point 497
11.5.3.4 ANI Port Configuration 498
11.5.3.5 UNI Port Configuration 498
11.5.3.6 IP-host Service Link 501
11.5.3.7 TDM Service Link 501
11.5.4 T-CONT Mode 502

11.5.4.1 GEM Port Configuration 503
11.5.4.2 Displaying T-CONT Information 503
11.5.5 IP Host Service Configuration 503
11.5.5.1 IP Address 504
11.5.5.2 DNS 504
11.5.5.3 VLAN Tagging Operating 504
11.5.5.4 VLAN Tagging Filtering 505
11.5.5.5 VoIP Service Link 505
11.5.5.6 TDM Service Link 505
11.5.6 VoIP Service Configuration (POTS UNI) 506
11.5.6.1 VoIP Service Management Mode 506
11.5.6.2 OMCI Managed VoIP 507
11.5.6.3 IP-path Managed VoIP 507
11.5.6.4 POTS UNI Configuration 508
11.5.6.5 UDP/TOS Configuration 509
11.5.7 TDM Service Configuration (CES UNI) 510
11.5.7.1 Expected Circuit Pack Type 510
11.5.7.2 Framing Structure 510
11.5.7.3 Encoding 511
11.5.7.4 Line Length 511
11.5.7.5 DS1 Mode 512
11.5.7.6 Line Type 512
11.5.7.7 TDM Service Configuration 512
11.5.7.8 Displaying TDM Pseudowire Information 513
11.5.8 Saving Traffic Profile 514
11.5.9 Adding/Applying Traffic Profile 514
11.5.10 Displaying Traffic Profile Information 515
11.5.11 Sample Configuration 515
11.6 VoIP Profile 516
11.6.1 OMCI Management Configuration 516
11.6.1.1 Creating VoIP Profile 516
11.6.1.2 VoIP Media Configuration 517
11.6.1.3 Voice Service Configuration 517
11.6.1.4 RTP Configuration 518
11.6.1.5 Signalling Code 519
11.6.1.6 DTMF Digit Configuration 520
11.6.1.7 Hook Flash Time Configuration 520
11.6.2 OMCI-based SIP Configuration 520
11.6.2.1 SIP Agent Configuration 521
11.6.2.2 VoIP Application Service 523
11.6.2.3 VoIP Feature Access Codes 524
11.6.2.4 SIP User Data 525
11.6.2.5 Network Dial Plan 526
11.6.3 Saving VoIP Profile 527
11.6.4 Displaying VoIP Information 527
11.6.5 Sample Configuration 528
11.7 TDM Pseudowire Profile 529
11.7.1 Creating TDM Pseudowire Profile 529
11.7.2 Basic Service Type 530
11.7.3 Signalling 530

11.7.4 Payload Size 530
11.7.5 Payload Encapsulation Delay 531
11.7.6 Timing Mode 531
11.7.7 RTP Pseudowire Parameter 531
11.7.7.1 Clock Reference 532
11.7.7.2 RTP Time Stamp Mode 532
11.7.7.3 RTP Payload Type 532
11.7.7.4 RTP Synchronization Source 533
11.7.8 Pseudowire Maintenance Configuration 533
11.7.9 Saving TDM Pseudowire Profile 533
11.7.10 Displaying TDM Pseudowire Information 534
11.8 Pseudowire Maintenance Profile 535
11.8.1 Creating Pseudowire Maintenance Profile 535
11.8.2 Jitter Buffer Maximum Depth 535
11.8.3 Jitter Buffer Desired Depth 536
11.8.4 Fill Policy 536
11.8.5 Alarm-related Policy 537
11.8.6 L-bit/R-bit Receive/Transmit Policy 538
11.8.7 SES Threshold 538
11.8.8 Saving Pseudowire Maintenance Profile 539
11.8.9 Displaying Pseudowire Maintenance Information 539
11.9 Performance Monitoring (PM) Profile 540
11.9.1 Creating PM Profile 540
11.9.2 Collecting ONU Traffic Statistics 540
11.9.3 Saving PM Profile 542
11.9.4 Displaying PM Profile Information 542
11.9.5 Displaying ONU Traffic Statistics 542
11.9.6 Sample Configuration 543
11.10 Multicast Profile 543
11.10.1 Creating Multicast Profile 543
11.10.2 IGMP Configurations 544
11.10.3 Saving Multicast Profile 545
11.10.4 Applying Multicast Profile 545
11.10.5 Displaying Multicast Information 546
11.11 ONU Service Profile 547
11.12 GPON Debug 548
11.13 Sample Configuration 549

12 System Software Upgrade 553

12.1 General Upgrade 553
12.2 Boot Mode Upgrade 554
12.3 FTP Upgrade 557
12.4 ONU Upgrade 559
12.4.1 Manual Upgrade 559
12.4.2 Auto Upgrade 560

13 Abbreviations 562

Illustrations

Fig. 2.1 V5812G 29
Fig. 3.1 Overview of Configuration Mode 41
Fig. 4.1 Process of 802.1x Authentication 71
Fig. 4.2 Multiple Authentication Servers 72
Fig. 5.1 Port Mirroring 85
Fig. 6.1 Ping Test for Network Status 104
Fig. 6.2 IP Source Routing 105
Fig. 7.1 EFM OAM Deployment Scenario 125
Fig. 7.2 Procedure of QoS operation 147
Fig. 7.3 Structure of Rule 148
Fig. 7.4 Token Bucket Meter 157
Fig. 7.5 Behavior of srTCM (1) 158
Fig. 7.6 Behavior of srTCM (2) 158
Fig. 7.7 Bahavior of srTCM (3) 159
Fig. 7.8 Behavior of trTCM (1) 160
Fig. 7.9 Behavior of trTCM (2) 160
Fig. 7.10 Behavior of trTCM (3) 161
Fig. 7.11 Strict Priority Queuing 171
Fig. 7.12 Deficit Round Robin 172
Fig. 7.13 Weighted Round Robin 172
Fig. 7.14 NetBIOS Filtering 176
Fig. 7.15 Proxy ARP 194
Fig. 7.16 ICMP Message Structure 195
Fig. 8.1 Port-based VLAN 210
Fig. 8.2 Subnet-based VLAN 213
Fig. 8.3 Example of QinQ Configuration 215
Fig. 8.4 QinQ Frame 216
Fig. 8.5 Outgoing Packets under Layer 2 Shared VLAN Environment 219
Fig. 8.6 Incoming Packets under Layer 2 Shared VLAN Environment (1) 220
Fig. 8.7 Incoming Packets under Layer 2 Shared VLAN Environment (2) 220
Fig. 8.8 Link Aggregation 224
Fig. 8.9 Example of Loop 231
Fig. 8.10 Principle of Spanning Tree Protocol 231
Fig. 8.11 Root Switch 232
Fig. 8.12 Designated Switch 233
Fig. 8.13 Port Priority 234
Fig. 8.14 Port State 234
Fig. 8.15 Alternate Port and Backup Port 236
Fig. 8.16 Example of Receiving Low BPDU 237
Fig. 8.17 Network Convergence of 802.1d 237
Fig. 8.18 Network Convergence of 802.1w (1) 238
Fig. 8.19 Network Convergence of 802.1w (2) 238
Fig. 8.20 Network Convergence of 802.1w (3) 239
Fig. 8.21 Compatibility with 802.1d (1) 239
Fig. 8.22 Compatibility with 802.1d (2) 240
Fig. 8.23 CST and IST of MSTP (1) 241
Fig. 8.24 CST and IST of MSTP (2) 241
Fig. 8.25 Example of PVSTP 248
Fig. 8.26 Root Guard 250

Fig. 8.27 Example of Layer 2 Network Design in RSTP Environment....255
Fig. 8.28 Example of Layer 2 Network Design in MSTP Environment....256
Fig. 8.29 ERP Operation in case of Link Failure....259
Fig. 8.30 Ring Protection....259
Fig. 8.31 Link Failure Recovery....260
Fig. 8.32 Ring Recovery....260
Fig. 8.33 Shared Link....261
Fig. 8.34 DHCP Service Structure....270
Fig. 8.35 Example of DHCP Relay Agent....283
Fig. 8.36 DHCP Option 82 Operation....289
Fig. 8.37 DHCP Server Packet Filtering....303
Fig. 8.38 VRRP Operation....305
Fig. 8.39 VRRP Track....310
Fig. 8.40 Example of Cascading....314
Fig. 8.41 Rate Limit and Flood Guard....319
Fig. 9.1 The V5812G with IGMP Snooping....325
Fig. 9.2 The V5812G with PIM-SM....326
Fig. 9.3 The Switch with IGMP Snooping and PIM-SM....326
Fig. 9.4 IGMP Snooping....339
Fig. 9.5 Multicast Equal Cost Multipath (ECMP)....365
Fig. 9.6 Rendezvous Point Tree....374
Fig. 9.7 Shortest Path Tree....375
Fig. 11.1 Example of GPON Network....452
Fig. 11.2 CLI Structure of *GPON Configuration* Mode....453
Fig. 11.3 ONU Profile....485
Fig. 11.4 Traffic Profile....495
Fig. 11.5 Priority of T-CONT types....502
Fig. 11.6 VoIP Service Architecture....506

Tables

Tab. 1.1 Overview of Chapters 25
Tab. 1.2 Command Notation of Guide Book 26
Tab. 3.1 Main Command of *Privileged EXEC View* Mode 34
Tab. 3.2 Main Command of *Privileged EXEC Enable* Mode 34
Tab. 3.3 Main Command of *Global Configuration* Mode 35
Tab. 3.4 Main Command of *Bridge Configuration* Mode 36
Tab. 3.5 Main Command of *DHCP Pool Configuration* Mode 36
Tab. 3.6 Main Command of *DHCP Option Configuration* Mode 37
Tab. 3.7 Main Command of *DHCP Option 82 Configuration* Mode 37
Tab. 3.8 Main Command of *Interface Configuration* Mode 38
Tab. 3.9 Main Command of *Rule Configuration* Mode 38
Tab. 3.10 Main Command of *RMON Configuration* Mode 39
Tab. 3.11 Main Command of *Router Configuration* Mode 39
Tab. 3.12 Main Command of *Route-map Configuration* Mode 40
Tab. 3.13 Main Command of *GPON-OLT Configuration* Mode 40
Tab. 3.14 Main Command of *ONU Profile Configuration* Mode 41
Tab. 3.15 Command Abbreviation 45
Tab. 6.1 World Time Zone 88
Tab. 6.2 Options for Ping for Multiple IP Addresses 103
Tab. 6.3 Options for Tracing Packet Route 106
Tab. 7.1 ICMP Message Type 195
Tab. 7.2 Mask Calculation of Default Value 197
Tab. 7.3 Examples of Wildcard Masking 203
Tab. 8.1 Advantages and Disadvantages of Tagged VLAN 214
Tab. 8.2 STP Path-cost 243
Tab. 8.3 RSTP Path-cost 243

1 Introduction

1.1 Audience

This manual is intended for V5812G 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.

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 V5812G 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.
10 IP Routing Protocol	Describes how to configure the IP routing protocols.
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

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.
PORTS	For entry this variable, see Section 5.1.
[ ]	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.

1.6 GPL/LGPL Warranty and Liability Exclusion

The Dasan Networks product, V5812G, contains both proprietary software and “Open Source Software”. The Open Source Software is licensed to you at no charge under the GNU General Public License (GPL) and the GNU Lesser General Public License (LGPL). This Open Source Software was written by third parties and enjoys copyright protection. You are entitled to use this Open Source Software under the conditions set out in the GPL and LGPL licenses indicated above. In the event of conflicts between Dasan Networks license conditions and the GPL or LGPL license conditions, the GPL and LGPL conditions shall prevail with respect to the Open Source portions of the software.

The GPL can be found under the following URL:
http://www.gnu.org/copyleft/gpl.html

The LGPL can be found under the following URL:
http://www.gnu.org/copyleft/lgpl.html

In addition, if the source code to the Open Source Software has not been delivered with this product, you may obtain the source code (including the related copyright notices) by sending your request to the following e-mail address: opensrc@dasannetworks.com.

You will, however, be required to reimburse Dasan Networks for its costs of postage and copying. Any source code request made by you must be sent within 3 years of your purchase of the product. Please include a copy of your sales receipt when submitting your request. Also please include the exact name and number of the devices and the version number of the installed software.

The use of Open Source Software contained in this product in any manner other than the simple running of the program occurs at your own risk, that is, without any warranty claims against Dasan Networks. For more information about the warranties provided by the authors of the Open Source Software contained in this product, please consult the GPL and LGPL.

You have no warranty claims against Dasan Networks when a defect in the product is or could have been caused by changes made by you in any part of the software or its configuration. In addition, you have no warranty claims against Dasan Networks when the Open Source Software infringes the intellectual property rights of a third party.

Dasan Networks provides no technical support for either the software or the Open Source Software contained therein if either has been changed.

2 System Overview

The Gigabit passive optical network (GPON) is the ideal solution for the bottleneck of Ethernet in the first mile, providing voice, data, and video solutions.

V5812G is a compact GPON Optical Line Terminal (OLT) that is comprised of GPON OLT 4-port modules with SFP GPON OLT transceiver. Up to four GPON links can be serviced through the development system's 8 Gigabit Ethernet interfaces as combo uplink ports. You can use an uplink interface as an optical (1000Base-X, SFP) port or electrical (10/100/1000Base-T, RJ45) port depending on the type of network it connected to.

With performance of a non-blocking switching capacity of up to 36 Gbps switching capacity and 26.8 Mpps throughput, the V5812G provides high speed networking environment.

For GPON, the PON layer is terminated on the interface unit and translated to Ethernet uplink to be transported through an Ethernet/IP environment. For improved system reliability, it adopts the design of redundancy architecture with dual power supplies.

The power feeding of the V5812G is provided by Power Supply Unit (PSU). Dual PSUs can be installed to guarantee constant system running. If power A's input fails, the system can be automatically switched to the other power B's input and normal operations of the system are not affected.

Fig. 2.1 shows the product view of the V5812G.



Fig. 2.1 V5812G

2.1 System Features

This section introduces the main features of the V5812G 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 V5812G recognizes 802.1Q tagged frame and supports maximum 4096 VLANs. Port-based, protocol-based, MAC-based, and subnet-based VLANs are supported in the V5812G.

Quality of Service (QoS)

For the V5812G, 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 V5812G 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 V5812G provides IGMPv2, IGMP snooping and PIM-SM for host membership management and multicast routing.

SNMP

Simple Network Management Protocol (SNMP) is to manage network elements using TCP/IP protocol. The V5812G supports SNMPv1, 2, 3 and Remote Monitoring (RMON). Network operator can use MIB also to monitor and manage the V5812G.

IP Routing

The V5812G is Layer 3 switch, which has routing table and IP address as router. Therefore, it supports static routing, RIPv1/v2, OSPFv2 and BGPv4 for unicast routing.

Dynamic Host Configuration Protocol (DHCP)

The V5812G 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 V5812G 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 V5812G supports Multiple Spanning Tree Protocol (MSTP) IEEE 802.1s.

Link Aggregation (Trunking)

The V5812G 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 V5812G can configure maximum 8 aggregate ports and up to 6 trunk groups.

Link Aggregation Control Protocol (LACP)

The V5812G 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 V5812G 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 V5812G 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 V5812G 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.

3 Command Line Interface (CLI)

The V5812G enables system administrators to manage the V5812G 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 V5812G 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 V5812G connects inband to the cascading switch, and then from the cascading switch to the management network through the outband interface.

The V5812G also provides the RS232 console interface to simply access the system with a provided RJ45-to-DB9 cable.

This chapter describes a basic instruction for using the command line interface (CLI) which is used for managing the V5812G system.

- Configuration Mode
- Configuration Mode Overview
- Useful Tips

3.1 Configuration Mode

You can configure and manage the V5812G 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
- Router Configuration Mode
- Route-Map 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

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.
route-map	Opens *Route-map Configuration* mode.
snmp	Configures SNMP.
ssh	Configures SSH.
stack	Configures a system stacking.
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, EFM OAM, 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.
oam efm	Configures EFM OAM.
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 V5812G 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. 3.7 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 V5812G 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 Router Configuration Mode

In *Router Configuration* mode, you can configure IP routing protocols and VRRP. The V5812G provides three IP routing protocols such as RIP v2, BGP v4 and OSPF v2.

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

Command	Mode	Description
router {*IP-PROTOCOL* | **vrrp**}	Global	Opens *Router Configuration* mode to configure IP routing protocols and VRRP.

Tab. 3.11 shows main commands of *Router Configuration* mode.

Command	Description
distance	Configures distance value to find better route.
neighbor	Configures neighbor router.
network	Configures network to operate each routing protocol.
redistribute	Registers transmitted routing information to another router's table.
associate	Configures associated IP address same with virtual router.
authentication	Configures password of virtual router group.
preempt	Activates/deactivates preempt.
vr-priority	Assigns priority to virtual router.
vr-timers	Configures advertisement time, which means the interval that master router distributes its information to another virtual router.

Tab. 3.11 Main Command of *Router Configuration* Mode

3.1.12 Route-Map Configuration Mode

In *Route-map Configuration* mode, you can configure to transmit routing information with various options.

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

Command	Mode	Description
route-map *NAME* {**permit** | **deny**} <1-65535>	Global	Opens *Route-map Configuration* mode.

Tab. 3.12 shows main commands of *Route-map Configuration* mode.

Command	Description
match	Classifies routing information to permit or deny.
set	Configures routing information options.

Tab. 3.12 Main Command of *Route-map Configuration* Mode

3.1.13 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.

3.1.13.1 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. 3.13 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. 3.13 Main Command of *GPON-OLT Configuration* Mode

3.1.13.2 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. 3.14 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. 3.14 Main Command of *ONU Profile Configuration* Mode

3.2 Configuration Mode Overview

Fig. 3.1 shows the overview of the configuration mode for the V5812G.

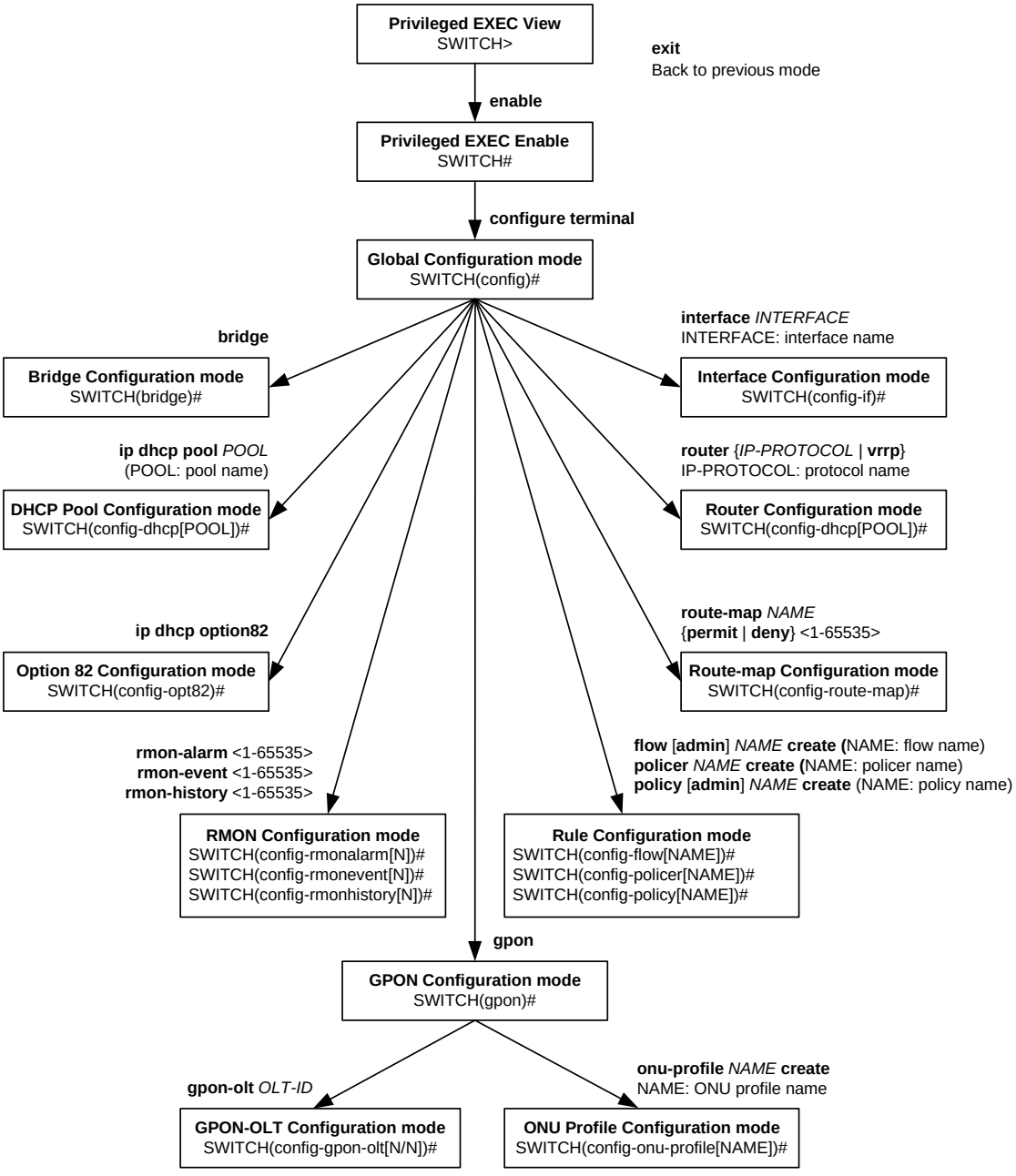


Fig. 3.1 Overview of Configuration Mode

3.3 Useful Tips

This section describes useful tips for operating the V5812G with a CLI.

- Listing Available Command
- Calling Command History
- Using Abbreviation
- Using Command of Privileged EXEC Enable Mode
- Exit Current Command Mode

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 V5812G.

```
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
  rcommand       Management stacking node
  release        Release the acquired address of the interface

(Omitted)

SWITCH#
```

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.

The following is an example of displaying the list of available commands of *Privileged EXEC Enable* mode.

```
SWITCH# show list
clear arp
  clear arp IFNAME
  clear coredump PID
  clear ip arp inspection log
  clear ip arp inspection statistics (vlan VLAN_NAME|)
  clear ip bgp *
  clear ip bgp * in
  clear ip bgp * in prefix-filter
  clear ip bgp * (unicast|multicast) in
  clear ip bgp * (unicast|multicast) in prefix-filter
  clear ip bgp * (unicast|multicast) out
  clear ip bgp * (unicast|multicast) soft
  clear ip bgp * (unicast|multicast) soft in
  clear ip bgp * (unicast|multicast) soft out
  clear ip bgp * out
  clear ip bgp * soft
  clear ip bgp * soft in
  clear ip bgp * soft out
  clear ip bgp * vpnv4 unicast in
  clear ip bgp * vpnv4 unicast out
  clear ip bgp * vpnv4 unicast soft
  clear ip bgp * vpnv4 unicast soft in
  clear ip bgp * vpnv4 unicast soft out
  clear ip bgp <1-65535>
  clear ip bgp <1-65535> in
  clear ip bgp <1-65535> in prefix-filter
  clear ip bgp <1-65535> (unicast|multicast) in
-- more --
```



Press the <**ENTER**> key to skip to the next list.

In case that the V5812G 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 V5812G.

```
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 V5812G also provides 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
Dasan 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

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. 3.15 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!

4 System Connection and IP Address

4.1 System Connection

After installing the system, the V5812G 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 V5812G. This section provides instructions how to change password for system connection and how to connect to the system through telnet as the following order.

- System Login
- Password for Privileged EXEC Enable Mode
- Changing Login Password
- Management for System Account
- Limiting Number of User
- Auto Log-out
- Telnet Access
- System Rebooting

4.1.1 System Login

After installing the V5812G, 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 Management for System Account

4.1.4.1 Creating System Account

For the V5812G, 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.



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.

4.1.4.2 Security Level

For the V5812G, 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 rip level <0-15> {*COMMAND* | **all**}		Uses the specific command of *RIP Configuration* mode in the level.
privilege bgp level <0-15> {*COMMAND* | **all**}		Uses the specific command of *BGP Configuration* mode in the level.
privilege ospf level <0-15> {*COMMAND* | **all**}		Uses the specific command of *OSPF 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.

Command	Mode	Description
privilege rmon-alarm level <0-15> {*COMMAND* | **all**}	Global	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 route-map level <0-15> {*COMMAND* | **all**}		Uses the specific command of *Route-map 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 should be input same as the displayed commands by **show list**. Therefore, it is not possible to input the commands in the bracket separately.

```
SWITCH# show list
  clear arp
  clear arp IFNAME
  clear coredump PID
  clear ip arp inspection log
  clear ip arp inspection statistics (vlan VLAN_NAME|)
  clear ip bgp *
  clear ip bgp * in
  clear ip bgp * in prefix-filter
  clear ip bgp * (unicast|multicast) in
  clear ip bgp * (unicast|multicast) in prefix-filter
  clear ip bgp * (unicast|multicast) out
  clear ip bgp * (unicast|multicast) soft
  clear ip bgp * (unicast|multicast) soft in
  clear ip bgp * (unicast|multicast) soft out
  clear ip bgp * out
  clear ip bgp * soft
  clear ip bgp * soft in
(Omitted)
```

It is not possible to input **clear ip bgp * unicast in**. You should input like **clear ip bgp *** {**unicast** | **multicast**} **in**.

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**}		Delete 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 rip level <0-15> {*COMMAND* | **all**}		
no privilege bgp level <0-15> {*COMMAND* | **all**}		
no privilege ospf 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 route-map level <0-15> {*COMMAND* | **all**}		

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

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

4.1.5 Limiting Number of Users

For the V5812G, you can limit the number of users accessing the switch through both console interface and 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.

4.1.6 Auto Log-out

For security reasons of the V5812G, if no command is entered within the configured inactivity time, the user is automatically logged out of the system. Administrator can configure the inactivity timer.

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.

4.1.7 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: IP address or host name



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.

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#
```

4.1.8 System Rebooting

4.1.8.1 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.

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

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

If you reboot the system without saving new configuration, new configuration will be deleted. So, you have to save the configuration before rebooting. Not to make that mistake, the V5812G is supported to print the following message to ask if user really wants to reboot and save configuration.

Please, press <**y**> key when you would like to save the configurations. Then, press <**y**> key, if you want to continue to reboot the system, press <**y**> key.

4.1.9 Auto Reset Configuration

The V5812G reboots the system according to user's configuration. There are 3 basises for system rebooting. These are CPU, ping 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.

4.1.9.1 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.

4.1.9.2 Memory

The V5812G 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.

4.1.9.3 Network Connection

You can use auto reset function by sending and then listening for a PING. If there is no response within a specified time period and option values, the V5812G will automatically reset the system. To configure the option values in use for monitoring the network connection using PING test, use the following command.

Command	Mode	Description
auto-reset ping { **default-gw** | *A.B.C.D*} <10-86400> <1-10> <1-10> <1-10> <1-100>	Bridge	Configures the value of parameters, which are used in ping transaction: default-gw: default gateway A.B.C.D: gateway IP address 10-86400: ping transaction interval 1-10: a number of requests in a ping transaction 1-10: ping request interval 1-10: a timeout of ping request 1-100: ping loss threshold
no auto-reset ping		Deletes the configured value of parameters that are used in a ping transaction.

To set the threshold of performing the auto rebooting by ping, use the following command.

Command	Mode	Description
auto-reset ping reboot-threshold <1-100>	Bridge	Sets the maximum number of auto rebooting by ping transaction. It stops auto rebooting after it reboots as many as its threshold value. 1-100: reboot stop threshold
no auto-reset ping reboot-threshold		Deletes the configured threshold to stop auto rebooting.

To enable/disable auto system rebooting by ping transaction, use the following command.

Command	Mode	Description
auto-reset ping {**enable** | **disable**}	Bridge	Enables/disables auto system rebooting in case of ping loss state.

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

Command	Mode	Description
show auto-reset ping	Enable/Global/Bridge	Shows a current configured auto system rebooting by ping transaction

To clear auto-reset counters of ping, use the following command.

Command	Mode	Description
clear auto-reset ping-reboot-counter	Bridge	Resets the counters of auto rebooting which has occurred by Ping.

4.2 System Authentication

For the enhanced system security, the V5812G 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 V5812G, 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 KEY: authentication key value auth_port: authentication port (optional) acct_port: accounting port (optional)
no login radius server [*A.B.C.D*]		Deletes an added RADIUS server.



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 V5812G 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 V5812G 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



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 V5812G 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 V5812G 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.

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

4.2.6 Accounting Mode

The V5812G 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 V5812G 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 by assigning an IP address as follows:

- Enabling Interface
- Assigning IP Address to Network Interface
- Static Route and Default Gateway
- Interface Description
- Displaying Interface

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)#
```



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* **primary**	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 8.6.9.

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**} [<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 1-255: distance value src: binding source IP address
ip route *A.B.C.D/M* {*GATEWAY* | **null**} [<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**} [<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 [**bgp** | **connected** | **kernel** | **ospf** | **rip** | **static** | *A.B.C.D* | *A.B.C.D/M* | **summary**]	Enable Global Bridge	Shows configured routing information.
show ip route database [**bgp** | **connected** | **kernel** | **ospf** | **rip** | **static**]		Shows configured routing information with IP routing table database.

4.3.4 Interface Description

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

Command	Mode	Description
description *DESCRIPTION*	Interface	Specifies a description on an 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)#
```

4.4 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.

4.4.1 SSH Server

The V5812G can be operated as SSH server. You can configure the switch as SSH server with the following procedure.

- Enabling SSH Server
- Displaying On-line SSH Client
- Disconnecting SSH Client
- Assigning Specific Authentication Key
- Displaying Connection History of SSH Client

4.4.1.1 Enabling SSH Server

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

Command	Mode	Description
ssh server enable	Global	Enables SSH server.
ssh server disable		Disables SSH server.

4.4.1.2 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.

4.4.1.3 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

4.4.1.4 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.

4.4.1.5 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.

4.4.2 SSH Client

The V5812G can be used as SSH client with the following procedure.

- Login to SSH Server
- Secured File Copy
- Authentication Key

4.4.2.1 Login to SSH Server

To login to SSH server after configuring the V5812G as SSH client, use the following command.

Command	Mode	Description
ssh login *DESTINATION* [*PUBLIC-KEY*]	Enable	Logins to SSH server. DESTINATION: IP address of SSH server PUBLIC-KEY: public key

4.4.2.2 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

4.4.2.3 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 V5812G, 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@V5812G
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#
```

4.5 802.1x 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 V5812G 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.

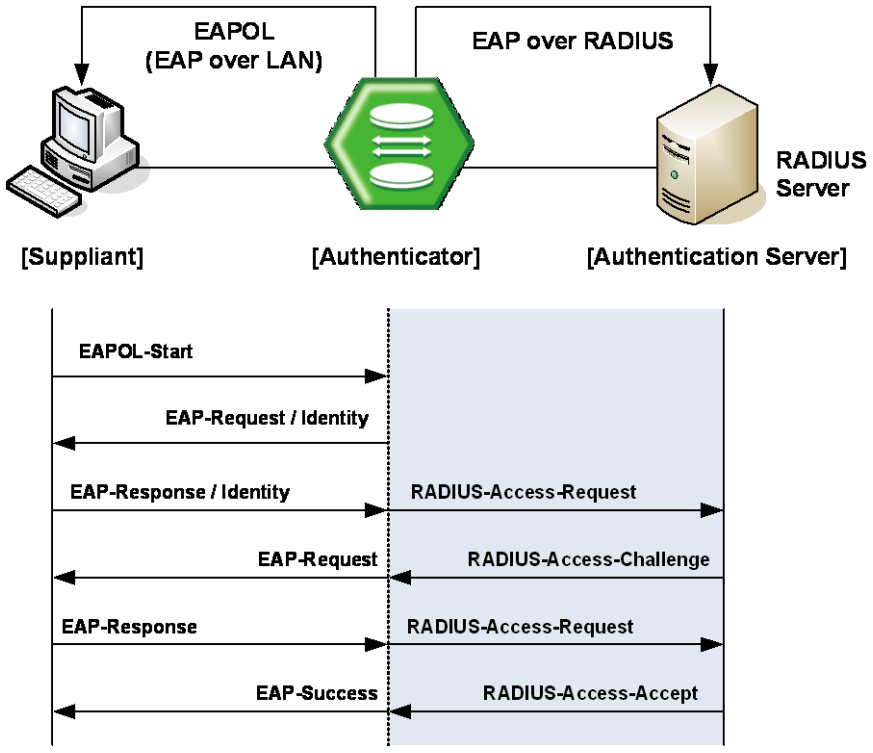


Fig. 4.1 Process of 802.1x Authentication

4.5.1 802.1x Authentication

4.5.1.1 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.

4.5.1.2 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.

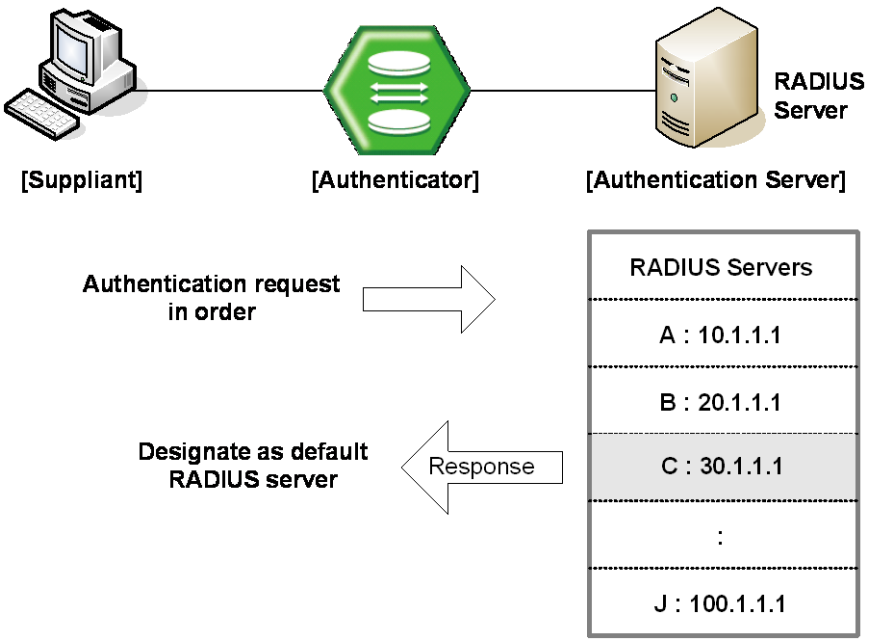


Fig. 4.2 Multiple Authentication Servers

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.

You can designate up to 5 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.

4.5.1.3 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 7.13.1.

4.5.1.4 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.

4.5.1.5 Force Authorization

The V5812G 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.

4.5.1.6 Interval for Retransmitting Request/Identity Packet

In the V5812G, 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.

4.5.1.7 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 V5812G, 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)

4.5.1.8 Interval of Request to RADIUS Server

For the V5812G, 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.

4.5.2 802.1x Re-Authentication

In the V5812G, 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.

4.5.2.1 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.

4.5.2.2 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 V5812G 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.

4.5.2.3 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 V5812G, 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.

4.5.2.4 802.1x Re-Authentication

In Section 4.5.2.2, 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 V5812G, 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.

4.5.3 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.

4.5.4 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.

4.5.5 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.

4.5.6 802.1x 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.

4.5.7 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 V5812G 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 V5812G.

This chapter contains the following sections.

- Port Basic
- Ethernet Port Configuration
- Port Mirroring

5.1 Port Basic

5.1.1 Selecting Port Type

V5812G provides the combo uplink ports either 1000Base-X optical interfaces or 10/100/1000Base-T electrical interfaces, you should select port type. (RJ45 and SFP).

To select port type, use the following command.

Command	Mode	Description
port medium *PORT* {**sfp** | **rj45**}	Bridge	Selects port type (Default: RJ45)

To view the configuration of switch port type, use the following command.

Command	Mode	Description
show port medium	Enable Global Bridge	Shows port type

5.2 Ethernet Port Configuration

5.2.1 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 5.

```
SWITCH(bridge)# show port 5
--------------------------------------------------------------------------
NO      TYPE      PVID    STATUS        MODE        FLOWCTRL      INSTALLED
                        (ADMIN/OPER)               (ADMIN/OPER)
--------------------------------------------------------------------------
5    Ethernet       1     Up/Down  Auto/Full/0     Off/ Off        Y
SWITCH(bridge)# port disable 5
SWITCH(bridge)# show port 5
--------------------------------------------------------------------------
NO      TYPE      PVID    STATUS        MODE        FLOWCTRL      INSTALLED
                        (ADMIN/OPER)               (ADMIN/OPER)
--------------------------------------------------------------------------
5    Ethernet       1   Down/Down  Auto/Full/0     Off/ Off        Y
SWITCH(bridge)#
```

5.2.2 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.

5.2.3 Transmit Rate

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

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



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

5.2.4 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

5.2.5 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

5.2.6 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.

5.2.7 Traffic Statistics

5.2.7.1 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 interface all-stats [*PORTS*]		Shows all the interface information of the specified Ethernet 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

5.2.7.2 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 display the statistics counters of protocol types, use the following command.

Command	Mode	Description
show cpu counters [*PORTS*]	Enable Global Bridge	Shows the statistics of the protocol for all of packets on CPU.
show cpu counters avg [*PORTS*]		Shows the statistics of the protocol for average packets on 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 V5812G 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.

5.2.7.3 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.

5.2.8 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).



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.

5.3 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.

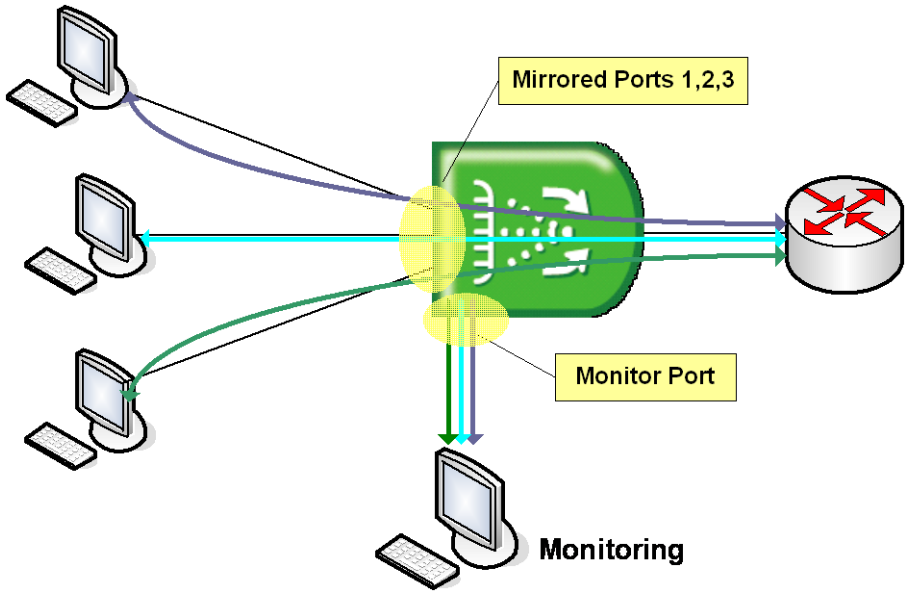


Fig. 5.1 Port Mirroring

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 Activate the port mirroring, using the following command.

Command	Mode	Description
mirror enable	Bridge	Activates port mirroring.

Step 2 Designate the monitor port, use the following command.

Command	Mode	Description
mirror monitor {*PORTS* | **cpu**}	Bridge	Designates the monitor port. PORTS: port number

Step 3 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

Step 4 To delete and modify the configuration, use the following command.

Command	Mode	Description
no mirror monitor	Bridge	Deletes a designated monitor port.
mirror del *PORTS* [**ingress** | **egress**]		Deletes a port from the mirrored port.

Step 5 To disable monitoring function, use the following command.

Command	Mode	Description
mirror disable	Bridge	Deactivate monitoring.

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

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

The following is an example of enabling the port mirroring on the port 5 and 6 with the monitoring port 1.

```
SWITCH(bridge)# mirror enable
SWITCH(bridge)# mirror monitor 1
SWITCH(bridge)# mirror add 5
SWITCH(bridge)# mirror add 6
SWITCH(bridge)# show mirror
 Mirroring enabled
 Monitor port = 1
      ------------------------------------
                           |        1
                           |123456789012
      ------------------------------------
      Ingress Mirrored Ports|....oo......
      Egress  Mirrored Ports|....oo......
SWITCH(bridge)#
```

6 System Environment

6.1 Environment Configuration

You can configure a system environment of the V5812G with the following items:

- Host Name
- Time and Date
- Time Zone
- Network Time Protocol (NTP)
- Simple Network Time Protocol (SNTP)
- Terminal Configuration
- Login Banner
- DNS Server
- Fan Operation
- Disabling Daemon Operation
- FTP Server
- FTP Bind Address
- System Threshold

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.

6.1.3 Time Zone

The V5812G 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 server *SERVER1* [*SERVER2*] [*SERVER3*]	Global	Enables NTP function with a specified NTP server. SERVER: server IP address (maximum 3 servers)
no ntp server *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.

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.

To configure the polling interval for NTP, use the following command.

Command	Mode	Description
ntp poll-interval *VALUE*	Global	Configures the polling interval for NTP. VALUE: 6 to 20 (default: 16)
no ntp poll-interval		Deletes the configured polling interval value for NTP.

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*] [*SERVER3*]		Deletes a specified SNTP server.
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 V5812G 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.
no dns server *A.B.C.D*		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 V5812G, 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 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#
```

6.1.11 FTP Server

The V5812G provides the FTP server feature, which is enabled by default. For security reason, however, the FTP server may need to be disabled to block an illegal access via the port 23.

To enable/disable the FTP server on the system, use the following command.

Command	Mode	Description
ftp server {**enable** | **disable**}	Global	Enables/disables the FTP server on the system. (default: enable)



If the FTP server is disabled, the system software upgrade cannot be done via FTP server!

6.1.12 FTP Bind Address

When used as an FTP client, the V5812G 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 V5812G may have multiple IP addresses. In such a multiple-IP environment, a primary IP address is normally used. You can configure the V5812G 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 IP addresses configured in an interface
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 V5812G 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.

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>	Bridge	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 <-40-100>	Global	Sets the threshold of system temperature in the unit of centigrade (°C). -40-100: system temperature (default: 80)
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* {**system** | **sfp**}	Global	Sets the Diagnostics threshold of SFP module by RX/TX power and monitors the module The range of RX/TX power: 0-6.5535 ㎽
threshold module temper {**alarm** | **warning**} *PORTS START-VALUE STOP-VALUE* {**system** | **sfp**}		Sets the Diagnostics threshold of SFP module depending on temperature and monitors the module. The range of temperature: -128～127.99℃
threshold module txbias {**alarm** | **warning**} *PORTS START-VALUE STOP-VALUE* {**system** | **sfp**}		Sets the Diagnostics threshold of SFP module depending on txbias and monitors the module. The range of txbias: 0- 131 ㎖
threshold module voltage {**alarm** | **warning**} *PORTS START-VALUE STOP-VALUE* {**system** | **sfp**}		Sets the Diagnostics threshold of SFP module depending on voltage and monitors the module. The range of voltage: 0-6.5535 V

To delete the threshld 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.

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 DDM

You can enable/disable DDM (Digital Diagnostic Monitoring) function, which allows you to be able to check the current status of modules based on the configured threshold for modules.

To enable/disable DDM, use the following command.

Command	Mode	Description
module ddm {**enable** | **disable**}	Global	Enables/disables DDM.

i This function is enabled by default. Thus, if you do not want to get DDM information, configure this setting as disable.

To display the configuration of DDM, use the following command.

Command	Mode	Description
show module ddm	Enable Global Bridge	Shows the current configuration of DDM.

To display the DDM-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).
show port module-info state [*PORTS*]		Shows the current DDM information for modules.

6.2 Configuration Management

You can verify if the system configurations are correct and save them in the system. This section contains the following functions.

- Displaying System Configuration
- Writing System Configuration
- Auto-Saving
- System Configuration File
- Restoring Default Configuration

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 system		
show running-config {**admin-flow** | **admin-policy** | **arp** | **bridge** | **dhcp** | **dns** | **flow** | **full** | **gpon** | **hostname** | **interface** [*INTERFACE*] | **login** | **policer** | **policy** | **qos** | **rmon-alarm** | **rmon-event** | **rmon-history** | **router** {**bgp** | **rip** | **ospf** | **vrrp**} | **snmp** | **syslog** | **time-out** | **time-zone**}		Shows a configuration of the system with the specific 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 V5812G 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 the name configured by user.

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 back up a system configuration file using SSH Secure Copy, use the following command.

Command	Mode	Description
copy scp os upload {**os1** | **os2**}	Enable	Uploads a file with a name of os1 or os2 using SSH copy.
copy scp os download {**os1** | **os2**}		Downloads a file with a name of os1 or os2 using SSH copy.

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
erase startup-config		Deletes a startup configuration file.

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 V5812G
SWITCH(config)# show config-list
=========================
       CONFIG-LIST
=========================
  l3_default
  V5812G
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 V5812G 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.

This section describes the following functions with CLI command:

- Network Connection
- IP ICMP Source Routing
- Tracing Packet Route
- Displaying User Connecting to System
- MAC Table
- System Running Time
- System Information
- System Memory Information
- CPU Packet Limit
- Running Process
- Displaying System Software
- Displaying Installed OS
- Default OS
- Switch Status
- Tech Support Information
- System Boot Information

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*]	Enable	Performs a ping test to verify 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
108 bytes from 10.55.193.110: icmp_seq=4 ttl=255 time=1.63 ms
108 bytes from 10.55.193.110: icmp_seq=5 ttl=255 time=0.414 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.

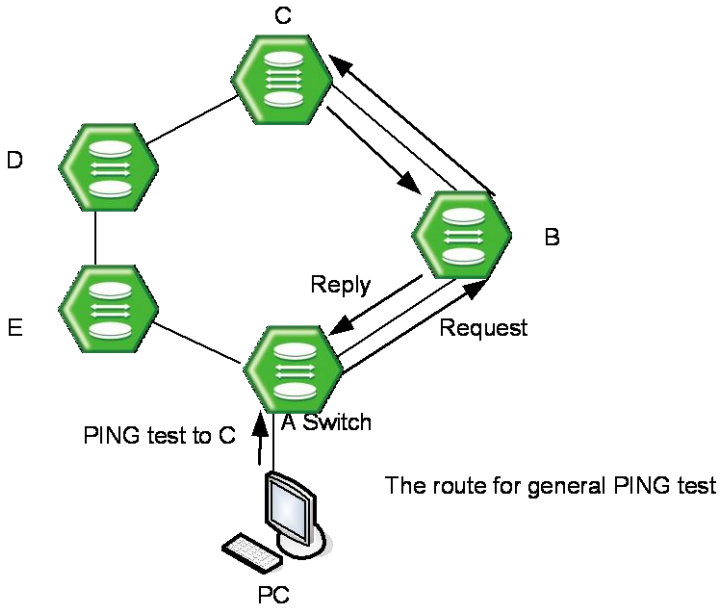


Fig. 6.1 Ping Test for Network Status

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 V5812G can enable to perform ping test from PC as the route of **A→E→D→C**.

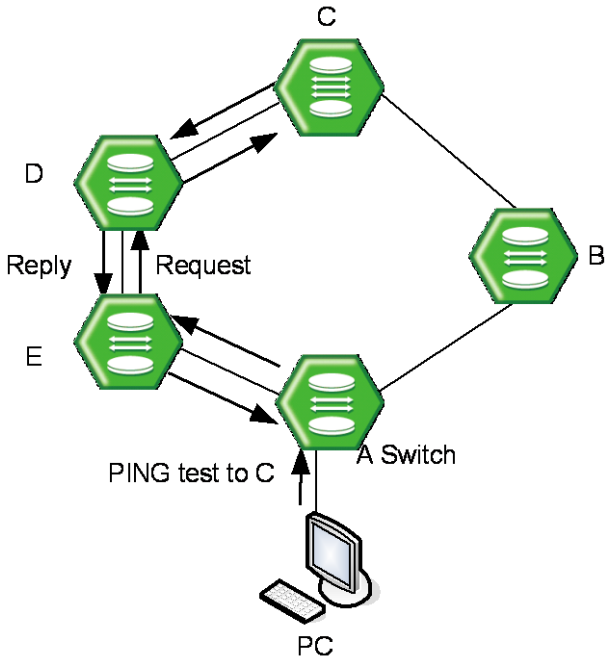


Fig. 6.2 IP Source Routing

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 V5812G, 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
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     00:d0:cb: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 {**bgp** | **dhcp** | **gpon-olt** | **imi** | **lib** | **nsm** | **ospf** | **pim** | **rip** | **swch**}		Shows system memory information with a specific option.

6.3.9 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 <500-6000>	Global	Limits the number of the packets handled by CPU. 500-6000: packets per second (default: 3500)

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 Running Process

The V5812G 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#
```

6.3.11 Displaying System Software

To display a current system software version, use the following command.

Command	Mode	Description
show version	Enable Global Bridge	Shows a version of system software.

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.

6.3.12 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.

6.3.13 Default OS

The V5812G 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)

6.3.14 Switch Status

To display the temperature of switch, power status, and fan status, use the following command.

Command	Mode	Description
show status fan	Enable Global Bridge	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.

6.3.15 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 V5812G 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.

6.3.16 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.

6.3.17 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.

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 V5812G enhances access management of SNMP agent and limits the range of OID opened to agents.

The following is how to configure SNMP.

- SNMP Community
- Information of SNMP Agent
- SNMP Com2sec
- SNMP Group
- SNMP View Record
- Permission to Access SNMP View Record
- SNMP Version 3 User
- SNMP Trap
- SNMP Alarm
- Displaying SNMP Configuration
- Disabling SNMP

7.1.1 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	Creates SNMP community. COMMUNITY: community name
no snmp community {**ro** | **rw**} *COMMUNITY*		Deletes created community.



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)#
```

7.1.2 Information of SNMP Agent

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.
snmp agent-address *A.B.C.D*		Sets an IP address of the SNMP agent.
no snmp contact		Deletes the specified basic information for each item.
no snmp location		
no snmp agent-address		

The following is an example of specifying basic information of SNMP agent.

```
SWITCH(config)# snmp contact Brad
SWITCH(config)# snmp location Germany
SWITCH(config)#
```

To display the basic information of the SNMP agent, use the following command.

Command	Mode	Description
show snmp contact	Enable Global Bridge	Shows the name of the administrator.
show snmp location		Shows the location of the SNMP agent.
show snmp agent-address		Shows the IP address of the SNMP agent.

7.1.3 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)#
```

7.1.4 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.

7.1.5 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)#
```

7.1.6 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.

7.1.7 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.

7.1.8 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.

7.1.8.1 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)

7.1.8.2 SNMP Trap Host

To set an SNMP trap host, use the following command.

Command	Mode	Description
snmp trap-host *A.B.C.D* [*COMMUNITY* | *COMMUNITY* **add** *TRAP-INDEX* | **add** *TRAP-INDEX* | **del** *TRAP-INDEX*]	Global	Specifies an SNMP trap v1 host.
snmp trap2-host *A.B.C.D* [*COMMUNITY* | *COMMUNITY* **add** *TRAP-INDEX* | **add** *TRAP-INDEX* | **del** *TRAP-INDEX*]		Specifies an SNMP trap v2 host.
snmp inform-trap-host *A.B.C.D* [*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*	Global	Deletes a specified SNMP trap v1 host.
no snmp trap2-host *A.B.C.D*		Deletes a specified SNMP trap v2 host.
no snmp inform-trap-host *A.B.C.D*		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)#
```

7.1.8.3 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.

- **auth-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.
- **link-up/down** is shown when network of port specified by user is disconnected, or when the network is connected again.
- **mem-threshold** is shown when memory usage exceeds the threshold specified by user. When memory usage falls below the threshold, the trap message will be shown to notify it.
- **cpu-threshold** is shown when CPU utilization exceeds the threshold specified by user. When CPU load 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. When port traffic falls below the threshold, trap message will be shown.

- **temp-threshold** is shown when the system temperature exceeds the thresh-old configured by user. when system temperature falls below the threshold, trap message will be shown.
- **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.
- **fan/power/module** is shown when there is any status-change of fan, power, and module.
- **pim-group-filter** trap is shown when the error of PIM group filtering occurs.



The system is configured to send all the SNMP traps by default.

To enable the SNMP trap, use the following command.

Command	Mode	Description
snmp trap auth-fail	Global	Configures the system to send SNMP trap when SNMP authentication is fail.
snmp trap cold-start		Configures the system to send SNMP trap when SNMP agent restarts.
snmp trap link-up *PORTS* [*NODE*]		Configures the system to send SNMP trap when a port is connected to network.
snmp trap link-down *PORTS* [*NODE*]		Configures the system to send SNMP trap when a port is disconnected from network.
snmp trap mem-threshold		Configures the system to send SNMP trap when memory usage exceeds or falls below the threshold.
snmp trap cpu-threshold		Configures the system to send SNMP trap when CPU load exceeds or falls below the threshold.
snmp trap port-threshold		Configures the system to send SNMP trap when the port traffic exceeds or falls below the threshold.
snmp trap temp-threshold		Configures the system to send SNMP trap when system temperature exceeds or falls below the threshold.
snmp trap dhcp-lease		Configures the system to send SNMP trap when no more IP address is left in the DHCP pool.
snmp trap fan		Configures the system to send SNMP trap when the fan begins to operate or stops.
snmp trap power		Configures the system to send SNMP trap when any problem occurs in power.
snmp trap module		Configures the system to send SNMP trap when there is any problem in module.
snmp trap pim-group-filter		Configures the system to send SNMP trap when there is an error of PIM group filtering function.

7.1.8.4 Disabling SNMP Trap

To disable the SNMP trap, use the following command.

Command	Mode	Description
no snmp trap auth-fail	Global	Disables each SNMP trap.
no snmp trap cold-start		
no snmp trap link-up *PORTS* [*NODE*]		
no snmp trap link-down *PORTS* [*NODE*]		
no snmp trap mem-threshold		
no snmp trap cpu-threshold		
no snmp trap port-threshold		
no snmp trap temp-threshold		
no snmp trap dhcp-lease		
no snmp trap fan		
no snmp trap power		
no snmp trap module		
no snmp trap pim-group-filter		



When you use the **no snmp** command, all configurations concerning SNMP will be deleted.

7.1.8.5 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-index <1-4095>		Shows the configuration of SNMP trap index. 1-4095: SNMP trap index
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)#
```

7.1.9 SNMP Alarm

The V5812G 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.

7.1.9.1 Alarm Notify Activity

Normally the V5812G 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)

7.1.9.2 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)

The order of alarm severity is **critical** > **major** > **minor** > **warning** > **intermediate**.

7.1.9.3 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)

7.1.9.4 Generic Alarm Severity

To set generic alarm severity, use the following command.

Command	Mode	Description
snmp alarm-severity fan-fail {**critical** | **major** | **minor** | **warning** | **intermediate**}	Global	Sets severity of an alarm for system fan failure.
snmp alarm-severity cold-start {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets severity of an alarm for system cold restart.
snmp alarm-severity broadcast-over {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets severity of an alarm for too much broadcast.
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** | **minor** | **warning** | **intermediate**}		Sets severity of an alarm for illegal DHCP entry.
snmp alarm-severity fan-remove {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets severity of an alarm for system fan removed.
snmp alarm-severity ipconflict {**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 pim-group-filter {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets severity of an alarm for PIM group filtering.
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-remove {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets severity of an alarm for Ethernet port removed.
snmp alarm-severity port-rx-threshold-over {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets severity of an alarm for port Rx threshold over.

snmp alarm-severity port-tx-threshold-over {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets severity of an alarm for port Tx threshold over.
snmp alarm-severity power-fail {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets severity of an alarm for system power failure.
snmp alarm-severity power-remove {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets severity of an alarm for system power removed.
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.
snmp alarm-severity module-remove {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets severity of an alarm for module removed.
snmp alarm-severity temperature-high {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets severity of an alarm for system temperature high.

To delete configured alarm severity, use the following command.

Command	Mode	Description
no snmp alarm-severity fan-fail	Global	Deletes configured alarm severity.
no snmp alarm-severity cold-start		
no snmp alarm-severity broadcast-over		
no snmp alarm-severity cpu-load-over		
no snmp alarm-severity dhcp-lease		
no snmp alarm-severity dhcp-illegal		
no snmp alarm-severity fan-remove		
no snmp alarm-severity ipconflict		
no snmp alarm-severity memory-over		
no snmp alarm-severity mfgd-block		
no snmp alarm-severity pim-group-filter		
no snmp alarm-severity port-link-down		
no snmp alarm-severity port-remove		
no snmp alarm-severity port-rx-threshold-over		
no snmp alarm-severity port-tx-threshold-over		
no snmp alarm-severity power-fail		
no snmp alarm-severity power-remove		
no snmp alarm-severity rmon-alarm-rising		
no snmp alarm-severity rmon-alarm-falling		
no snmp alarm-severity system-restart		
no snmp alarm-severity module-remove		
no snmp alarm-severity temperature-high		

7.1.9.5 ADVA Alarm Severity

To set ADVA alarm severity, use the following command.

Command	Mode	Description
snmp alarm-severity adva-fan-fail {**critical** | **major** | **minor** | **warning** | **intermediate**}	Global	Sets ADVA severity of an alarm for system temperature high.
snmp alarm-severity adva-if-misconfig {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets ADVA severity of an alarm for wrong configuration.
snmp alarm-severity adva-if-opt-thres {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets ADVA severity of an alarm for traffic threshold over for an Ethernet optical interface.
snmp alarm-severity adva-if-rcv-fail {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets ADVA severity of an alarm for failure to receive packets.
snmp alarm-severity adva-if-trans-fault {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets ADVA severity of an alarm for failure to transmit packets.
snmp alarm-severity adva-if-sfp-mismatch {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets ADVA severity of an alarm for SFP module mismatched.
snmp alarm-severity adva-psu-fail {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets ADVA severity of an alarm for PSU failure.
snmp alarm-severity adva-temperature {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets ADVA severity of an alarm for system temperature high.
snmp alarm-severity adva-voltage-high {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets ADVA severity of an alarm for input voltage high.
snmp alarm-severity adva-voltage-low {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets ADVA severity of an alarm for input voltage low.

To delete configured ADVA alarm severity, use the following command.

Command	Mode	Description
no snmp alarm-severity adva-fan-fail	Global	Deletes configured ADVA alarm severity.
no snmp alarm-severity adva-if-misconfig		
no snmp alarm-severity adva-if-opt-thres		
no snmp alarm-severity adva-if-rcv-fail		
no snmp alarm-severity adva-if-sfp-mismatch		
no snmp alarm-severity adva-if-trans-fault		
no snmp alarm-severity adva-psu-fail		
no snmp alarm-severity adva-temperature		
no snmp alarm-severity adva-voltage-high		
no snmp alarm-severity adva-voltage-low		

7.1.9.6 STP Guard Alarm Severity

To set severity of an alarm for STP guard, use the following command.

Command	Mode	Description
snmp alarm-severity stp-bpdu-guard {**critical** | **major** | **minor** | **warning** | **intermediate**}	Global	Sets severity of an alarm for BPDU guard disabled.
snmp alarm-severity stp-root-guard {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sets severity of an alarm for root guard disabled.

To delete configured severity of alarm for STP guard, use the following command.

Command	Mode	Description
no snmp alarm-severity stp-bpdu-guard	Global	Deletes configured severity of an alarm for STP guard.
no snmp alarm-severity stp-root-guard		

7.1.9.7 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		Deletes a collected alarm report in the system.

7.1.10 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.

7.1.11 Disabling SNMP

To disable SNMP, use the following command.

Command	Mode	Description
no snmp	Global	Disables SNMP.

When you use the **no snmp** command, all configurations of SNMP will be lost.

7.2 Operation, Administration and Maintenance (OAM)

In the enterprise, Ethernet links and networks have been managed via Simple Network Management Protocol (SNMP). Although SNMP provides a very flexible management solution, it is not always efficient and is sometimes inadequate to the task.

First, using SNMP assumes that the underlying network is operational because SNMP relies on IP connectivity; however, you need management functionality even more when the underlying network is non-operational. Second, SNMP assumes every device is IP accessible. This requires provisioning IP on every device and instituting an IP overlay network even if the ultimate end-user service is an Ethernet service. This is impractical in a carrier environment.

For these reasons, carriers look for management capabilities at every layer of the network. The Ethernet layer has not traditionally offered inherent management capabilities, so the IEEE 802.3ah Ethernet in the First Mile (EFM) task force added the Operations, Administration and Maintenance (OAM) capabilities to Ethernet like interfaces. These management capabilities were introduced to provide some basic OAM function on Ethernet media.

OAM is complementary, not competitive, with SNMP management in that it provides some basic management functions at Layer 2, rather than using Layer 3 and above as required by SNMP over an IP infrastructure.

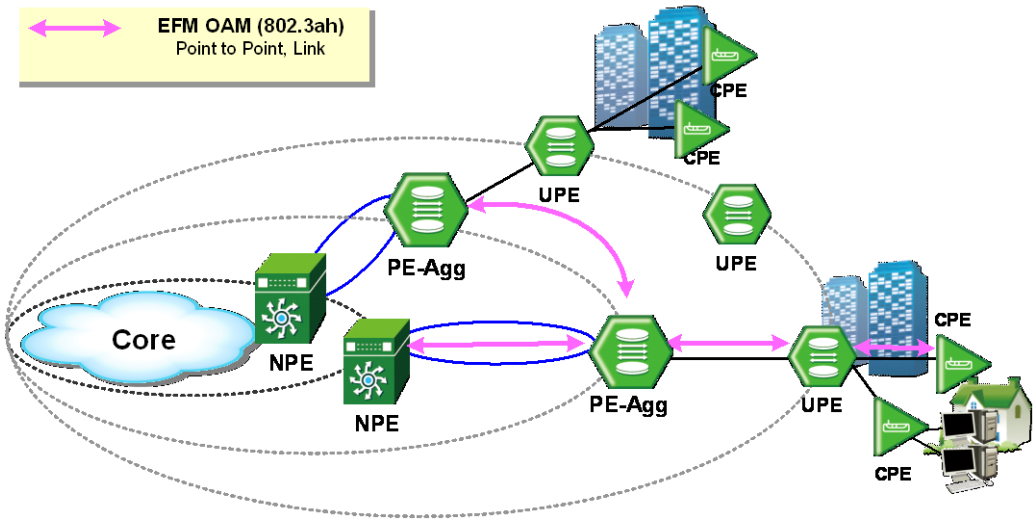


Fig. 7.1 EFM OAM Deployment Scenario

OAM is responsible for monitoring and troubleshooting individual Ethernet links or end-to-end Ethernet instances.

EFM OAM provides mechanisms for remote fault detection and loopback controls. It provides single-hop functionality in that it works only between two directly connected Ethernet stations, called local Data Terminal Equipment (DTE) and a remote DTE. OAMPDUs are interchanged between local DTE and remote DTE. A local DTE manages a remote DTE by referring to OAMPDUs containing the information of critical link events or faults with its remote DTE.

EFM OAM Operation

EFM OAM capabilities are a need for Ethernet subscriber access link monitoring in L2, remote loopback and remote failure indication. 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.

7.2.1 Enabling OAM

To enable/disable EFM OAM function, use the following command.

Command	Mode	Description
oam efm enable *PORTS*	Global	Enables EFM OAM.
oam efm disable *PORTS*		Disables EFM OAM.

To configure an interval of EFM OAMPDUs which are exchanged between local DTE and remote DTE, use the following command.

Command	Mode	Description
oam efm interval <1-10> *PORTS*	Global	Configures the interval of OAMPDUs. (default: 1 second)

To configure a lost-link-packet of EFM OAMPDUs which are exchanged between local DTE and remote DTE, use the following command.

Command	Mode	Description
oam efm lost-link-packet <5-60> *PORTS*	Global	Configures the lost-link-packet counts of OAMPDUs. It decides a local_lost_link_timer. (default: 5)

7.2.2 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.
oam efm link-monitor disable *PORTS*		Disables link monitoring function.

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: 100 msec, default:1) 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 frames) 0-65535: threshold value (default:10)
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.

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.
oam efm link-monitor action snmp-trap *PORTS*		Generates a snmp trap message when event notifications are received.

7.2.3 EFM OAM Mode

To configure EFM OAM mode, use the following command.

Command	Mode	Description
oam efm mode {**active** | **passive**} *PORTS*	Global	Configures the mode of EFMOAM.

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.

7.2.4 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.
oam efm remote-loopback deny *PORTS*		Ignores the loopback control commands from its remote peer switch. (Default)

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

To reset loopback function, use the following command.

Command	Mode	Description
oam efm remote-loopback reset *PORTS*	Global	Resets loopback function of local device.

7.2.5 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.
oam efm unidir disable *PORTS*		Disables to transmit the information by using TX.

7.2.6 Displaying EFM OAM Configuration

To display OAM configuration, use the following command.

Command	Mode	Description
show oam efm	Enable Global Bridge	Shows EFM OAM configuration.
show oam efm link-monitor {**local** | **remote**} *PORTS*		Shows the link monitoring status on ports.
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

7.3 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.

7.3.1 LLDP Operation

The V5812G 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.

7.3.2 Enabling LLDP

To enable/disable LLDP, use the following command.

Command	Mode	Description
lldp *PORTS* **mgmtaddr** *A.B.C.D*	Bridge	Enables LLDP function on a port. A.B.C.D: IP address that is given to LLDP packet
no lldp *PORTS* **mgmtaddr** *A.B.C.D*		Disables LLDP function.

7.3.3 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)

7.3.4 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 V5812G, 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. mgmtaddr: management address 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.

7.3.5 LLDP Message

For the V5812G, 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)

7.3.6 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)

7.3.7 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.

7.4 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 V5812G supports two MIB groups of them, most basic ones: Statistics (only for uplink ports) and History.

7.4.1 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])#
```

7.4.1.1 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)

7.4.1.2 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).

7.4.1.3 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)

7.4.1.4 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.

7.4.1.5 Activating RMON History

To activate RMON history, use the following command.

Command	Mode	Description
active	RMON	Activates RMON history.

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.

7.4.1.6 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.

7.4.1.7 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.

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])#
```

7.4.2 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

7.4.2.1 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).

7.4.2.2 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.

7.4.2.3 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.

7.4.2.4 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

7.4.2.5 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.

7.4.2.6 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.

7.4.2.7 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)

7.4.2.8 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.

7.4.2.9 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.

7.4.3 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

7.4.3.1 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

7.4.3.2 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.

7.4.3.3 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.

7.4.3.4 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.

7.4.3.5 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.

7.4.3.6 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.

7.5 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.

This section contains the following contents.

- Syslog Output Level
- Facility Code
- Syslog Bind Address
- Debug Message for Remote Terminal
- Disabling Syslog
- Displaying Syslog Message
- Displaying Syslog Configuration

7.5.1 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*		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*		

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** | **notice** | **info**} **console**	Global	Generates a user-defined syslog message with a priority and forwards it to the 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*		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*		

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**} *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** | **physical-entity** | **dhcp** | **filter** | **gpon**} *INDEX*		Deletes a specified user-defined syslog nessage 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**} [*INDEX*]		Shows the syslog index information of each parameter

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)#
```

7.5.2 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)#
```

7.5.3 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*	Global	Specifies the IP address to bind to a syslog message.
no syslog bind-address		Deletes a specified IP address.

7.5.4 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.

7.5.5 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.

7.5.6 Displaying Syslog Message

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.

7.5.7 Displaying Syslog Configuration

To display the configuration of the syslog, use the following command.

Command	Mode	Description
show syslog [**status**]	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

7.6 Rule and QoS

The V5812G 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.

7.6.1 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. 7.2 shows the simple procedure of QoS operation.

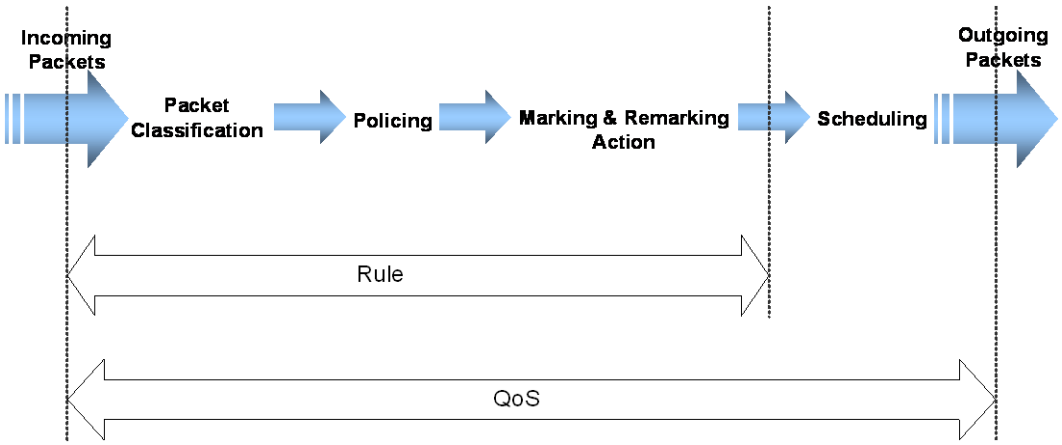


Fig. 7.2 Procedure of QoS operation

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 V5812G 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. 7.3 shows the relationship of Flow, Class, Policer and Policy on basic structure of Rule.

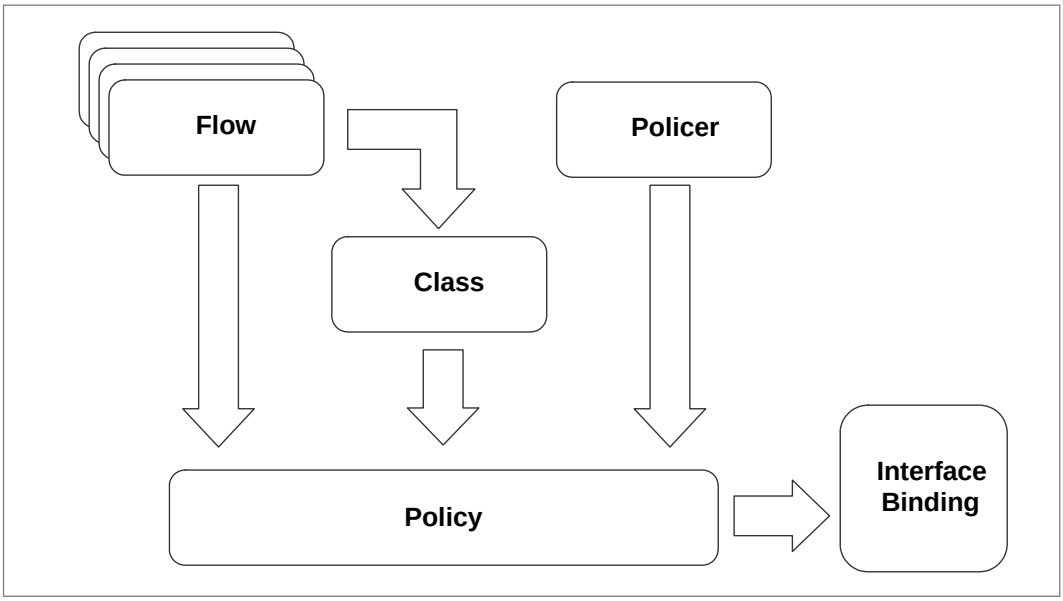


Fig. 7.3 Structure of Rule

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.

7.6.2 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 V5812G classifies the packets corresponding to the parameters.

7.6.2.1 Flow Mode

The V5812G gives you two flow modes. The flow mode decides the number of rule you can create. The default mode can have up to 1024 flows while the extension mode can have up to 512 flows. However if you set the default mode on the system, it causes NetBios Filtering function to be disabled. There is any other restriction on the extension mode.

To select the flow mode, use the following command.

Command	Mode	Description
flow default	Global	Operates the system in the default flow mode
flow extension		Operates the system in the extension flow mode

7.6.2.2 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.

7.6.2.3 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
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 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 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. (This can be used only in the extension mode!) 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

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 ip header-length		
no ip header-error		

7.6.2.4 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.



You should save and apply the flow to system whenever you modify or configure the flow.

7.6.2.5 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.

7.6.3 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.

7.6.3.1 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.

- 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.

7.6.3.2 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 Global Bridge	Resets a collected policy counter.

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.

7.6.3.3 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.

7.6.3.4 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.

7.6.4 Rule Action

7.6.4.1 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.

7.6.4.2 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 V5812G 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.

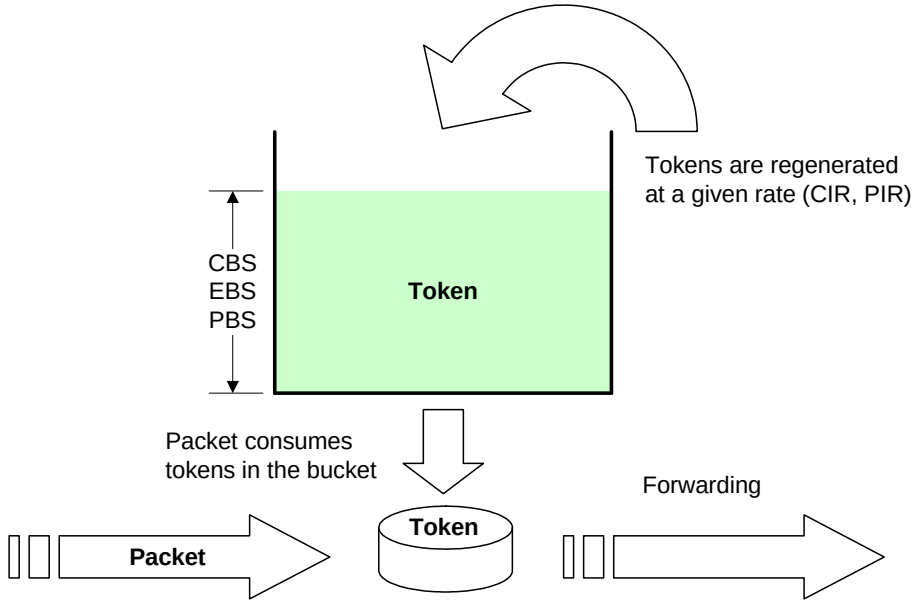


Fig. 7.4 Token Bucket Meter

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.

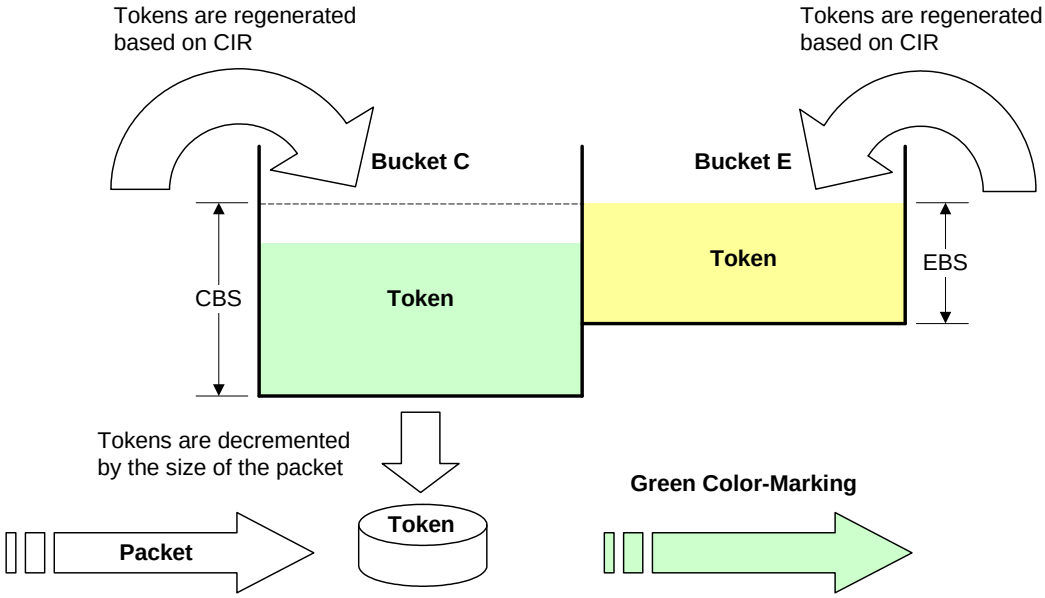


Fig. 7.5 Behavior of srTCM (1)

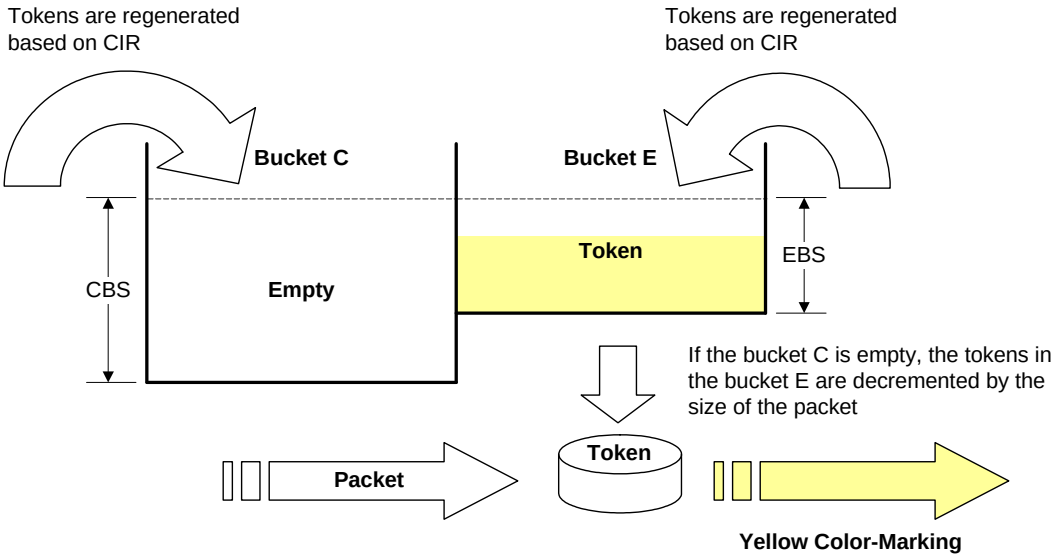


Fig. 7.6 Behavior of srTCM (2)

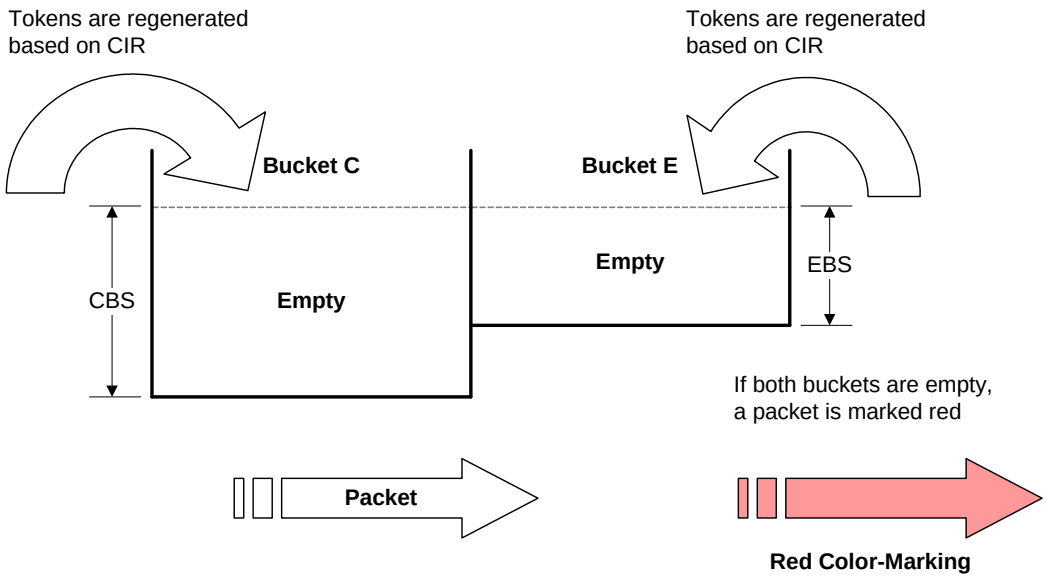


Fig. 7.7 Bahavior of srTCM (3)

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.

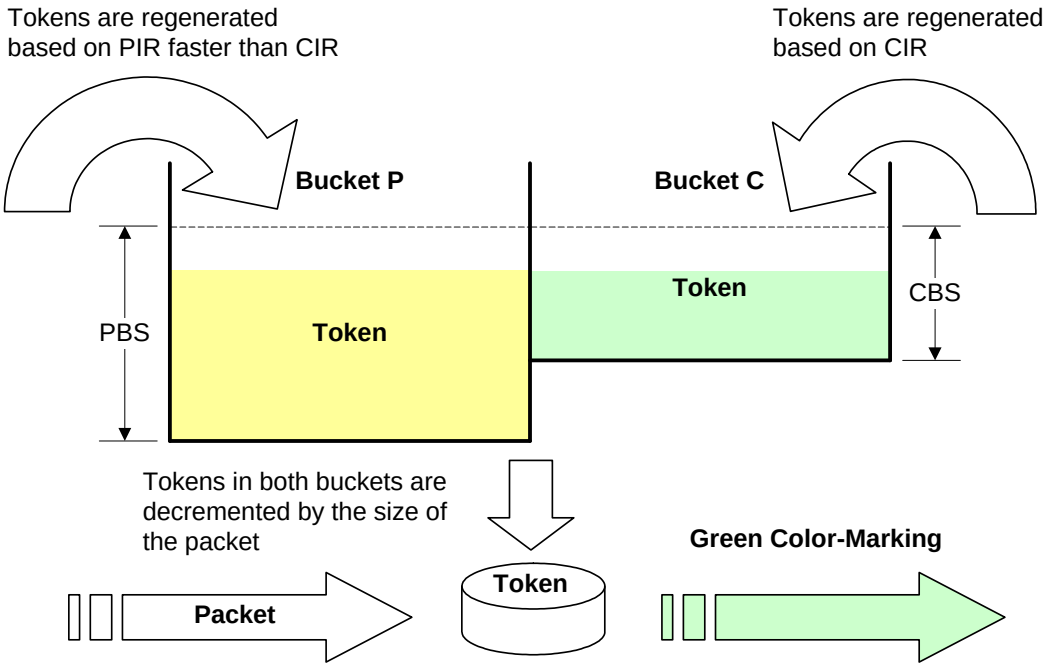


Fig. 7.8 Behavior of trTCM (1)

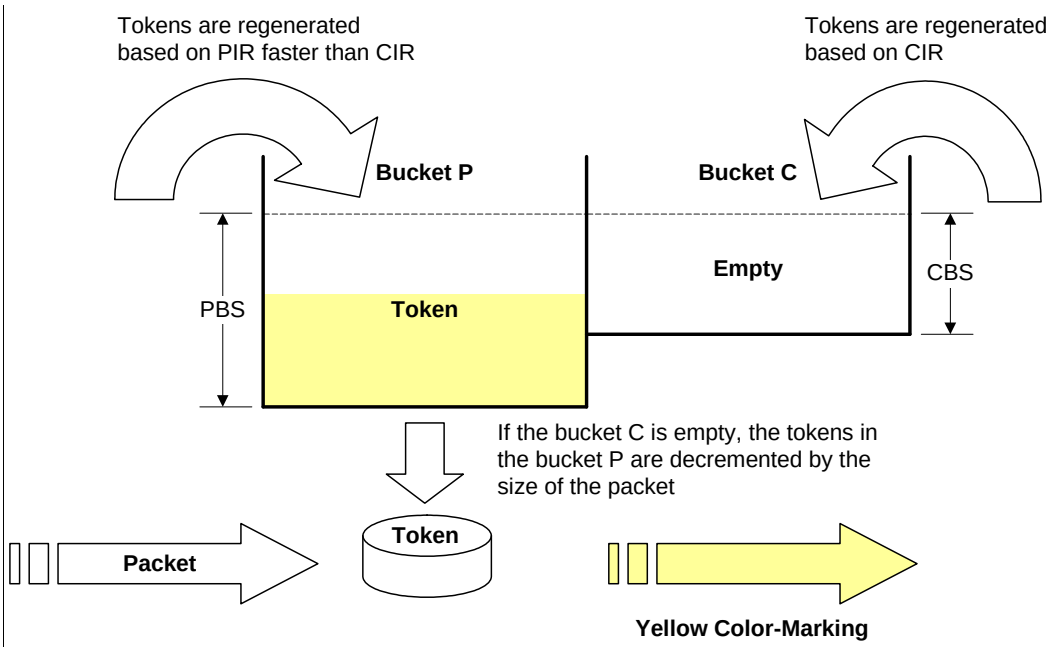


Fig. 7.9 Behavior of trTCM (2)

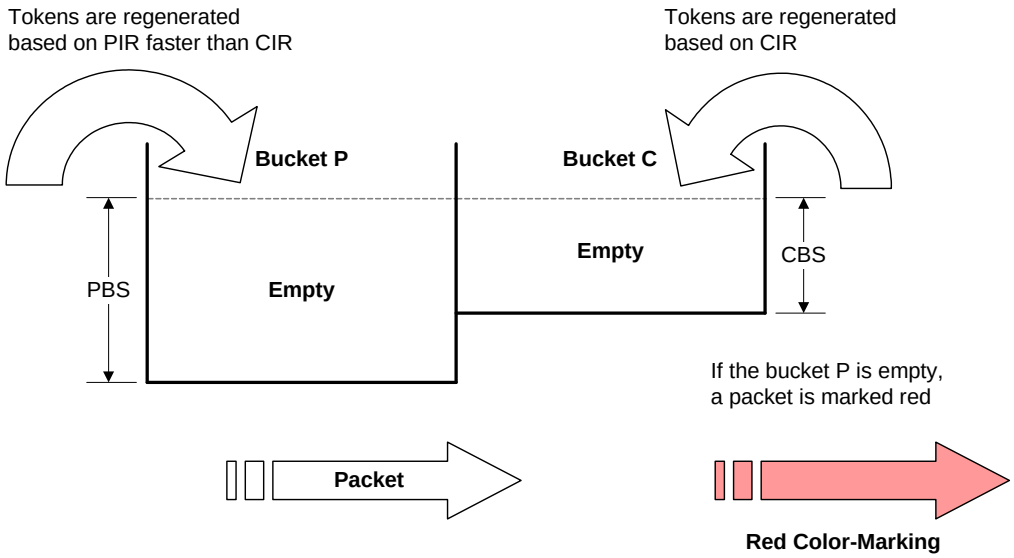


Fig. 7.10 Behavior of trTCM (3)

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.

i In the color-blind mode, the meter assumes that the packet stream is uncolored. In the 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 red-colored or yellow-colored packets to discard. To configure the meter to discard all red-colored or yellow-colored packets, use the following command.

Command	Mode	Description
color {**red** | **yellow**} **action drop**	Policer	Configures the meter to discard red-colored or yellow-colored packets.
no color {**red** | **yellow**} **action**		Configures the meter to permit 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 {**red** | **yellow**} **action marking**	Policer	Configures DSCP remarking for red-colored or yellow-colored packets.
color {**red** | **yellow**} **action marking drop-precedence** {**red** | **yellow** | **green**}		Configures DSCP remarking and drop precedence for red-colored or yellow-colored packets.

7.6.4.3 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** | **highest**}	Policy	Sets a priority for a policy. (default: low)

7.6.4.4 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 dmac *DST-MAC-ADDR*		Overwrites a specified destination MAC address.

Command	Mode	Description
action match egress filter *PORT*	Policy	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 dmac		
no action match egress		

7.6.4.5 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> **overwrite**	Policy	Configures the 802.1p class of service value. 0-7: CoS value 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 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 cos same-as-tos overwrite		
no action match ip-precedence		
no action match ip-precedence same-as-cos		

7.6.4.6 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.

7.6.4.7 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.

7.6.5 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

7.6.6 Admin Rule

For the V5812G, it is possible to block a specific service connection like telnet, FTP, ICMP, etc with an admin rule function.

7.6.6.1 Creating Admin Flow for packet classification

To classify packets by a specific admin flow for the V5812G, 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.

- 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.

7.6.6.2 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 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 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 ip header-length		

7.6.6.3 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.

7.6.6.4 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

7.6.7 Admin Rule Action

7.6.7.1 Admin Policy Creation

For the V5812G, 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.

- 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.

7.6.7.2 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)

7.6.7.3 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		

7.6.7.4 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.

7.6.8 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.

7.6.9 Scheduling

To process incoming packets by the queue scheduler, the V5812G 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.

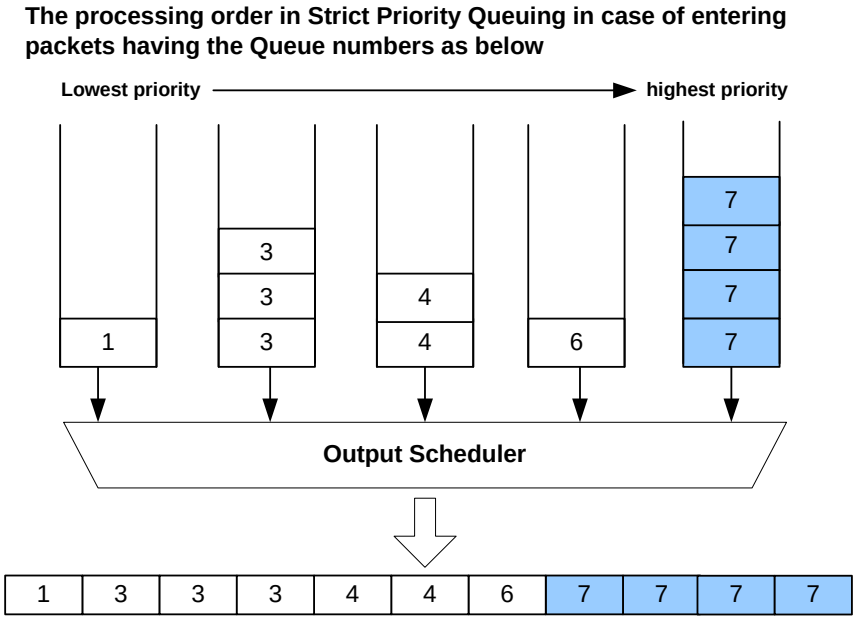


Fig. 7.11 Strict Priority Queuing

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.

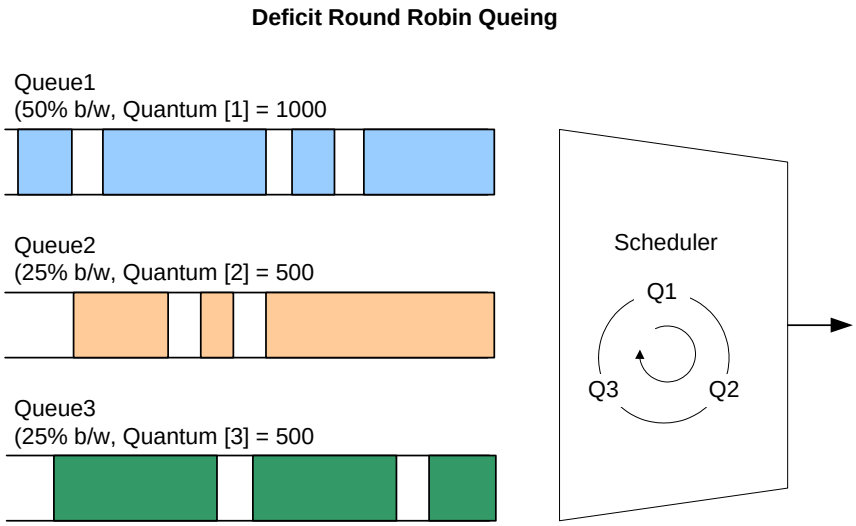


Fig. 7.12 Deficit Round Robin

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.

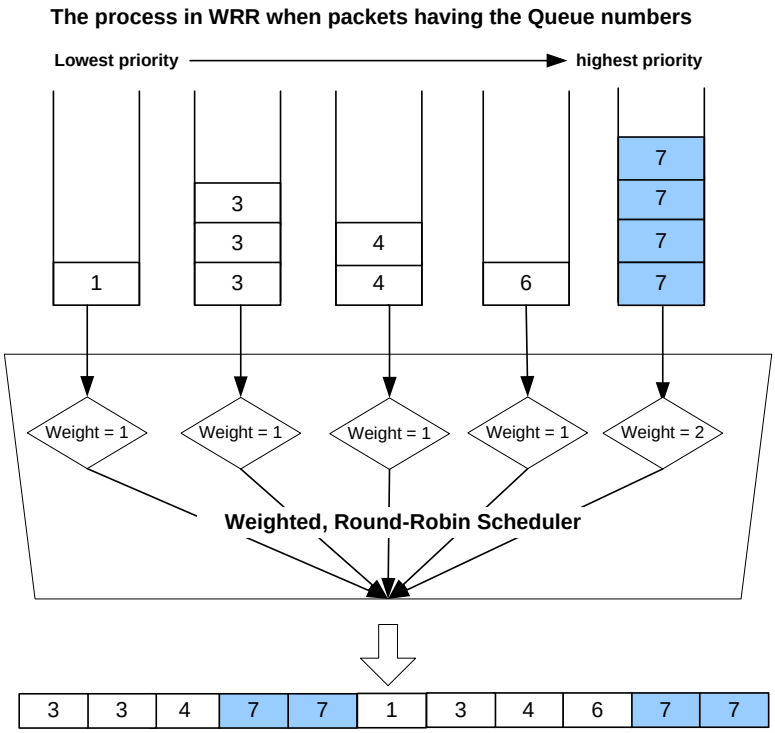


Fig. 7.13 Weighted Round Robin

7.6.9.1 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.

The default scheduling mode is **WRR**. And it is possible to assign a different scheduling mode to each port.

7.6.9.2 Weight and Quantum

To set a weight for WRR scheduling mode, use the following command.

Command	Mode	Description
qos weight *PORTS* <0-3> {<1-127> | **unlimited**}	Global	Sets a weight for each port and queue: PORTS: port numbers 0-3: queue number 1-127: weight value (default: 1) unlimited: strict priority based queuing
qos cpu weight <0-3> {<1-15> | **unlimited**}		Sets a weight of queue for CPU packets: 0-3: queue number 1-15: 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* <0-3> {<1-127> | **unlimited**}	Global	Sets a quantum for each port and queue: PORTS: port numbers 0-3: queue number 1-127: quantum value (default: 1) unlimited: strict priority queuing

7.6.9.3 Maximum and Minimum Bandwidth

To set a maximum bandwidth, use the following command.

Command	Mode	Description
qos max-bandwidth *PORTS* <0-3> {*BANDWIDTH* | **unlimited**}	Global	Sets a maximum bandwidth for each port and queue: PORTS: port numbers 0-3: 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* <0-3> {*BANDWIDTH* | **unlimited**}	Global	Sets a minimum bandwidth for each port and queue: PORTS: port numbers 0-3: 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.

7.6.9.4 Limiting traffic and buffer

To fix the buffer size of a port for incoming traffic control, use the following command.

Command	Mode	Description
qos ibp *PORTS* <1-8191>	Global	Sets the buffer size of the port. The default is 81Kbit. 1-8191: IBP segment limit value (Kbit)
no qos ibp *PORTS*		Removes the fixed size of the port buffer.

You can limit the amount of packet that waits to be processed in a queue and the queue buffer size. For outgoing traffic control, use the following command.

Command	Mode	Description
qos pktlimit *PORTS* <0-3> <4-1023>	Global	Specifies the packet limit value.in the queue. 0-3: queue number 4-1023: packet limit value
qos seglimit *PORTS* <0-3> <1-8191>		Specifies the buffer size of the queue. 0-3: queue number 1-8191: segment limit value
no qos pktlimit *PORTS* <0-3>		Deletes the packet limit value.in the queue.
no qos seglimit *PORTS* <0-3>		Deletes the buffer size of the queue.

You can also limit the number of dynamic cell value per port or system. A cell unit is the pointer of 128 bytes. To set the dynamic cell limit value, use the following command.

Command	Mode	Description
qos dcell-limit *PORTS* <1-8191>	Global	Specifies the dynamic cell limit value.of the port. 1-8191: dynamic cell limit value (default: 1024)
qos total-dcelllimit <1-8191>		Specifies the total dynamic cell limit value. 1-8191: dynamic cell limit value (default: 3864)
no qos dcell-limit *PORTS*		Deletes the dynamic cell limit value.per port
no qos total-dcelllimit		Deletes the dynamic cell of the system.

To display the configuration result of packet and buffer limit, use the following command.

Command	Mode	Description
show qos buffer *PORTS*	Global	Shows the configured packet and buffer limit of the port.

7.6.9.5 The Traffic of Queue

To display the traffic statistic information on each queue, use the following command.

Command	Mode	Description
show queue status *PORTS* [<0-3>]	Enable Global Bridge	Shows the traffic statistic information on each queue.

7.6.9.6 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.

7.7 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 V5812G 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.

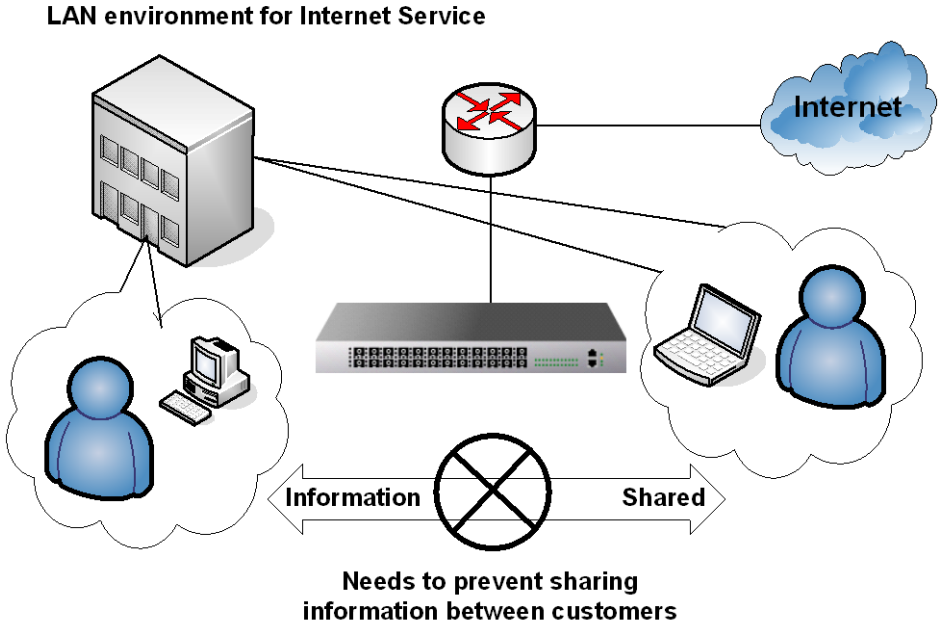


Fig. 7.14 NetBIOS Filtering

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 V5812G 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 V5812G'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 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)

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*		



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**>.

7.13 MAC Filtering

It is possible to forward frame to MAC address of destination. Without specific performance degradation, maximum 4096 MAC addresses can be registered.

7.13.1 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)#
```

7.13.2 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.

7.13.3 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.

7.13.4 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.

7.14 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. Dasan Networks switches and DSLAMs find their 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.

7.14.1 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 V5812G 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.

7.14.1.1 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.

7.14.1.2 ARP Log Interval

To set the interval for displaying the syslog messages of duplicate address detection with ARP, use the following command.

Command	Mode	Description
arp logs interval <1-65536>	Global	Sets the interval for displaying syslog messages of duplicate address detection with ARP. 1-65536: interval value in second (default: 300s)
no arp logs interval		Deletes the configured interval for displaying syslog messages of duplicate address detection with ARP.

7.14.1.3 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*}		
show arp flag-mask-count		

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   00:d0:cb: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#
```

7.14.2 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 V5812G 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.

7.14.3 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.

7.14.3.1 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.



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.

7.14.3.2 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.

7.14.3.3 ARP Address Validation

The V5812G 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.

The **src-mac**, **dst-mac**, and **ip** options can be configured together.

7.14.3.4 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.

7.14.3.5 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 V5812G 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.

7.14.3.6 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.

7.14.4 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.

7.14.5 Proxy ARP

The V5812G 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.

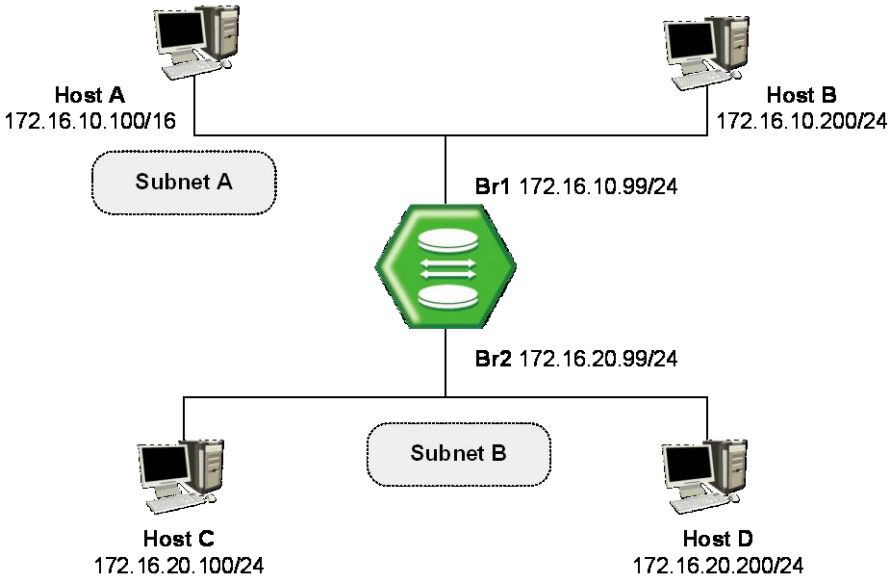


Fig. 7.15 Proxy ARP

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 V5812G's br1 interface, but does not reach the host D. By default, the V5812G does not forward broadcasts. Since the V5812G 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 V5812G 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 V5812G. Since the V5812G 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 V5812G for all the hosts on the subnet B. Hence, all packets destined to the subnet B are sent to the router. The V5812G 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.

7.15 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.

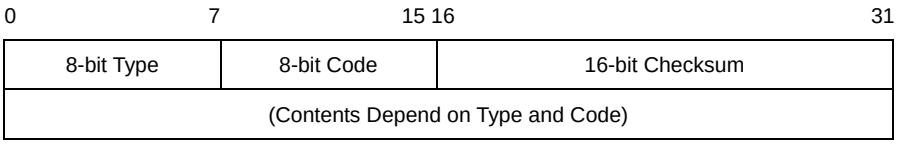


Fig. 7.16 ICMP Message Structure

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.

7.15.1 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.

7.15.2 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_PARAMETERPROB (12)	ON

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)

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.

7.16 TCP Flag Control

Transmission Control Protocol (TCP) header includes six kinds of flags that are URG, ACK, PSH, RST, SYN, and FIN. For the V5812G, you can configure RST and SYN as the below.

7.16.1 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.

7.16.2 SYN Configuration

SYN sets up TCP connection. The V5812G 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.

7.17 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 V5812G 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.

The V5812G also provides debug command for Layer 3 routing protocols (BGP, OSPF, RIP and PIM). If you want to debug about them, refer to the each configuration chapter.

7.17.1 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.

7.17.2 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

7.17.3 Debug Packet Dump

The V5812G 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.



You can save a current configuration with the **write memory** command. However, the dump file will not be saved.

7.17.4 Displaying Dump Packets

To display the dump packets, use the following command.

Command	Mode	Description
show dump packets	Enable Global	Shows the dump packets.

7.17.5 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.



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.

7.18 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 V5812G 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. For example, ACL could be applied to another command such as **ip igmp access-group** or **ip pim rp-address**. 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
```



Scan through conditions in the order of creation

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.

7.18.1 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)#
```

7.18.2 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> | <2000-2699>} {**deny** | **permit**} **ip host** *A.B.C.D* **host** *A.B.C.D*		Specifies a deny or permit statement of the extended 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> | <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)#
```

7.18.3 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

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)#
```

7.18.4 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> | *WORD*} **remark** *LINE*	Global	Writes comments for the specified ACL range. 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.

7.18.5 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.

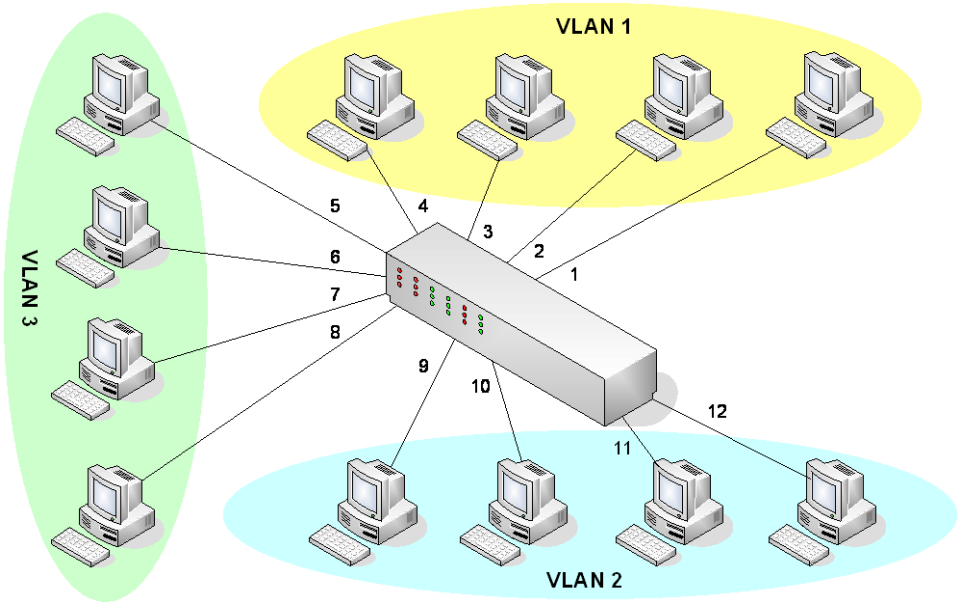


Fig. 8.1 Port-based VLAN

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.

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 V5812G 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 V5812G 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.

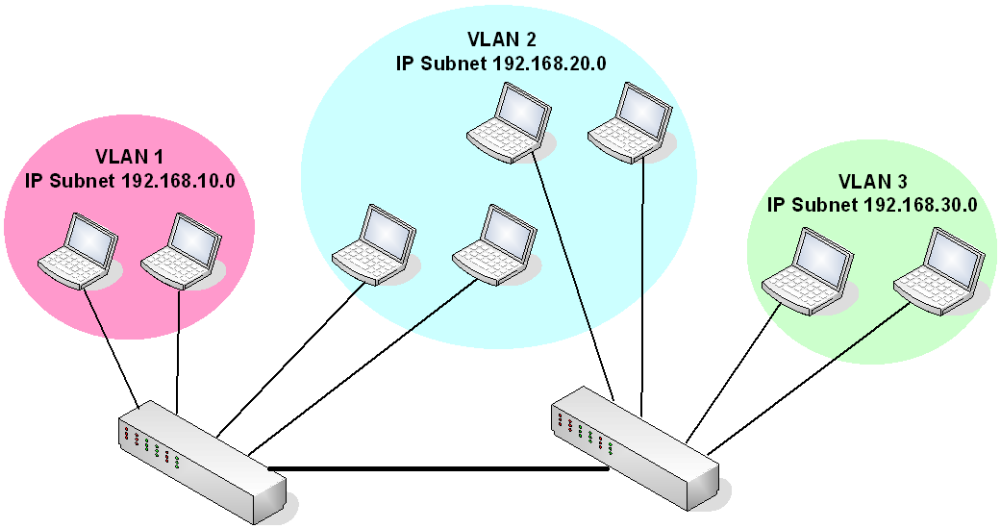


Fig. 8.2 Subnet-based VLAN

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)

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.

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 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.

8.1.7 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.

8.1.8 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 port protected		Shows port isolation configuration.

8.1.9 QinQ

QinQ or Double Tagging is one way for tunneling between several networks.

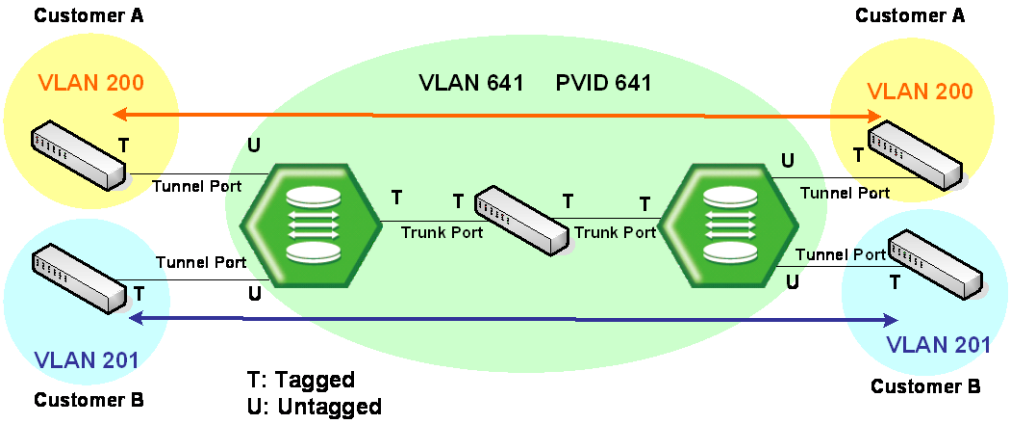


Fig. 8.3 Example of QinQ Configuration

If QinQ is configured on the V5812G, 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.

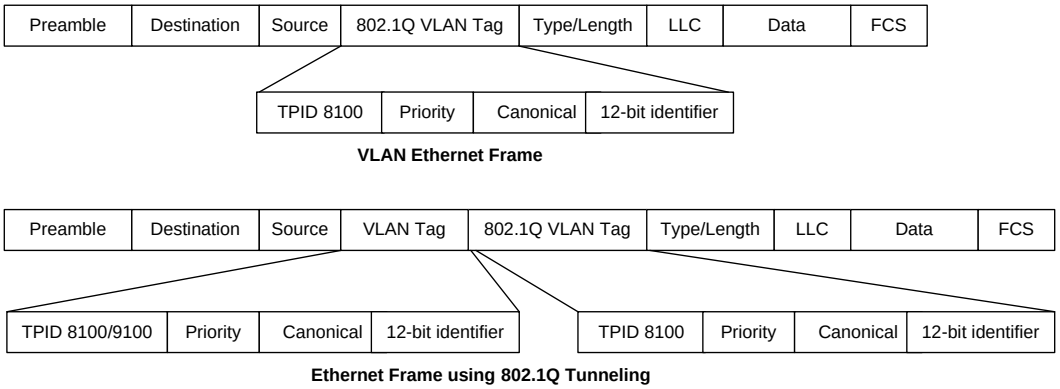


Fig. 8.4 QinQ Frame

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.

8.1.9.1 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 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 V5812G switch has 0x8100 TPID value as default and other values are used as hexadecimal number.

8.1.9.2 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	Configures a qinq port. 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	Configures a qinq port. PORTS: qinq port to be disabled

i When you configure Double tagging on the V5812G, 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

8.1.9.3 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.

Use the following command to set TPID on a QinQ port.

Command	Mode	Description
vlan dot1q-tunnel tpid *TPID*	Bridge	Configures TPID.

8.1.10 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 V5812G 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 V5812G switch, refer to Port Isolation configuration.

8.1.10.1 Port Isolation

trong 1 vlan . none conversation

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.

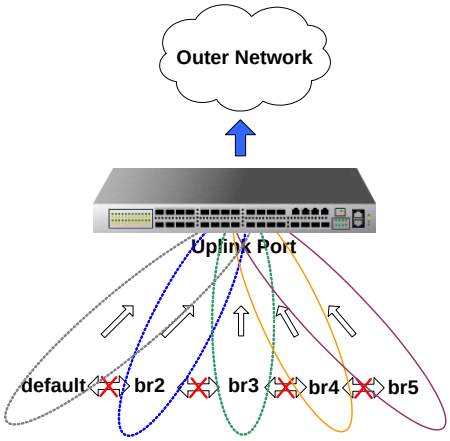
Command	Mode	Description
port protected *PORTS*	Bridge	Enables port isolation.
no port protected [*PORTS*]		Disables port isolation.

To display the configured port isolation, use the following command.

Command	Mode	Description
show port protected	Enable Global Bridge	Shows port isolation configuration.

8.1.10.2 Shared VLAN

This chapter is only for Layer 2 switch operation. The V5812G is Layer 3 switch, but it can be used for Layer 2 also. 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 V5812G 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...uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu
     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.

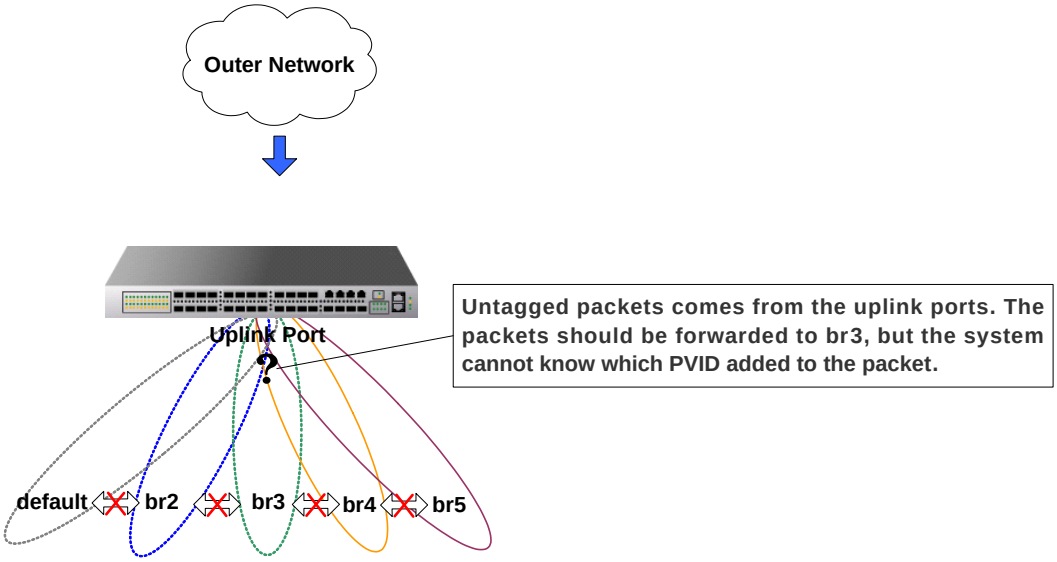
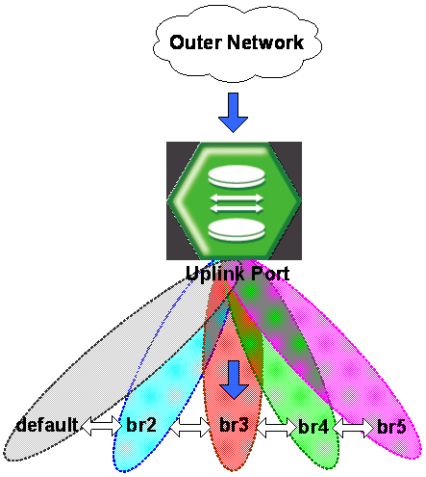


Fig. 8.6 Incoming Packets under Layer 2 Shared VLAN Environment (1)

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) |1234567890123456789012345678901234567890123456789012
-------------------------------------------------------------------------
 default(   1|   6) |u...uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu
     br2(   2|   6) |.u.....................u.................
     br3(   3|   6) |..u.....................u................
     br4(   4|   6) |...u.....................u...............
     br5(   5|   6) |....u.....................u..............
     br6(   6|   6) |uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu

SWITCH(bridge)#
```

Fig. 8.7 Incoming Packets under Layer 2 Shared VLAN Environment (2)

In conclusion, to use the V5812G 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.

8.1.11 VLAN Translation

VLAN Translation is simply an action of Rule. This function is to translate the value of specific VLAN ID which classified by Rule. The switch makes Tag adding PVID on Untagged packets, and use Tagged Packet as it is. That is, all packets are tagged in the Switch, and VLAN Translation is to change the VLAN ID value of Tagged Packet in the Switch. This function is to adjust traffic flow by changing the VLAN ID of packet.

Step 1 Open *Rule Configuration* mode using the **flow** *NAME* **create** command.
See Section 7.6.2.2.

Step 2 Classify the packet that VLAN Translation will be applied by Rule.
See Section 7.6.2.3.

Step 3 Designate the VLAN ID that will be changed in the first step by the **match vlan** <1-4094> command.

Step 4 Open *Bridge Configuration* mode using the **bridge** command.

Step 5 Add the classified packet to VLAN members of the VLAN ID to be changed to.

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) |12345678901234567890123456789012345678901234
      ----------------------------------------------------------------
       default(   1|   1) |u...uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu
           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 >

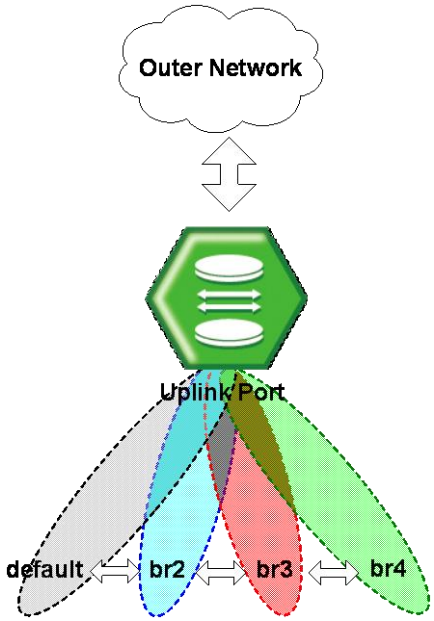
```
SWITCH(bridge)# vlan dot1q-tunnel enable 10
SWITCH(bridge)# vlan pvid 10 11
SWITCH(bridge)# show vlan dot1q-tunnel
          Tag Protocol Id : 0x8100 (d: double-tagging port)
        ------------------------------------------------------
             |        1        2        3        4
          Port |12345678901234567890123456789012345678901234
        ------------------------------------------------------
          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 |12345678901234567890123456789012345678901234
        ------------------------------------------------------
          dtag  ..........d...............................
SWITCH(bridge)#
```

Sample Configuration 5: Configuring Shared VLAN with FID

Configure br2, br3, br4 in the V5812G 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) |12345678901234567890123456789012345678901234
      ------------------------------------------------------------------
       default(   1|   5)  |uu......uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu
           br2(   2|   5)  |..uu..................u...................
           br3(   3|   5)  |....uu................u...................
           br4(   4|   5)  |......uu..............u...................
           br5(   5|   5)  |uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu
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.

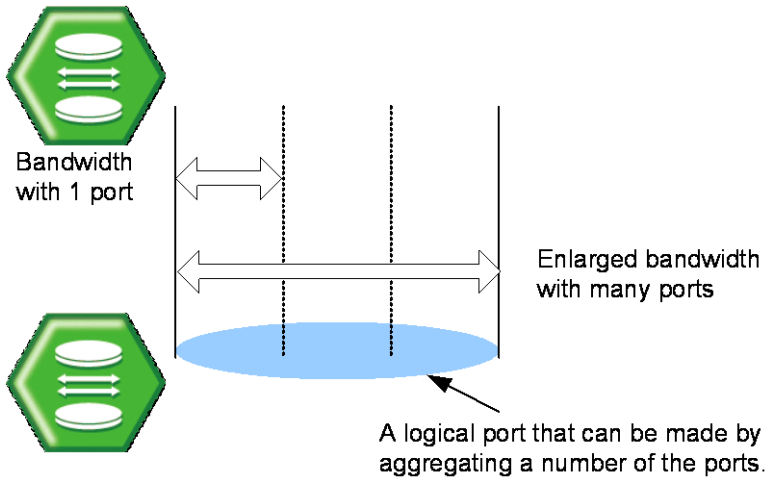


Fig. 8.8 Link Aggregation

The V5812G 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 <0-5>
trunk distmode *GID* {**dstip** | **dstmac** | **srcdstip** | **srcdstmac** | **srcip** | **srcmac**}		Selects the distribution mode for a specified aggregation group. (default: srcdstmac)

i It is possible to input 0 to 5 to the trunk group ID because the V5812G supports 6 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 V5812G 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*		



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.

LACP can generate up to 6 aggregators whose number value could be 0 to 5. 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

điều kiện cùng 3 tham số : Vlan , speed ,

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 5).

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 V5812G 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.

For the V5812G, 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(0-5) 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

active mode

passive 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 quan tâm 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)

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 V5812G, 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.

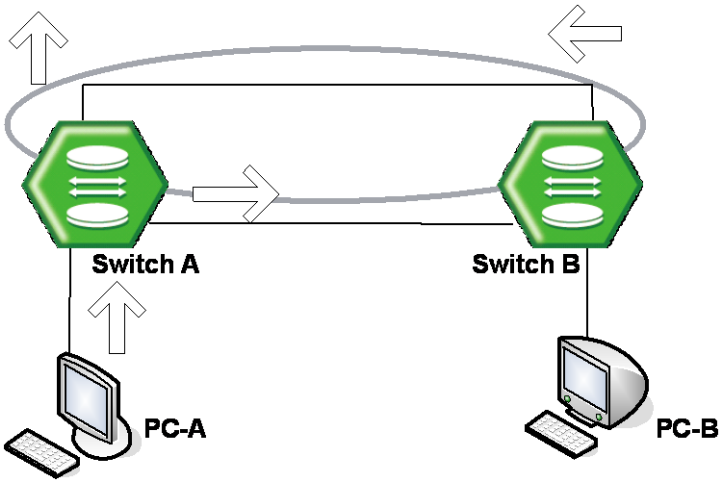


Fig. 8.9 Example of Loop

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.

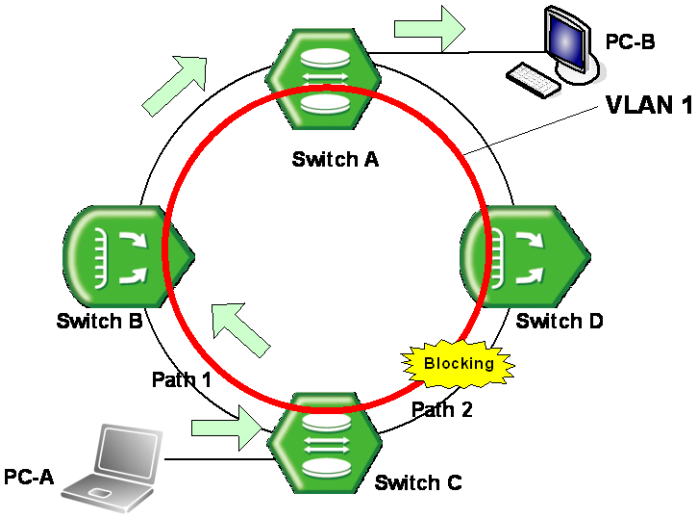


Fig. 8.10 Principle of Spanning Tree Protocol

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.

The V5812G provides STP, RSTP and MSTP. For more detail description of STP and RSTP, refer to the following sections.

- STP Operation
- RSTP Operation
- MSTP Operation
- Configuring STP/RSTP/MSTP/PVSTP/PVRSTP Mode (Required)
- Configuring PVSTP/PVRSTP
- Root Guard
- Restarting Protocol Migration
- BPDU Configuration
- Sample Configuration

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.

Root Switch

The critical information to decide a root switch is the bridge ID. Bridge ID is composed of two bytes-priority and six bytes-MAC address. The root switch is decided with the lowest bridge ID.

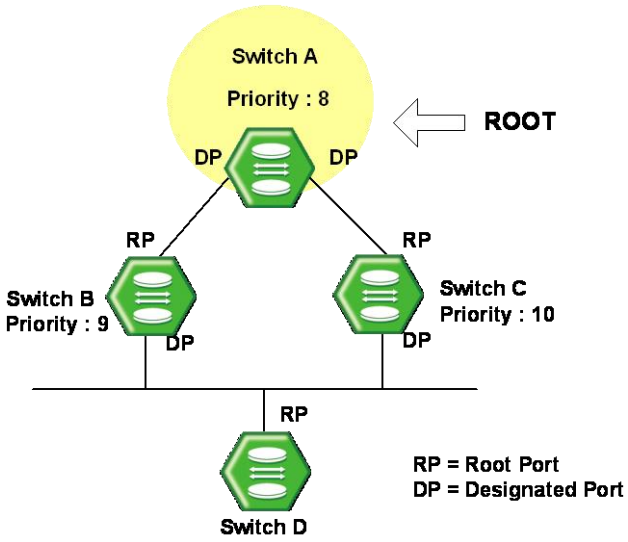


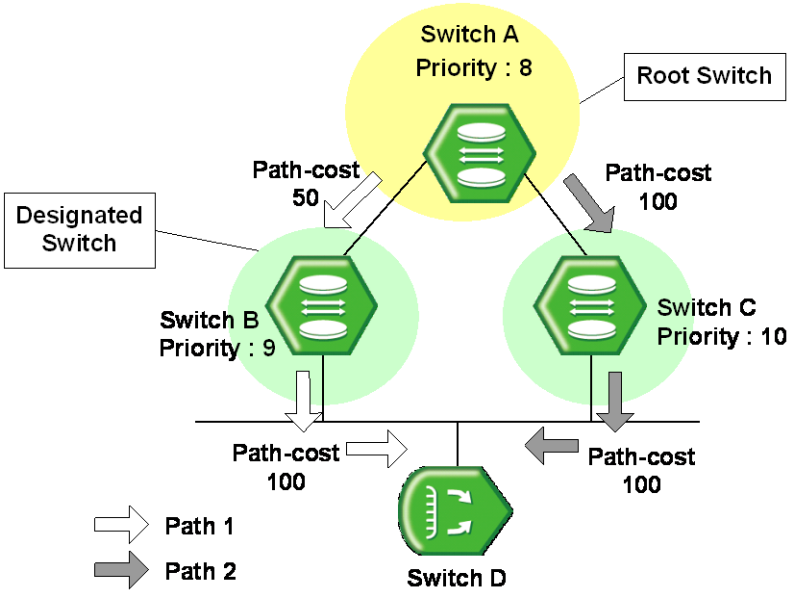
Fig. 8.11 Root Switch

After configuring STP, 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 root switch.

Designated Switch

After deciding a root switch, when SWITCH A transmits packet to SWITCH C, SWITCH A compares the exchanged BPDU to decide a path. The critical information to decide path is path-cost. Path-cost depends on the transmit rate of LAN interface and path with lower path-cost is selected.

The standard to decide a designated switch is total root path-cost which is added with path-cost to the root switch. Path-cost depends on transmit rate of switch LAN interface and switch with lower path-cost is selected to be a 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 picture showing SWITCH C sends packet, path-cost of PATH 1 is 150 and path- cost of PATH 2 is total 200(100 + 100 ; path-cost of SWITCH C to B + path-cost of SWITCH B to C). Therefore lower path-cost, PATH 1 is chosen. In this case, port connected to root switch is named root port. In the above picture, port of SWITCH C connected to SWITCH A as Root switch is root port. There can be only one root port on equipment.

i When root path-costs are same, bridge ID is compared.

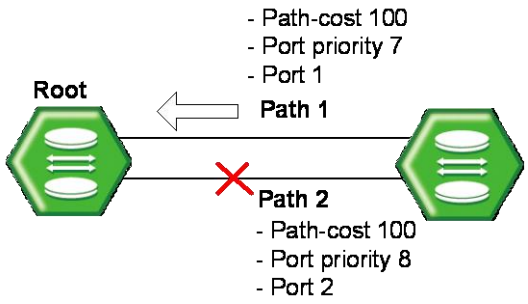
Designated Port and Root Port

A root port is the port in the active topology that provides connectivity from the designated switch toward the root. A designated port is a port in the active topology used to forward traffic away from the root onto the link for which this switch is the designated switch. That is; except root port in each switch, the selected port to communicate is a designated port.

Port Priority

Meanwhile, when the path-cost of two paths are same, port-priority is compared. As the below picture, suppose that two switches are connected. Since the path-costs of two paths are 100, same, their port priorities are compared and port with smaller port priority is selected to transmit packet.

i All these functions are automatically performed by BPDU, which is the bridge information exchanged between switches to activate or disable a specific port. It is also possible to configure BPDU to change a root switch or 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.

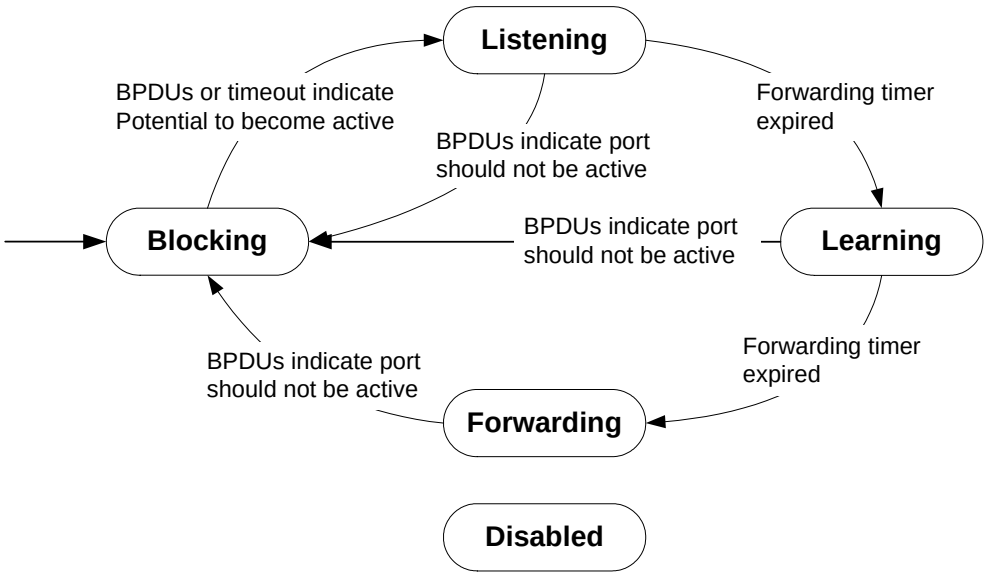


Fig. 8.14 Port State

- **Blocking**
  a port that is enabled, but that is 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 for 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 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 some time 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.

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.

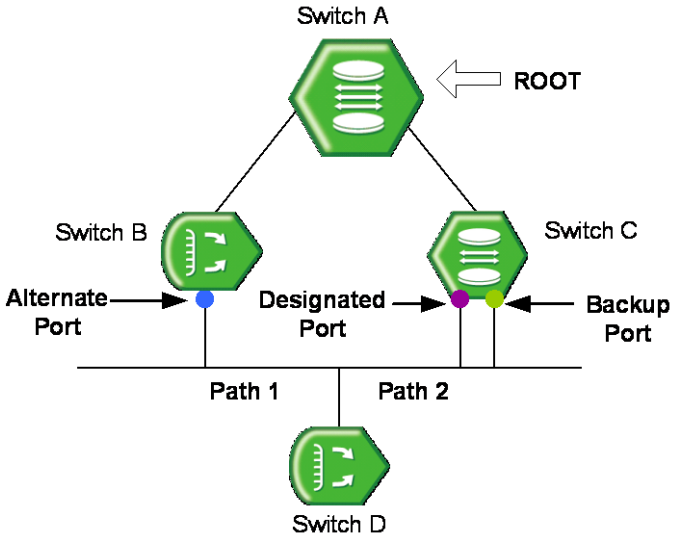


Fig. 8.15 Alternate Port and Backup Port

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.

BPDU Policy

In 802.1d, only root switch can generate BPDU every hello time and other swithches cannot. They can create BPDU when receiving BPDU from the root switch. However, in 802.1w not only root switch but also all the other switches forward BPDU following Hello-time. BPDU is more frequently issued than the interval the root switch exchanges, but with 802.1w conversion to the forwarding state become faster to keep up with changing network.

By the way, when low BPDU is received from root switch or designated switch, it is immediately accepted. For example, suppose that root switch is disconnected to SWITCH B. Then, SWITCH B is considered to be root because of the disconnection and forwards BPDU.

However, SWITCH C recognizes root existing, so it transmits BPDU including information of root to Bridge B. Thus, SWITCH B configures a port connected to SWITCH C as new root port.

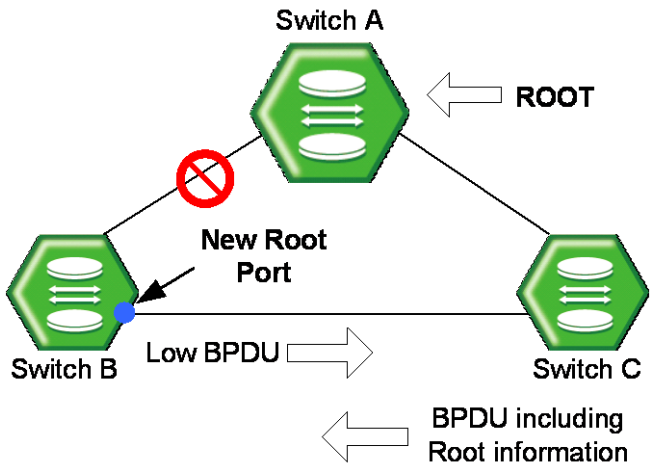


Fig. 8.16 Example of Receiving Low BPDU

Rapid Network Convergence

A new link is connected between SWITCH A and root. Root and SWITCH A is not directly connected, but indirectly through SWITCH D. After SWITCH A is newly connected to root, packet cannot be transmitted between the ports because state of two switches becomes listening, and no loop is created.

In this state, if root transmits BPDU to SWITCH A, SWITCH A transmits new BPDU to SWITCH A and SWITCH C, switch C transmits new BPDU to SWITCH D. SWITCH D, which received BPDU from SWITCH C makes port connected to SWITCH C Blocking state to prevent loop after new link.

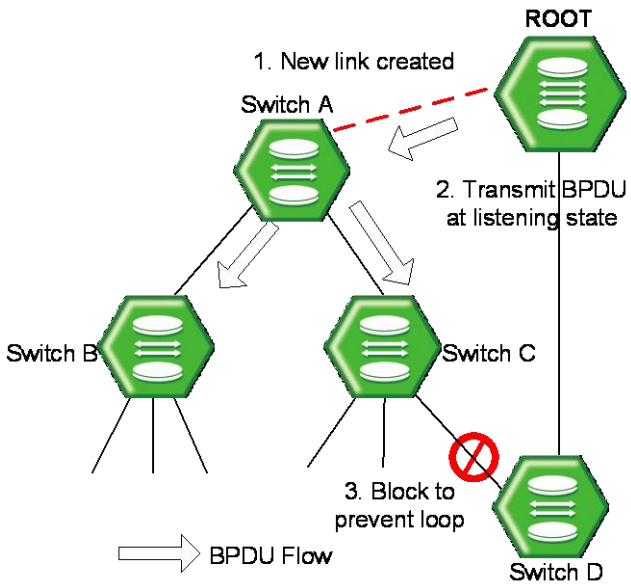


Fig. 8.17 Network Convergence of 802.1d

This is very epochal way of preventing a loop. The matter is that communication is

disconnected during two times of BPDU Forward-delay till a port connected to switch D and SWITCH C is blocked. Then, right after the connection, it is possible to transmit BPDU although packet cannot be transmitted between switch A and root.

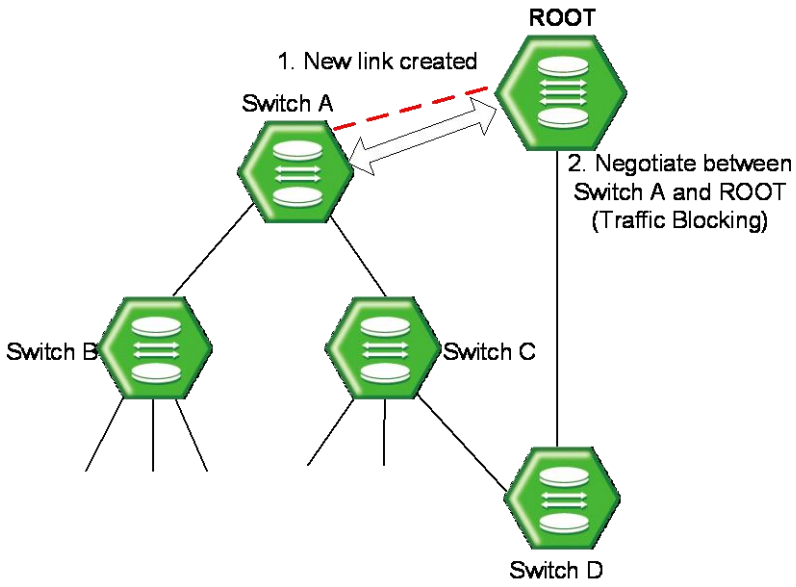


Fig. 8.18 Network Convergence of 802.1w (1)

SWITCH A negotiates with root through BPDU. To make link between SWITCH A and root, port state of non-edge designated port of SWITCH is changed to blocking. Although SWITCH A is connected to root, loop will not be created because SWITCH A is blocked to SWITCH Band C. In this state, BPDU form root is transmitted to SWITCH B and C through SWITCH A. To configure forwarding state of SWITCH A, SWITCH A negotiates with SWITCH B and SWITCH C.

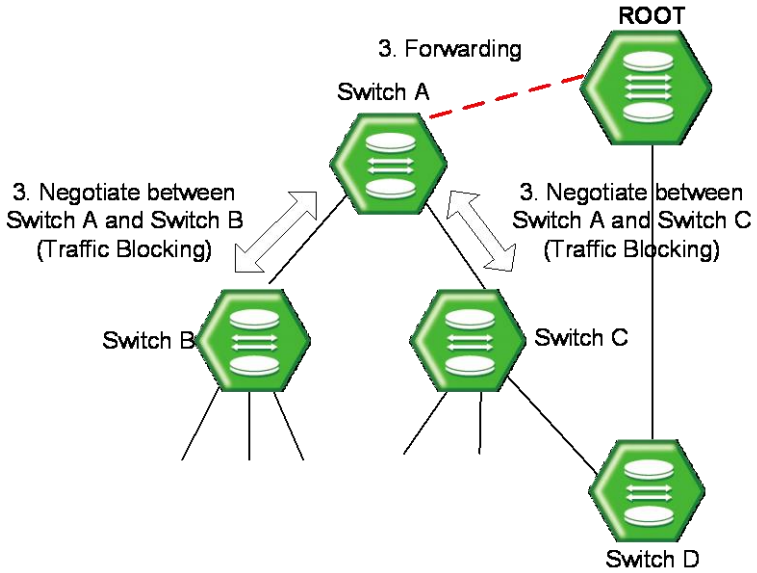


Fig. 8.19 Network Convergence of 802.1w (2)

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 forwarding state of SWITCH A. However since SWITCH C has a port connected to SWITCH D, you should make blocking state of the port.

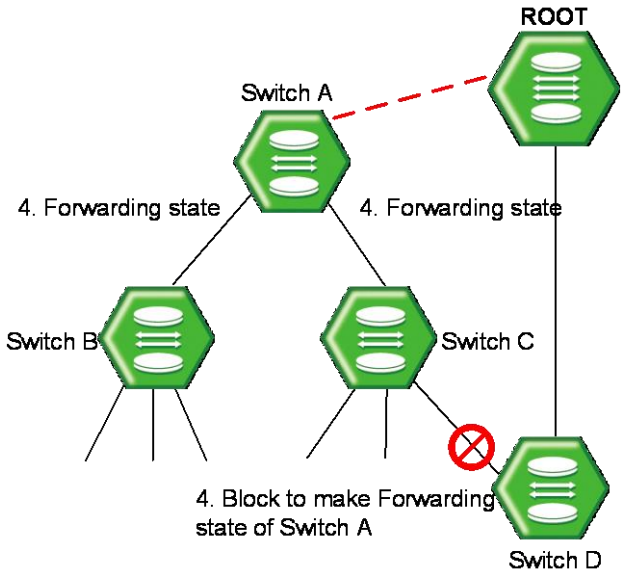


Fig. 8.20 Network Convergence of 802.1w (3)

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 forwarding state of specific port. So it is very fast progressed. During progress to forwarding state of port, listening and learning are not needed. These negotiations use BPDU.

Compatibility with 802.1d

RSTP internally includes STP, so it has compatibility with 802.1d. Therefore, RSTP can recognize BPDU of STP. But, STP cannot recognize BPDU of RSTP. For example, assume that SWITCH A and SWITCH B are operated as RSTP and SWITCH A is connected to SWITCH C as designated switch. Since SWITCH C, which is 802.1d ignores RSTP BPDU, it is interpreted that switch C is not connected to any switch or segment.

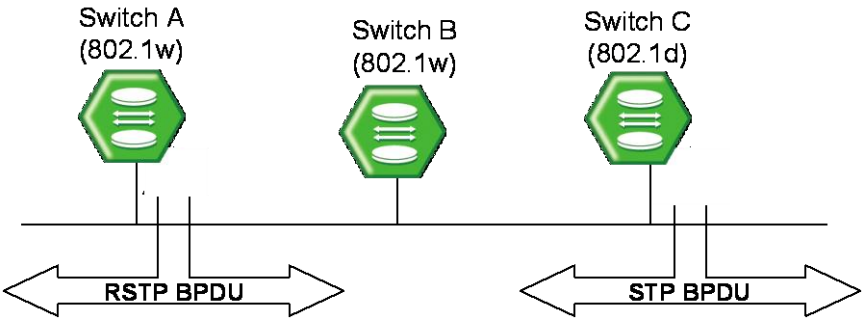


Fig. 8.21 Compatibility with 802.1d (1)

However, SWITCH A converts a port received BPDU into RSTP of 802.1d because it can read BPDU of SWITCH C. Then SWITCH C can read BPDU of SWITCH A and accepts SWITCH A as designated switch.

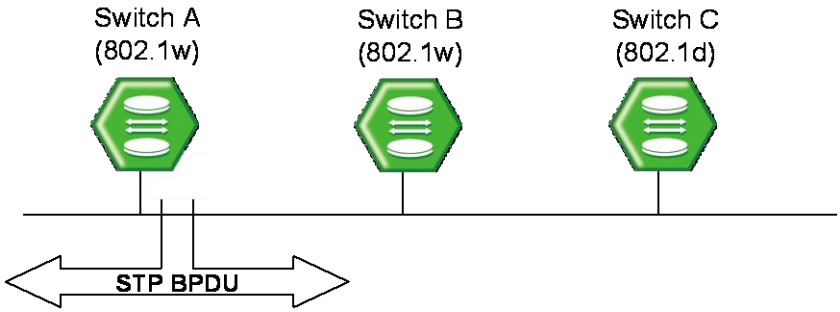


Fig. 8.22 Compatibility with 802.1d (2)

8.3.3 MSTP Operation

To operate the network more efficiently, the V5812G uses MSTP (Multiple Spanning-Tree Protocol). It constitutes the network with VLAN subdividing existing LAN domain logically and configure the route by VLAN or VLAN group instead of existing routing protocol.

Operation

Here explains how STP/MSTP differently operates on the LAN. Suppose to configure 100 of VLANs from SWITCH A to B and C. In case of STP, there is only one STP on all the VLANs and it does not provide multiple instances.

While the existing STP is a protocol to prevent a loop in a LAN domain, MSTP establishes STP per VLAN in order to realize routing suitable to 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, it realizes load balancing and provides many VLANs through Instances.

MSTP

In MSTP, VLAN is classified to groups with same configuration ID. Configuration ID is composed of revision name, region name and VLAN/instance mapping. Therefore, to have same configuration ID, all of these tree conditions should be the same. VLAN classified with same configuration ID is called an MST region. In a region, there is only one STP so that it is possible to reduce the number of STP comparing to PVSTP. There's no limitation for region in a network environment but it is possible to generate Instances up to 64. Therefore instances can be generated from 1 to 64. Spanning-tree which operates 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 exchange BPDU and CST root which is decided by comparing their BPDU. Here, the switches that do not operate with MSTP have instance 0 so that they can also join BPUD exchanges. The operation of deciding CST root is CIST (Common & Internal Spanning-Tree).

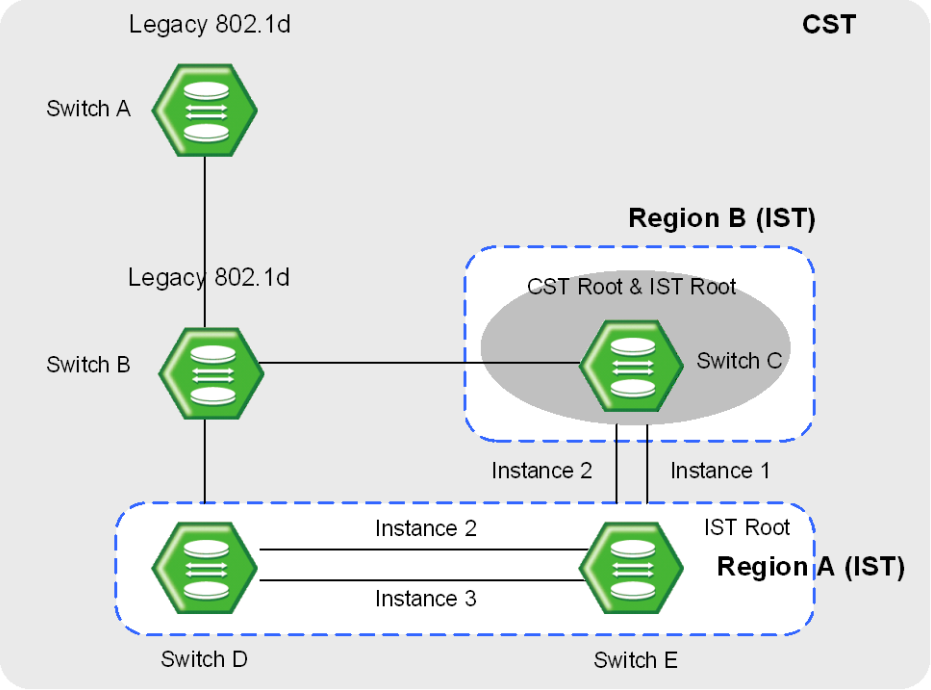


Fig. 8.23 CST and IST of MSTP (1)

In CST, SWITCH A and B are operating with STP and SWITCH C, D and E are operating with MSTP. First, in CST, CIST is established to decide a CST root. After the CST root is decided, the closest switch to the CST root is decided as IST root of the region. Here, CST root in IST is an IST root.

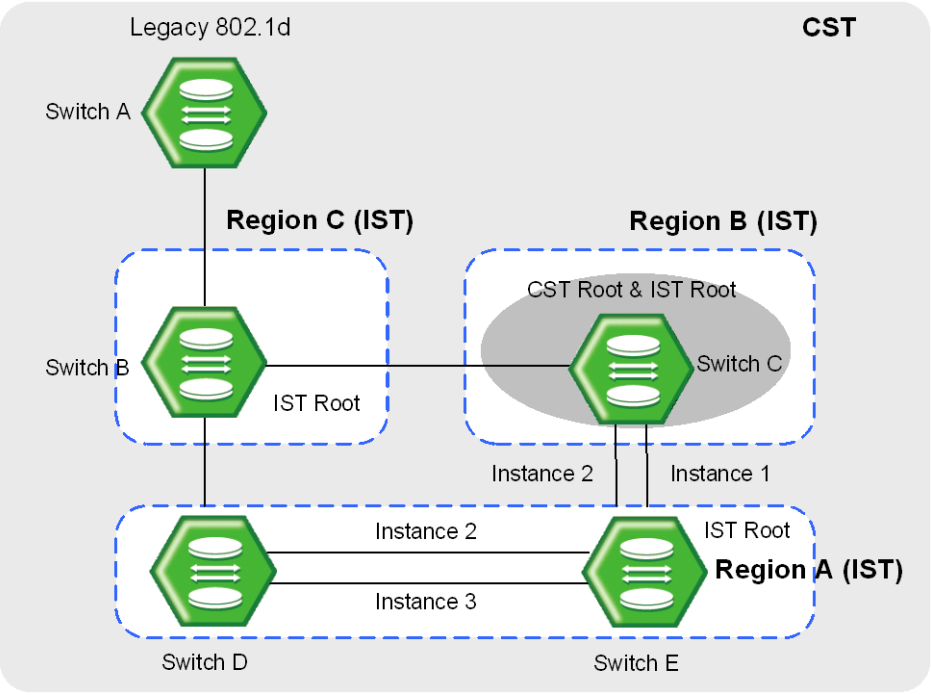


Fig. 8.24 CST and IST of MSTP (2)

In the above situation, if SWITCH B operates with MSTP, it will send its BPDU to the CST root and IST root in order to request itself to be a CST root. However, if any BPDU having higher priority than that of SWITCH B is sent, SWITCH B cannot be a CST root.

For the V5812G, the commands configuring MSTP are also used to configure STP and RSTP.

8.3.4 Configuring STP/RSTP/MSTP/PVSTP/PVRSTP Mode (Required)

To configure STP, first of all, configure force-version in order to decide the mode.

To decide force-version, use the following command.

Command	Mode	Description
stp force-version {**stp** | **rstp** | **mstp** | **pvstp** | **pvstp+** | **pvrstp** | **pvrstp+**}	Bridge	Configures force-version in the bridge.

To clear STP configuration from the switch, use the following command.

Command	Mode	Description
no stp force-version	Bridge	Clears force-version configuration.

8.3.5 Configuring STP/RSTP/MSTP

To configure STP and RSTP, use the following steps.

Step 1 Decide STP mode using the **stp force-version** {**stp** | **rstp**} command.

Step 2 Activate MST daemon using the **stp mst enable** command.

Step 3 Configure detail options if specific commands are required.

8.3.5.1 Activating STP/RSTP/MSTP

To enable/disable STP, RSTP, and MSTP in the force-version, use the following command.

Command	Mode	Description
stp mst {**enable** | **disable**}	Bridge	Enables/disables STP, RSTP or MSTP function.

Even though STP function does not operate, loop event does not occur in a switch which belongs to the non-dual path LAN environment.

8.3.5.2 Root Switch

To establish STP, RSTP, or MSTP function, first of all, a root switch should be decided. In STP or RSTP, it is named as root switch and in MSTP it is as IST root switch. Each switch has its own bridge ID, and root switch on same LAN is decided by comparing their bridge ID. However, the user can change the root switch by configuring priority for it. The switch

having the lowest priority is decided as root switch.

To change the root switch by configuring priority for it, use the following command.

Command	Mode	Description
stp mst priority *MSTID-RANGE* <0-61440>	Bridge	Configures the priority of the switch: MSTID-RANGE: select instance number 0. 0-61440: priority value in steps of 4096 (default: 32768)
no stp mst priority *MSTID-RANGE*		Clears the Priority of the switch, enter the instance number.

8.3.5.3 Path-cost

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	Path-cost
4M	250
10M	100
100M	19
1G	4
10G	2

Tab. 8.2 STP Path-cost

Transmit Rate	Path-cost
4M	20000000
10M	2000000
100M	200000
1G	20000
10G	2000

Tab. 8.3 RSTP Path-cost

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 configure the path-cost, use the following command.

Command	Mode	Description
stp mst path-cost *MSTID-RANGE PORTS* <1-200000000>	Bridge	Configures path-cost to configure route: MSTID-RANGE: select instance number (0-64). PORTS: select the port number. 1-200000000: enter the path cost value.
no stp mst path-cost *MSTID-RANGE PORTS*		Clears the configured path-cost, enter the instance number and the port number.

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. In order to configure port-priority, use the following command.

Command	Mode	Description
stp mst port-priority *MSTID-RANGE PORTS* <0-240>	Bridge	Configures port-priority.
no stp mst port-priority *MSTID-RANGE PORTS*		Disables port priority configuration.

8.3.5.5 MST Region

If MSTP is established in the V5812G, decide a MST 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.

Command	Mode	Description
stp mst config-id name *NAME*	Bridge	Designate the name for the region: name: set the MST region name. NAME: enter name to give the MST region.
stp mst config-id map <1-64> *VLAN-RANGE*		Configure the range of VLAN that is going to be grouping as a region: 1-64: select an instance ID number. VLAN-RANGE: enter a number of the VLANs to be mapped to the specified instance.
stp mst config-id revision <0-65535>		Configure the switches in the same MST boundary as same number: 0-65535: set the MST 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.

To delete the configuration ID, use the following command.

Command	Mode	Description
no stp mst config-id	Bridge	Delete the entire configured configuration ID.
no stp mst config-id name		Deletes the name of region, enter the MST region name.
no stp mst config-id map <1-64> *VLAN-RANGE*		Deletes entire VLAN-map or part of it, select the instance ID number and the number of the VLANs to remove from the specified instance.
no stp mst config-id map <1-64>		Deletes entire VLAN-map or part of it, select the instance ID number.
no stp mst config-id revision		Deletes the configured revision number.

After configuring the configuration ID in the V5812G, 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 switch after configuring the configuration ID, use the following command.

Command	Mode	Description
stp mst config-id commit	Bridge	Commits the configuration of the region.

i After deleting the configured configuration ID, apply it to the switch using the above command.

8.3.5.6 MSTP Protocol

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 protocol manually.

To configure the protocol, use the following command.

Command	Mode	Description
stp clear-detected-protocol *PORTS*	Bridge	Clears detected protocol: PORTS: select the port number.

8.3.5.7 Point-to-point MAC Parameters

The internal sublayer service makes available a pair of parameters that permit inspection of, and control over, the administrative and operational state of the point-to-point status of the MAC entity by the MAC relay entity.

To configure the point-to-point status, use the following command.

Command	Mode	Description
stp point-to-point-mac *PORTS* {**auto** | **force-true** | **force-false**}	Bridge	Sets point-to-point MAC: PORTS: select the port number auto: auto detect force-true: force to point-to-point MAC force-false: force to shared MAC (not point-to point MAC)

True means, the MAC is connected to a point-to-point LAN, i.e., there is at most one other system attached to the LAN. False means, the MAC is connected to a non point-to-point LAN, i.e., there can be more than one other system attached to the LAN.

To delete the point-to-point configuration, use the following command.

Command	Mode	Description
no stp point-to-point-mac *PORT*	Bridge	Deletes point-to-point MAC configuration

8.3.5.8 Edge Ports

Edge ports are used for connecting end devices. There are no switches or spanning-tree bridges after the edge port. To configure the edge port mode, use the following command.

Command	Mode	Description
stp edge-port *PORTS*	Bridge	Sets port edge mode: PORTS: select the port number.
no stp edge-port *PORTS*		Deletes port edge mode

To configure an edge port mode with the default values, use the following command.

Command	Mode	Description
stp edge-port default	Bridge	Sets a default port edge mode:
no stp edge-port default		Deletes a configured default port edge mode.

8.3.5.9 Displaying Configuration

To display the configuration after configuring STP, RSTP, and MSTP, use the following command.

Command	Mode	Description
show stp	Enable Global Bridge	Shows the configuration of STP/RSTP/MSTP.
show stp mst *MSTID-RANGE*		Shows the configuration of specific Instance, enter the instance number.
show stp mst *MSTID-RANGE* [**all** | *PORTS*] [**detail**]		Shows the configuration of the specific Instance for the ports: MSTID-RANGE: select the MST instance number.

		all: select all ports. PORTS: select port number. detail: show detail information (as option).

With the **show stp** command, it is possible to check the information for STP/RSTP/MSTP. How to distinguish them is to check which one is marked on the **mode**.

In case STP or RSTP is configured in the V5812G, you should configure *MSTID-RANGE* as 0.

To display the configured MSTP of the switch, use the following command.

Command	Mode	Description
show stp mst config-id {**current** | **pending**}	Enable Global Bridge	Shows the MSTP configuration identifier: current: shows the current configuration as it is used to run MST. pending: shows the edited configuration.

For example, after user configures the configuration ID, if you apply it to the switch with the **stp mst config-id commit** command, you can check the configuration ID with the **show stp mst config-id current** command.

However, if the user did not use the **stp mst config-id commit** command in order to apply to the switch after configuration, the configuration could be checked with the **show stp mst config-id pending** command.

8.3.6 Configuring PVSTP/PVRSTP

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.

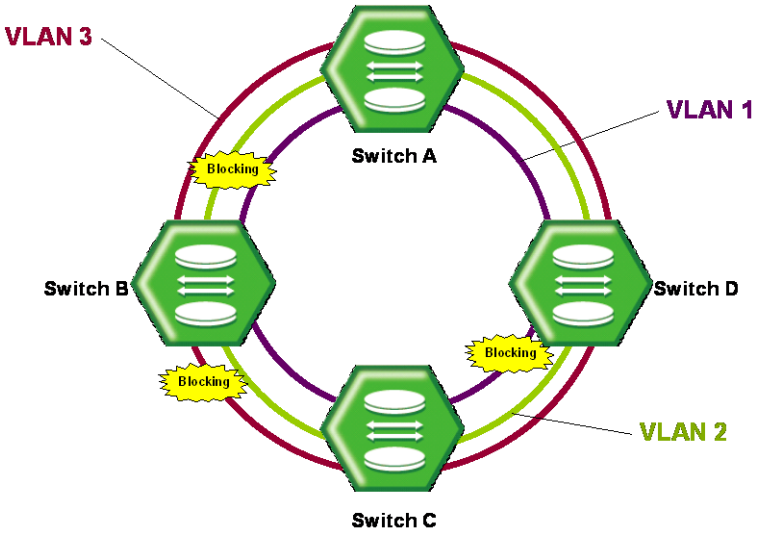


Fig. 8.25 Example of PVSTP

8.3.6.1 Activating PVSTP/PVRSTP

To configure PVSTP or PVRSTP, configure force-version in order to decide the mode. In order to decide force-version, use the following command.

Command	Mode	Description
stp pvst enable *VLAN-RANGE*	Bridge	Activates PVSTP or PVRSTP function.

PVSTP is activated after selecting PVSTP in Force-version using the above command and PVRSTP is activated after selecting PVRSTP using the above commands. In PVSTP and PVRSTP, it is possible to configure only the current VLAN. If you input VLAN that does not exist, error message is displayed.

For the switches in LAN where dual path doesn't exist, Loop does not generate even though STP function is not configured. To disable configured PVSTP, PVRSTP, use the following command.

Command	Mode	Description
stp pvst disable	Bridge	Disables PVSTP or PVRSTP in VLAN.

8.3.6.2 Root Switch

To establish PVSTP and PVRSTP function, first of all, Root switch should be decided. Each switch has its own Bridge ID and Root switch on same LAN is decided by comparing their Bridge ID. However, the user can change Root switch by configuring Priority for it. The switch having the lowest priority is decided as Root switch.

To change Root switch by configuring Priority for it, use the following command.

Command	Mode	Description
stp pvst priority *VLAN-RANGE* <0-61440>	Bridge	Configures a priority of switch.
no stp pvst priority *VLAN-RANGE*		Clears a priority of switch.

8.3.6.3 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 Path-cost, use the following command.

Command	Mode	Description
stp pvst path-cost *VLAN-RANGE PORTS* <1-200000000>	Bridge	Configures path-cost to configure route on user's own.
no stp pvst path-cost *VLAN-RANGE PORTS*		Clears path-cost configuration.

8.3.6.4 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 port priority, use the following command.

Command	Mode	Description
stp pvst port-priority *VLAN-RANGE PORTS* <0-240>	Bridge	Configures port-priority.
no stp pvst port-priority *VLAN-RANGE PORTS*		Disables port priority configuration.

8.3.7 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.

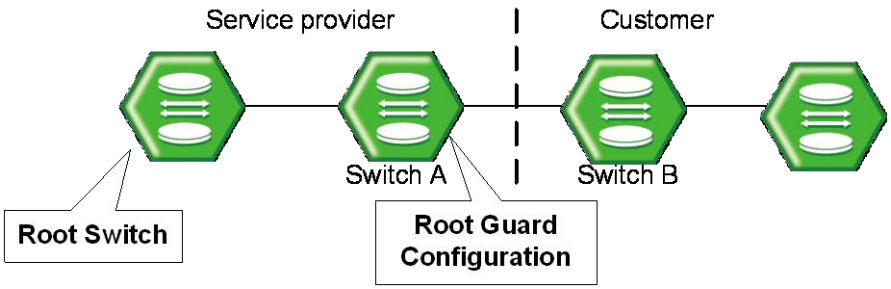


Fig. 8.26 Root Guard

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
stp pvst root-guard *VLAN-RANGE PORTS*	Bridge	Configures Root Guard on PVST network.
stp mst root-guard *MSTID-RANGE PORTS*		Configures Root Guard on MST network.
no stp pvst root-guard *VLAN-RANGE PORTS*		Disables Root Guard.
no stp mst root-guard *MSTID-RANGE PORTS*		
show stp		Shows STP configuration.

8.3.8 Restarting Protocol Migration

There are two switches which configured as STP and RSTP. Usually, in this case, STP protocol is used between two switches. But if someone configures the STP switch to RSTP mode, what happens? Because the RSTP switch already received STP protocol packet, the two switches still can work with STP mode even though RSTP is enabled at both.

To prevent this, the V5812G provides the **stp clear-detected-protocol** command. If you use this command, the switch checks STP protocol packet once again.

To clear configured Restarting Protocol Migration, use the following command.

Command	Mode	Description
stp clear-detected-protocol *PORTS*	Bridge	Configures restarting protocol migration function.

8.3.9 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.



The configuration for BPDU is applied as selected in force-version. The same commands are used for STP, RSTP, MSTP, PVSTP and PVRSTP.

8.3.9.1 Hello Time

Hello time decides an interval time when a switch transmits BPDU. To configure hello time, use the following command.

Command	Mode	Description
stp mst hello-time <1-10>	Bridge	Configures hello time to transmit the message in STP, RSTP and MSTP. 1-10: set the hello time. (default: 2)
stp pvst hello-time *VLAN-RANGE* <1-10>		Configures hello time to transmit the message in PVSTP and PVRSTP. 1-10: set the hello time. (default: 2)

To clear configured hello-time, use the following command.

Command	Mode	Description
no stp mst hello-time	Bridge	Returns to the default hello time value of STP, RSTP and MSTP.
no stp pvst hello-time *VLAN-RANGE*		Returns to the default hello time value of PVSTP and PVRSTP.

8.3.9.2 Forward Delay

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
stp mst forward-delay <4-30>	Bridge	Modifies forward-delay in STP, RSTP or MSTP, enter a delay time value. (default: 15)
stp pvst forward-delay *VLAN-RANGE* <4-30>		Modifies forward-delay in PVSTP and PVRSTP, enter a delay time value of VLAN. (default: 15)

To delete a configured forward delay, use the following command.

Command	Mode	Description
no stp mst forward-delay	Bridge	Returns to the default value of STP, RSTP and MSTP.
no stp pvst forward-delay *VLAN-RANGE*		Returns to the default value of PVSTP and PVRSTP per VLAN.

8.3.9.3 Max Age

Max age shows how long path message is valid. To configure max age to delete useless messages, use the following command.

Command	Mode	Description
stp mst max-age <6-40>	Bridge	Configures max age of route message of STP, RSTP or MSTP, enter a max age time value. (default: 20)
stp pvst max-age *VLANS* <6-40>		Configures max age of route message of PVSTP, PVRSTP, enter a max age time value of VLAN. (default: 20)

i It is recommended that max age is configured less than twice of forward delay and more than twice of hello time.

To delete a configured max age, use the following command.

Command	Mode	Description
no stp mst max-age	Bridge	Returns to the default max-age value of STP, RSTP and MSTP.
no stp pvst max-age *VLAN-RANGE*		Returns to the default max-age value of PVSTP and PVRSTP.

8.3.9.4 BPDU Hop

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
stp mst max-hops <1-40>	Bridge	Configures the number of hops for BPDU, set the number of possible hops in the region.
no stp mst max-hops		Deletes the number of hops for BPDU in MSTP.

8.3.9.5 BPDU Filter

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 set the BPDU filter on the port, use the following command.

Command	Mode	Description
stp bpdu-filter {**enable** | **disable**} *PORTS*	Bridge	Sets a BPDU filter state on the port.

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.

8.3.9.6 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
stp edge-port *PORTS*	Bridge	Configures the port as Edge port.

Step 2 Configure BPDU guard.

Command	Mode	Description
stp bpdu-guard	Bridge	Configures BPDU guard function on switch.
no stp bpdu-guard		Disables BPDU guard function.

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 V5812G provides BPDU guard auto-recovery function. When an edge port is down for BPDU packet, which came from other switch, the port is recovered automatically after configured time.

To enable BPDU guard auto recovery, use the following command.

Command	Mode	Description
stp bpdu-guard auto-recovery	Bridge	Enables BPDU guard auto recovery on the switch.
stp bpdu-guard auto-recovery-time <10-1000000>		Enables BPDU guard auto recovery time.

To disable BPDU guard auto recovery, use the following command.

Command	Mode	Description
no stp bpdu-guard auto-recovery	Bridge	Disables BPDU guard auto recovery.
no stp bpdu-guard auto-recovery-time		

To recover a blocked port by manually, use the following command.

Command	Mode	Description
stp bpdu-guard err-recovery *PORTS*	Bridge	Recovers a blocked port by manually.

To display the changed status of port by BPDU guard, use the following command.

Command	Mode	Description
show stp bpdu-guard detect	Bridge	Shows the status of port by BPDU guard.

8.3.9.7 Displaying BPDU Configuration

To display the configuration for BPDU, use the following command.

Command	Mode	Description
show stp	Enable Global Bridge	Shows a configuration for BPDU for STP, RSTP and MSTP.
show stp pvst *VLAN-RANGE* [**all** | *PORTS*] [**detail**]		Shows a configuration for BPDU for PVSTP and PVRSTP.

8.3.10 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.

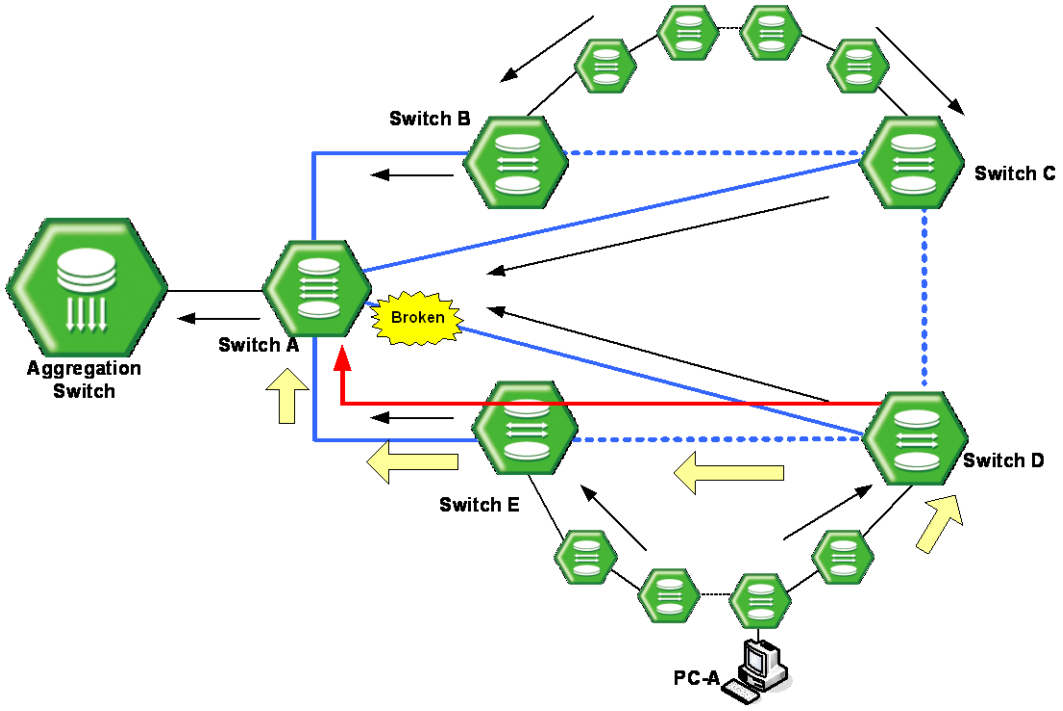


Fig. 8.27 Example of Layer 2 Network Design in RSTP Environment

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

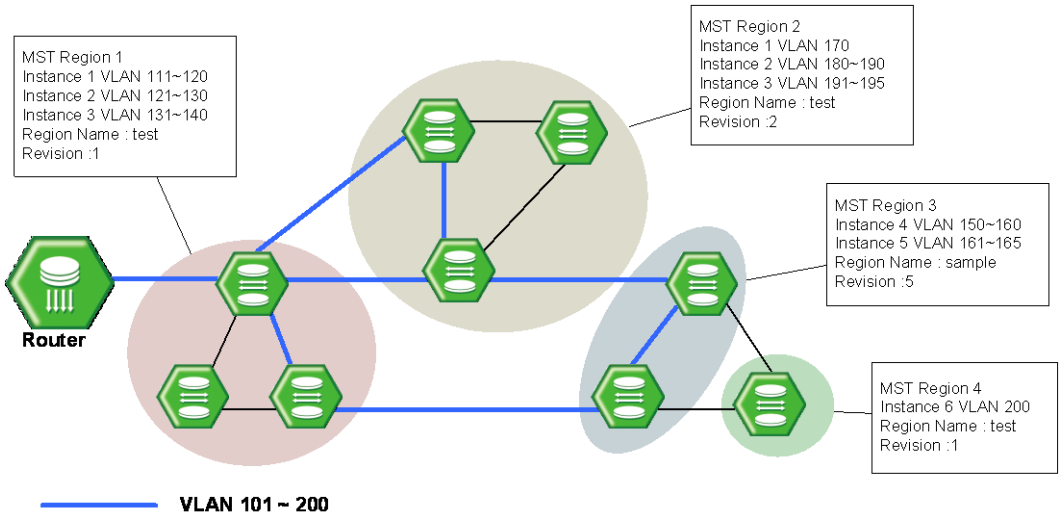


Fig. 8.28 Example of Layer 2 Network Design in MSTP Environment

The following is an example of configuring MSTP in the switch.

```
SWITCH(bridge)# stp force-version mstp
SWITCH(bridge)# stp mst enable
SWITCH(bridge)# stp mst config-id map 2 1-50
SWITCH(bridge)# stp mst config-id name 1
SWITCH(bridge)# stp mst config-id revision 1
SWITCH(bridge)# stp mst config-id commit
SWITCH(bridge)# show stp mst

Status              enabled
bridge id           8000.00d0cb000183
designated root     8000.00d0cb000183
root port           0                   path cost 0
max age             20.00               bridge max age          20.00
hello time          2.00                bridge hello time       2.00
forward delay       15.00               bridge forward delay    15.00
CIST regional root  8000.00d0cb000183   CIST path cost          0
max hops            20
name                TEST
revision            1
instance vlans
------------------------------------------------------------------------
CIST      51-4094
  2       1-50
------------------------------------------------------------------------
SWITCH(bridge)#
```

8.4 Ethernet Ring Protection (ERP)

The ERP is Dasan Networks protection protocol for Ethernet ring topology to prevent Loop from a link failure or recovery. It is designed to minimize the time for removing Loop within 50 milliseconds while there is an enormous amount of traffic flow in Metro Ethernet network.

It is a unique robustness functionality which runs on every network element involved in the ring configurations. It means that each system is active part of the ring protection mechanism. Therefore, it guarantees to switch over towards a new topology after link or system failure within 50 milliseconds.

8.4.1 ERP Mechanism

The purpose of Ethernet Ring Protection (ERP) is to prevent the Loop by performing the Redundancy Manager Node (RM Node) to detect a link failure and recover from it. An Ethernet ring consists of one or more ERP domains. ERP domain is an identifier of a single ring topology to be controlled by ERP mechanism. A node is one of the switches on the ERP ring. Each switch is configured as either RM node or normal node. RM node is responsible for keeping an open loop whenever all nodes and links are operating correctly. One ERP domain should have one RM node. Normal nodes are responsible to inform RM node of Link failures/recovery.

Both RM node and normal node have a primary and secondary port. You need to specify primary and secondary port which is directly connected to the node within an Ethernet ring. A secondary port of RM node is blocked as unused link for traffic while it runs without the link failure detection.

ERP Operation

If a link failure occurs, the normal nodes adjacent to the failure block their ports that detecting the link failure and send Link Down message to RM node. After RM node receives Link Down messages from the normal nodes, it unblocks its secondary port for traffic transmission. RM node responds to those messages using RM Link Down message which informs the other nodes that its secondary port has been unblocked.

If the link failure is recovered, the normal nodes send Link Up message to RM node. And they keep the blocking status of those failed ports. If the blocked ports of the normal nodes start to forward right after a Link Failure is recovered, a temporary loop can occur.

If RM node receives Link Up message, it blocks its own secondary port and sends RM Link UP message which informs the nodes of the secondary port’s blocking status. If the nodes receive RM Link Up message, they unblocks the ports which are detected a Link Failure recovery. The Ethernet ring is back to normal state.

ERP Messages

There are five types of ERP messages of concern to the RM node-Normal node interaction in ERP ring as shown below:

- **Normal Node messages**
  The following messages are sent by the normal nodes to inform RM node of their link changes.
  – **Link Down**: A normal node sends Link Down messages detecting its link failure.
  – **Link Up**: A normal node sends Link Up messages detecting its link recovery.
- **RM Node messages**
  A RM node is in charge of protecting the Ethernet ring. It sends periodic Test Packet messages to normal nodes and receives Link Down/Up message from those nodes to detect the link failure or recovery.
  – **Test Packet (TP)**: This is used to determine if any loops occur in the Ethernet ring.
  – **RM Link Down**: This is used to inform the normal nodes of unblocking status of its secondary port caused by link failure.
  – **RM Link Up**: This is used to inform the normal nodes of re-blocking status of its secondary port caused by link recovery.

ERP implementation of the V5812G has the following restrictions, so you should keep in mind those before configuring ERP.



- ERP can not be configured with STP. If ERP is enabled in the system, STP is automatically disabled.
- A primary and secondary port number should not be same.
- ERP mechanism should be used for Ethernet Ring topology only.

If the link failure occurs, the nodes adjacent (Node A & B) to the failure detect their state and send Link Down message to RM node. If an intermediate node (Node C) between RM node and a node adjacent to link failure receives Link Down message, it starts to perform Forwarding Database (FDB) Flushing. FDB Flushing consists in erasing in the forwarding database of the switch all MAC entries of the protected VLANs that are forwarded to the ring ports. The Flushing of FDB is always followed by a period with learning disabled. To prevent wrong MAC learning due to the remaining packets in the buffer, a node does not learn MAC addresses during a configured learning disable time.

Fig. 8.29 shows an example of ERP operation when a link failure occurs.

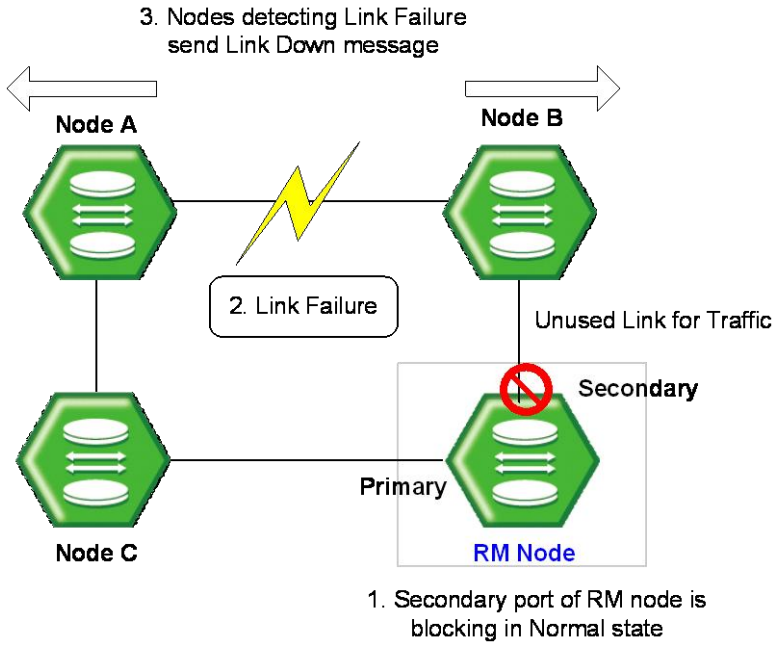


Fig. 8.29 ERP Operation in case of Link Failure

After RM node receives Link Down messages from other nodes, it unblocks its secondary port for traffic transmission with Node B directly connected to the secondary port. RM node sends RM Link Down messages and informs the other nodes that its secondary port begins forwarding the traffic.

Fig. 8.30 shows an example of a ring protection after a link failure.

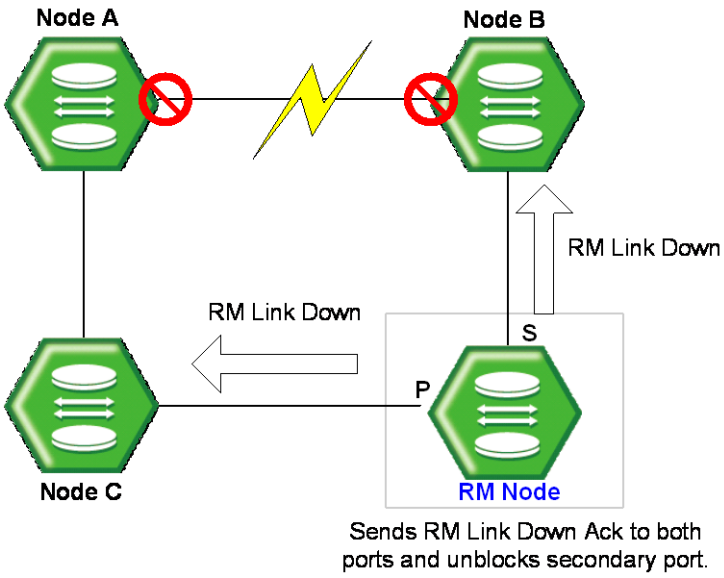


Fig. 8.30 Ring Protection

If Node A and Node B detect the link failure being recovered, they send Link Up message to RM node. But these nodes keep the blocking status of the link recovered ports.

Fig. 8.31 shows an example of a Link Failure Recovery operation.

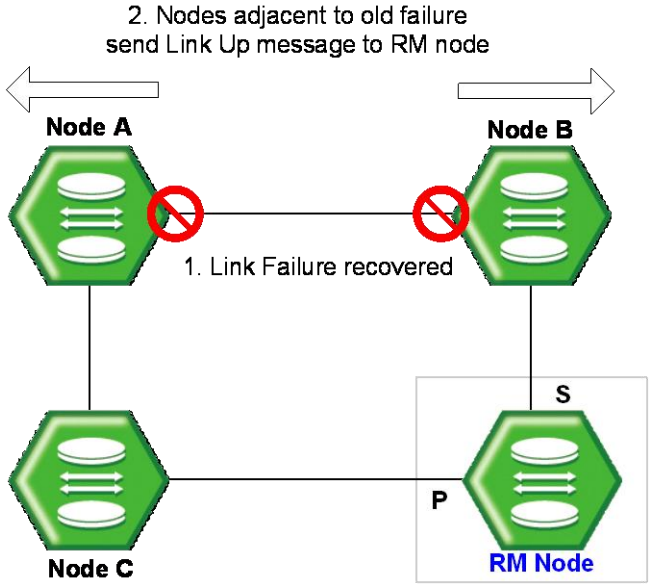


Fig. 8.31 Link Failure Recovery

After RM node receives Link Up message, it blocks its own secondary port. RM node sends RM Link UP message that informs other nodes the blocking status of secondary port. If the nodes receives RM Link Up message, they unblocks the ports which are detected a Link Failure recovery. The Ethernet ring is back to normal state.

Fig. 8.32 shows an example of a Ring Recovery operation.

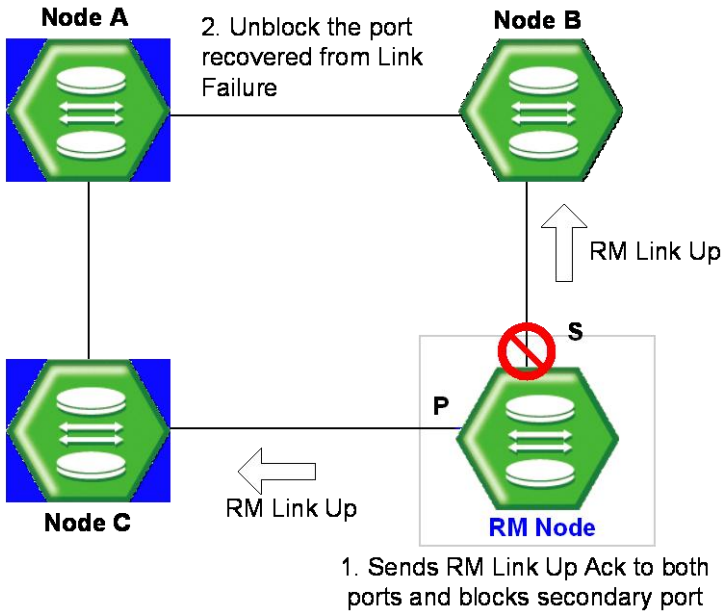


Fig. 8.32 Ring Recovery

8.4.2 Loss of Test Packet (LOTP)

ERP recognizes the Link Failure using Loss of Test Packet (LOTP) mechanism. RM Node periodically sends periodic “RM Test Packet” message. The state of LOTP means that “RM Test Packet” message does not return three consecutive times to RM node through Ethernet Ring. If RM node receives its “RM Test Packet” message through Ethernet Ring, it continues to block its secondary port.

You can configure the interval for sending “RM Test Packet” message.

8.4.3 ERP Shared Link

Sharing a link between two ERP rings allows the two nodes adjacent to the link to be common to the two rings. Sharing one link between two rings would create a “super loop” if that link failed. To prevent the super loop, two ERP domains should have different priorities. This concept is called “ERP ring priority”. When a link is shared by two or more rings, one RM node with the highest priority is responsible to protect failures of the shared link. Two normal nodes of a shared link belong to both ERP domains. The control packets (TPs) can be transmitted from the lower priority domain to higher priority domain only.

Fig. 8.33 shows the example of ring interconnection using one shared link.

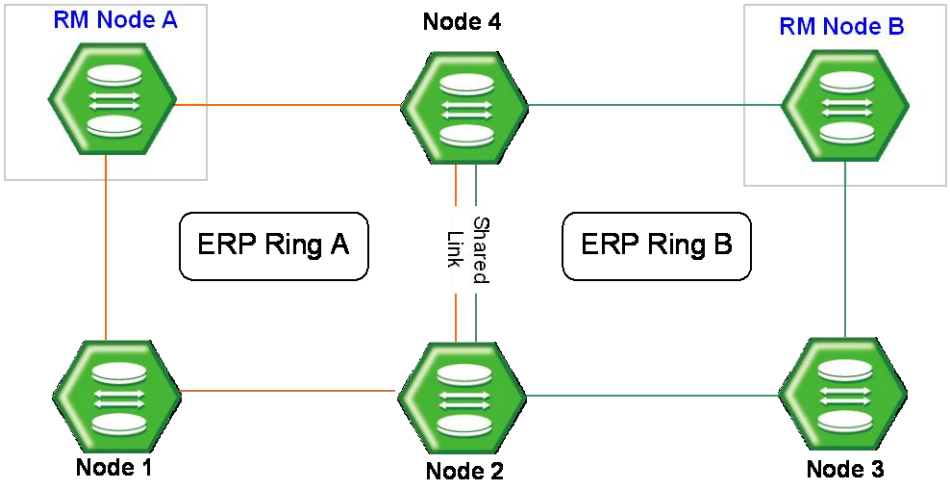


Fig. 8.33 Shared Link

ERP shared link environment has the following requirements, so you should keep in mind them before configuring ERP ring topology with a shared link.

- A port adjacent to the shared link should not be blocked. It means that a shared link that is used as the one of the secondary ports of a RM node.
- If there are two ERP domains with a single shared link, you should specify different priority of ERP domains.
- The higher priority domain should include all protected and control VLANs of the lower priority domain to protect and manage the lower priority ring more effectively.

8.4.4 Configuring ERP Domian

8.4.4.1 ERP Domain

To configure the switch with ERP, you should create ERP domain first. To create an ERP domain, use the following command.

Command	Mode	Description
erp domain <1-4094>	Bridge	Creates ERP domain. 1-4094: domain ID and control VLAN ID
no erp domain { **all** | <1-4094>}		Deletes the configured ERP domain.

8.4.4.2 ERP Domain Description

To specify a description for configured domain, use the following command.

Command	Mode	Description
erp description <1-4094> *DESCRIPTION*	Bridge	Specifies a description of domain.

8.4.4.3 Node Mode

To configure ERP domain as RM node or normal node, use the following command.

Command	Mode	Description
erp rmnode <1-4094>	Bridge	Configures ERP domain as RM node (Redundancy manager node)
no erp rmnode <1-4094>		Configures ERP domain as normal node. (default)

8.4.4.4 Primary and Secondary Port

To configure Primary Port and Secondary port of a specific domain ID, use the following command.

Command	Mode	Description
erp port <1-4094> **primary** *PPORT* **secondary** *SPORT*	Bridge	Configures primary port and secondary port of an ERP domain PPORT: primary port number SPORT: secondary port number

i Primary port and secondary port should be different.

8.4.5 Protected Activation

When you finish configuring specific ERP domain with Domain ID, primary port and secondary port, you should activate the ERP domain to apply to the system. To activate an ERP domain, use the following command.

Command	Mode	Description
erp activation <1-4094>	Bridge	Configures ERP Protected Activation.

To deactivate an ERP domain, use the following command.

Command	Mode	Description
no erp activation <1-4094>	Bridge	Deactivates an ERP domain. (default)

8.4.6 Primary/Secondary Port State

A secondary port is supposed to be blocked as unused link for traffic while ERP runs without any link failure. While a primary port forwards the traffic to other nodes. But you can configure a primary port to be blocked as a secondary port role. A secondary port is automatically changed to forward the traffic. To manually configure a primary or secondary port as an unused link that should be blocked for traffic in normal condition of Ethernet ring, use the following command.

Command	Mode	Description
erp ms-s <1-4094>	Bridge	Unblocks a primary port and blocks a secondary port of ERP domain as RM node (default)

To delete the configured state of primary/secondary port, use the following command.

Command	Mode	Description
no erp ms-s <1-4094>	Bridge	Unblocks a secondary port and blocks a primary port of ERP domain as RM node

8.4.7 Learning Disable Time

To prevent wrong MAC learning due to the remaining packets of buffer, a node does not learn MAC addresses during the learning disable time. This parameter holds the time, in milliseconds, during which learning is disabled after FDB flushing and can be configured by the operator. The learning is only disabled for the protected VLAN of the domain on the ERP ports.

To configure a Learning Disable Time, use the following command.

Command	Mode	Description
erp learn-dis-time <1-4094> <0-500>	Bridge	Configures ERP learning disable time 1-4094: domain ID and control VLAN ID 0-500: learning disabling time (unit: millisecond, default: 0ms)

To delete the configured a Learning Disable Time, use the following command.

Command	Mode	Description
no erp learn-dis-time <1-4094>	Bridge	Configures ERP learning disable time as default value

8.4.8 Wait-to-Restore Time

If a port's link failure is recovered on the normal node, the blocked port should be changed to the forwarding status. However, the loop may occur when this port start to forward the traffic before a secondary port of RM node is blocked. To prevent the loop, the normal node waits for the time until it receives RM Link Up message. Even if it does not receive RM Link Up message, the port starts to forward the traffic.

i The normal node waits for real waiting timeout to forward the traffic again. The formula is simply shown as below:

Real Waiting timeout = Wait-to-Restore Time + 3Test Packet Interval
e.g. 1.3 seconds = 1 second + (10 milliseconds x 3)

To specify a wait-to-restore time, use the following command.

Command	Mode	Description
erp wait-to-restore <1-4094> <1-720>	Bridge	Configures wait-to-restore time. 1-720: Wait to restore time in second (default: 1s)

To delete the configured wait-to-restore time, use the following command.

Command	Mode	Description
no erp wait-to-restore <1-4094>	Bridge	Deletes the configured wait-to-restore time.

8.4.9 Test Packet Interval

RM Node periodically sends "RM Test Packet" message to detect the loop. To configure an interval to send Test Packet message of RM node, use the following command.

Command	Mode	Description
erp test-packet-interval <1-4094> <10-500>	Bridge	Specifies an interval of test packet message. 1-4094: domain ID and control VLAN ID 10-500: test packet interval (default:10ms, unit: millisecond)

To delete a specified interval of Test Packet, use the following command.

Command	Mode	Description
no erp test-packet-interval <1-4094>	Bridge	Deletes the configured interval of test packet message.

8.4.10 ERP Ring Priority

The Super Loop occurs because of a shared link's failure between two ERP rings. A domain with higher priority (one of the RM nodes) is the only responsible for monitoring the ports of a shared link. The control packets of a domain with lower ring priority can be transmitted to another domain with higher priority to prevent the super loop.

It means that the higher ring priority domain guarantees the detour path against a shared link of lower ring priority domain.

To specify ERP ring priority, use the following command.

Command	Mode	Description
erp ring-priority <1-4094> <1-255>	Bridge	Specifies ERP ring priority 1-4094: domain ID and control VLAN ID 1-255: ERP ring priority value (default: 0)

To return ERP ring priority as default, use the following command.

Command	Mode	Description
no erp ring-priority <1-4094>	Bridge	Configures ERP ring priority as default value

8.4.11 LOTP Hold Off Time

It is necessary to prevent lower priority rings to trigger protection because of loss of test packets before the protection of the higher priority ring and transmission of test packets over this ring.

LOTP hold-off time determines the hold-off time for ERP switching in case of detection of LOTP. This parameter provides independence between ERP rings. Hold-off time for LOTP triggered ERP delays ERP switching if a ring protection of this domain is also provided by other higher priority rings. LOTP Hold-Off Time value depends on the ring priority of ERP rings.

To specify LOTP hold-off time, use the following command.

Command	Mode	Description
erp hold-off-time <1-4094> <1-20000>	Bridge	Configures LOTP hold-off time 1-20000: ERP hold-off time (default: 0 ms, unit: millisecond)

To configure LOTP hold-off time as default, use the following command.

Command	Mode	Description
no erp hold-off-time <1-4094>	Bridge	Configures LOTP hold-off time as default value

8.4.12 ERP Trap

To enable the system to generate ERP trap message, use the following command.

Command	Mode	Description
erp trap <1-4094> {**lotp** | **ulotp** | **multiple-rm** | **rmnode-reachability**}	Bridge	Enables the system to send ERP Trap message in case of the event.

To disable the system to generate ERP trap message, use the following command.

Command	Mode	Description
no erp trap <1-4094> {**lotp** | **ulotp** | **multiple-rm** | **rmnode-reachability**}	Bridge	Disables the system to generate ERP trap

The following options hold the configuration of the ability to transmit LOTP, ULOTP, Multiple RM or RMNode reachability Traps.

– **lotp**: Enables/disables an RM node to transmit the LOTP traps.
– **ulotp**: Enables/disables an RM node to transmit the ULOTP (Undirectional Loss Of Test Packets) traps.
– **multiple-rm**: Enables/disables an RM node to transmit the trap in case of Multiple RM nodes.
– **rmnode-reachability**: Enables/disables a normal node to transmit RMnode Reachablility traps.

8.4.13 Registering ERP MAC

To register MAC address of a port for ERP implementation, use the following command.

Command	Mode	Description
erp register-mac *VLAN PORTS*	Bridge	Sets a register ERP MAC address.

To delete the registered MAC address of a port, use the following command.

Command	Mode	Description
no erp register-mac *VLAN* [*PORTS*]	Bridge	Deletes the registered MAC address.

8.4.14 Private VLAN with ERP

A protected port is for the function of port isolation in local switch. That is, it cannot work on between two different switches with protected ports. A protected port can not transmit any traffic to other protected ports.

Private VLAN provides L2 isolation within the same Broadcast Domain ports. That means another VLAN is created within a VLAN. You can choose two types of port in ERP protected mode.

- **Promiscuous**: A promiscuous port can communicate with all interfaces, including the

promiscuous and protected ports within a PVLAN.

- **Protected**: An protected port has complete Layer 2 separation from the other ports within the same PVLAN, but it floods the traffic to the promiscuous ports. PVLANs block all traffic to protected ports except traffic from promiscuous ports. Traffic from protected port is forwarded only promiscuous ports.

To configure all ports as the protected ports while ERP is enabled in the system, use the following command.

Command	Mode	Description
port protected erp	Bridge	Specifies all ports as protected ports while ERP is running in the system
no port protected erp		Deletes all protected ports in ERP protected mode

To specify promiscuous ports, use the following command.

Command	Mode	Description
port protected erp promiscuous *PORTS*	Bridge	Specifies the promiscuous port while ERP is running in the system
no port protected erp promiscuous *PORTS*		Deletes the configured promiscuous port.



If a port is already configured by Port Isolation, this port should be disabled by **no port proteced** command to be set ERP promiscuous port.



Except for the specified promiscuous ports, the rest of ports are automatically set as the protected ports.

To display the information of port protected mode, use the following command.

Command	Mode	Description
show port protected	Enable Global Bridge	Shows the status of port protected mode.

8.4.15 Displaying ERP Configuration

To display a configuration of ERP, use the following command.

Command	Mode	Description
show erp [**all** | <1-4094>]	Enable Global Bridge	Shows the information of ERP 1-4094: domain ID and control VLAN ID

8.5 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 V5812G 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 00:d0:cb:00:00:01, the source MAC address will be changed to 02:d0:cb: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.

8.6 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.

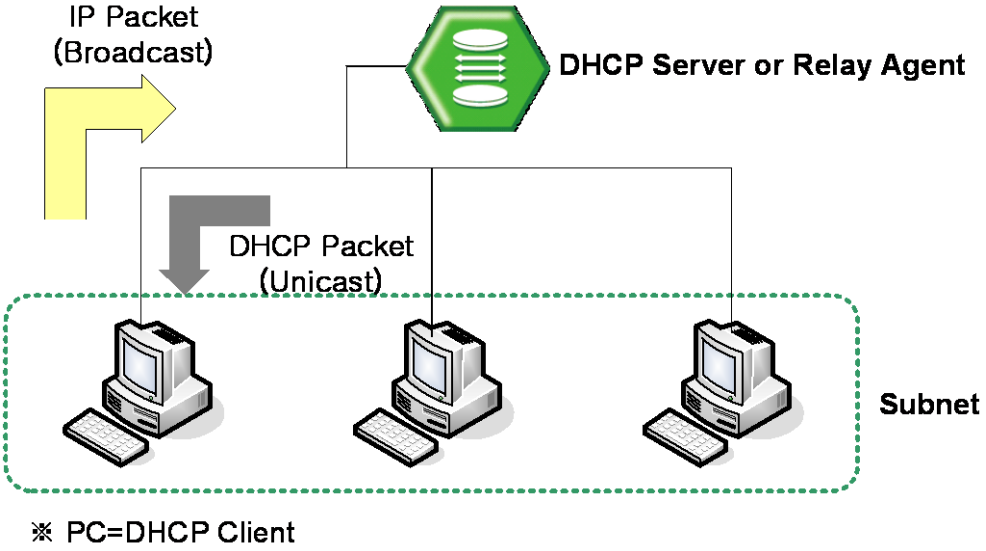


Fig. 8.34 DHCP Service Structure

The V5812G 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

8.6.1 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.

Before configuring DHCP server or relay, you need to use the **service dhcp** command first to activate the DHCP function in the system.

8.6.1.1 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])#
```

8.6.1.2 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])#
```



You can also specify several subnets in a single DHCP pool.

8.6.1.3 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])#
```



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.

8.6.1.4 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])#
```

8.6.1.5 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])#
```

8.6.1.6 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])#
```



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.

8.6.1.7 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.

8.6.1.8 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.

8.6.1.9 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 8.6.5 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>		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.

8.6.1.10 Static Mapping

The V5812G 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.

For more information of the file naming of a DHCP lease database, see Section 8.6.3.1.

8.6.1.11 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

8.6.1.12 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)

8.6.1.13 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.

8.6.1.14 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 V5812G 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.

8.6.1.15 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.

8.6.1.16 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)#
```

8.6.1.17 Setting DHCP Pool Size

To limit a size of DHCP pool, use the following command.

Command	Mode	Description
ip dhcp max-pool-size <1-8>	Global	Configures a maximum size of DHCP pool.

8.6.1.18 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)#
```

8.6.2 DHCP Address Allocation with Option 82

The DHCP server provided by the V5812G 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.

8.6.2.1 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.

8.6.2.2 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.

8.6.2.3 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.

8.6.2.4 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.

8.6.2.5 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.

8.6.3 DHCP Lease Database

8.6.3.1 DHCP Database Agent

The V5812G 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.

8.6.3.2 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*]		

8.6.3.3 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.

8.6.4 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.

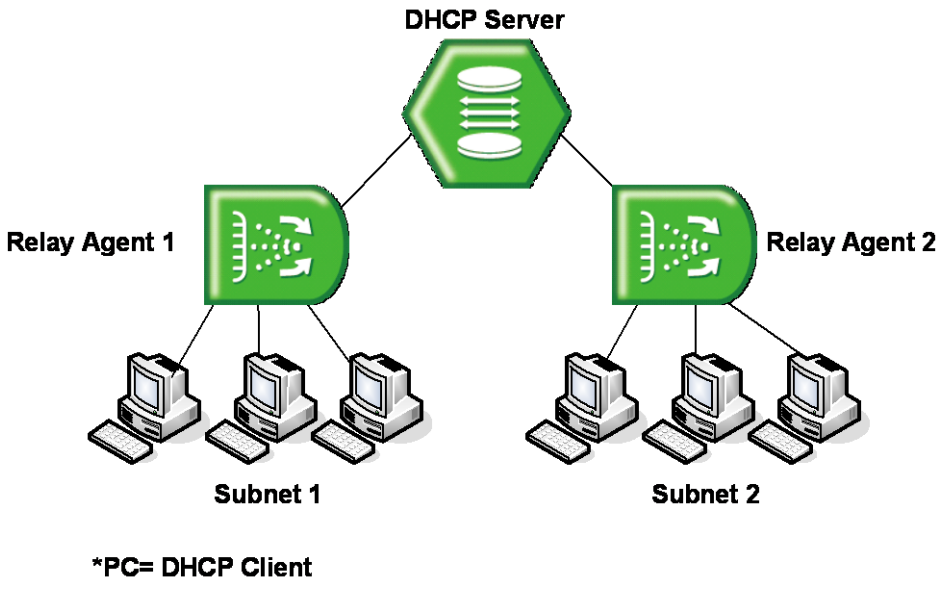


Fig. 8.35 Example of DHCP Relay Agent

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.

Before configuring DHCP server or relay, you need to use the **service dhcp** command first to activate the DHCP function in the system.

8.6.4.1 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.

If a DHCP helper address is specified on an interface, the V5812G 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.

8.6.4.2 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.

8.6.4.3 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.

8.6.4.4 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.

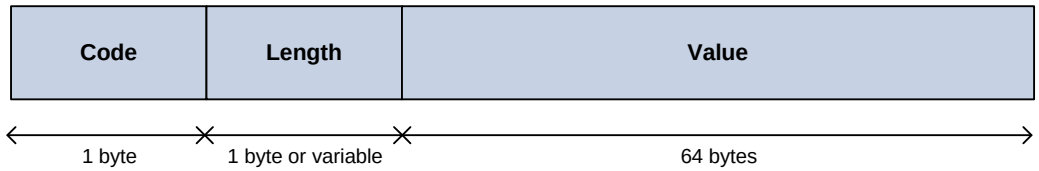
To delete collected DHCP relay statistics, use the following command.

Command	Mode	Description
clear ip dhcp relay statistics	Enable Global Bridge	Deletes collected DHCP relay statistics.

8.6.5 DHCP Option

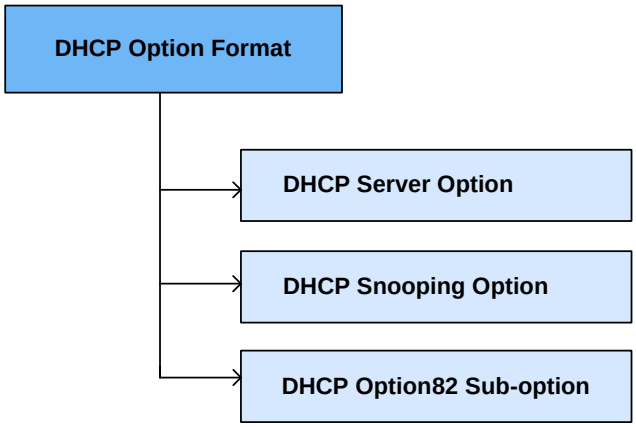
This function enables administrators to define DHCP options that are carried in the DHCP communication between DHCP server and client or relay agent. The following indicates the format of the DHCP options field.

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.



8.6.5.1 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

8.6.5.2 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	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. 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.

- The value should be within 64 bytes.
- A hidden-length variable should be set once in a single attribute.
- The total length of an option format cannot exceed 254 bytes.

8.6.5.3 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.

8.6.5.4 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.

8.6.6 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. 8.36 shows how the DHCP relay agent with the DHCP option 82 operates.

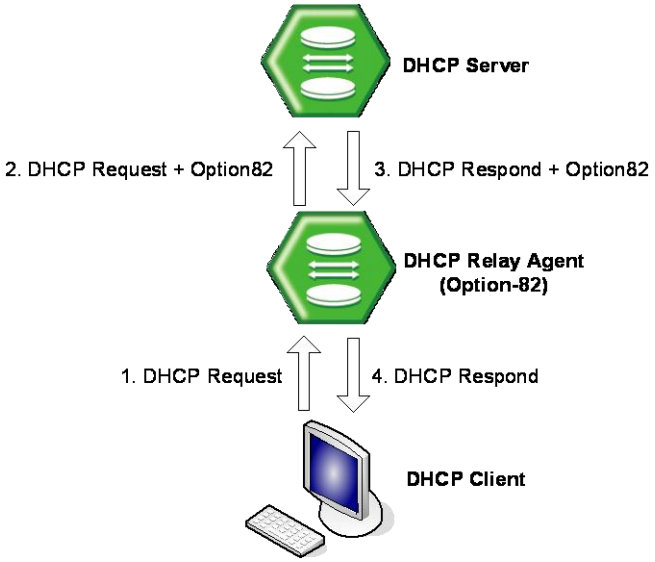


Fig. 8.36 DHCP Option 82 Operation

8.6.6.1 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.

8.6.6.2 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*		

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		

8.6.6.3 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).
policy drop {**normal** | **option82** | **none**}		normal: DHCP packet option82: DHCP option 82 packet none: no DHCP packet (default)

8.6.6.4 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.

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.

8.6.7 DHCP Snooping

For enhanced security, the V5812G 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.

The DHCP snooping only filters the DHCP server message such as a DHCP_OFFER or DHCP_ACK, which is received from untrusted interfaces.

8.6.7.1 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.

8.6.7.2 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)

8.6.7.3 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.

8.6.7.4 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

8.6.7.5 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.

8.6.7.6 Source MAC Address Verification

The V5812G 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.

8.6.7.7 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

8.6.7.8 DHCP Snooping Database Agent

When 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.

To maintain the binding when reload the system, you must use DHCP snooping database agent. If the agent is not used, the DHCP snooping binding will be lost when the switch is rebooted. The mechanism for the database agent saves the binding in a file at a remote location. Upon reloading, the switch reads the file to build the database for the binding. The system keeps the current file by writing to the file as the database changes.

To specify a DHCP database agent and enable an automatic DHCP snooping database back-up, use the following command.

Command	Mode	Description
ip dhcp snooping database *A.B.C.D INTERVAL*	Global	Specifies a DHCP snooping database agent and back-up interval. A.B.C.D: DHCP snooping database agent address INTERVAL: 120-2147483637 (unit: second)
no ip dhcp snooping database		Deletes a specified DHCP snooping database agent.

To request snooping binding entries from a DHCP snooping database agent, use the following command.

Command	Mode	Description
ip dhcp snooping database renew *A.B.C.D*	Global	Requests snooping binding entries from a DHCP snooping database agent. A.B.C.D: DHCP snooping database agent address

i The DHCP snooping database agent should be TFTP server.

8.6.7.9 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 V5812G may be rebooted with any reason, then DHCP snooping binding table entries, which are dynamically learned from DHCP packets back and forth the V5812G, 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.

8.6.7.10 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 V5812G, 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

8.6.7.11 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 8.6.5 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.

8.6.7.12 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		Shows DHCP snooping binding entries.

8.6.8 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.

8.6.8.1 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.

8.6.8.2 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.

8.6.8.3 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.

8.6.9 DHCP Client

An interface of the V5812G 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 V5812G cannot be configured as a DHCP server or relay agent.

8.6.9.1 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.

8.6.9.2 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.

8.6.9.3 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.

8.6.9.4 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.

8.6.9.5 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.

8.6.9.6 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.

8.6.9.7 Forcing Release or Renewal of DHCP Lease

The V5812G 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.

8.6.9.8 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.

8.6.10 DHCP Filtering

8.6.10.1 DHCP Packet Filtering

For the V5812G, 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
ip dhcp filter-address *MAC-ADDR* **type** {**ack** | **decline** | **discover** | **inform** | **nak** | **offer** | **release** | **request** }		Blocks a MAC address with DHCP message type options.
no ip dhcp filter-address *MAC-ADDR* [**type** {**ack** | **decline** | **discover** | **inform** | **nak** | **offer** | **release** | **request**}]		Disables DHCP MAC filtering.

8.6.10.2 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. 8.37, 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.

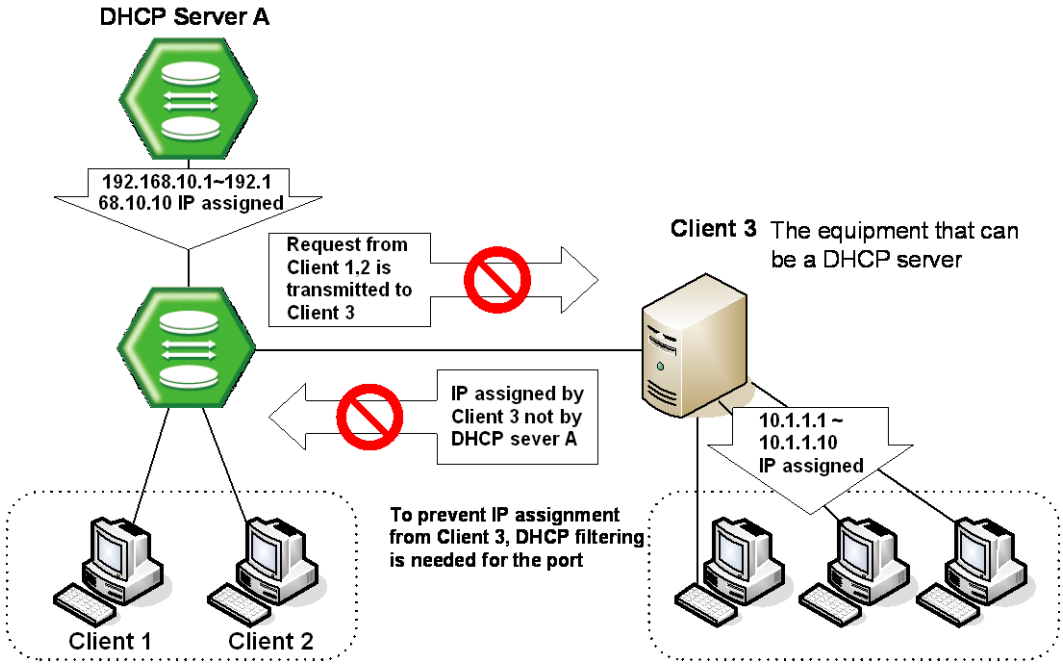


Fig. 8.37 DHCP Server Packet Filtering

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.

8.6.11 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.

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 V5812G. 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.

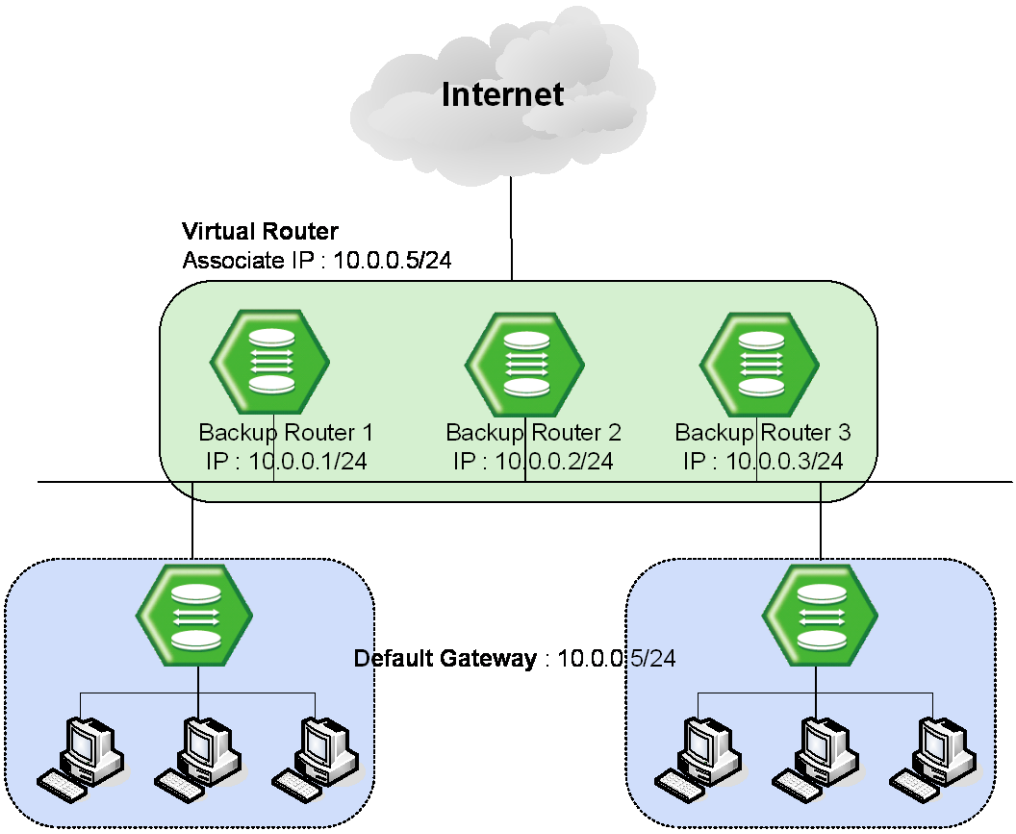


Fig. 8.38 VRRP Operation

In case routers have same priorities, then a router, which has higher IP address, gets the precedence. Fig. 8.38 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 V5812G 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 V5812G 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.

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 V5812G 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 lower IP address is configured as

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 V5812G, 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.

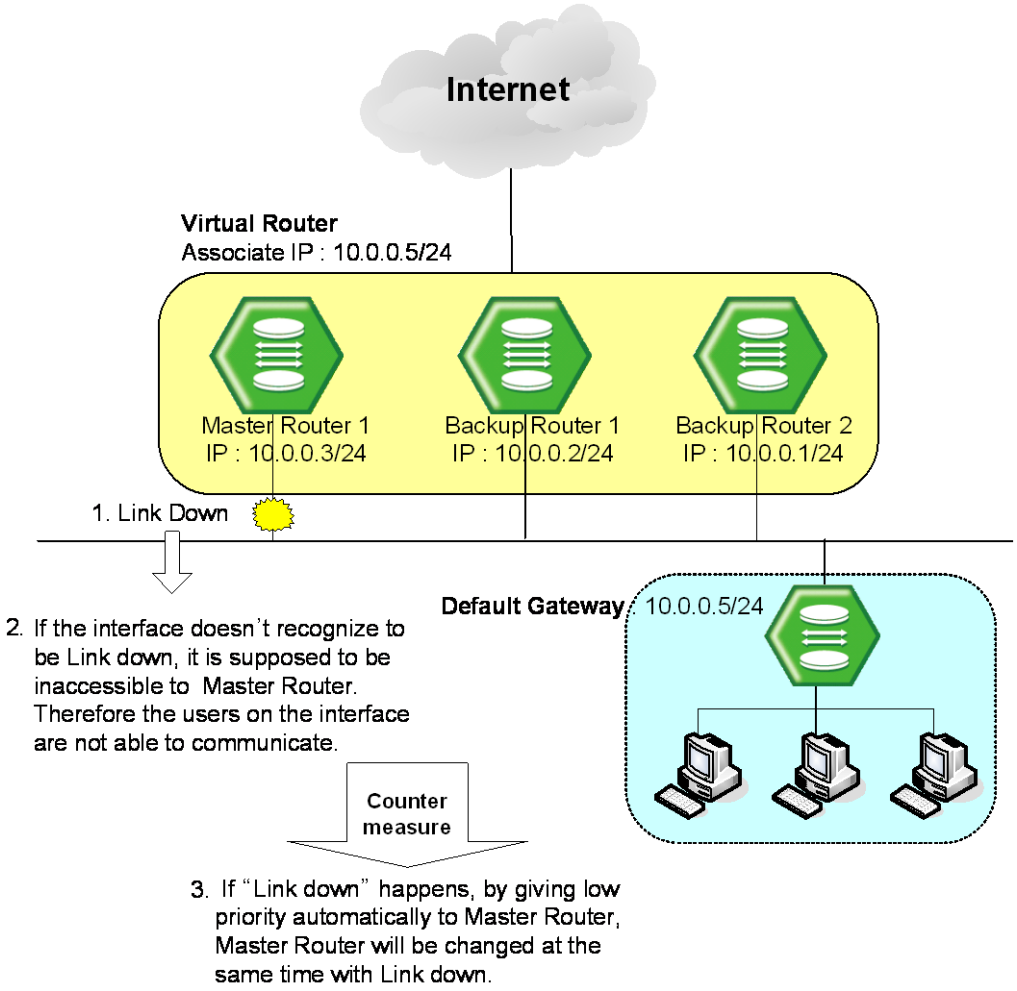


Fig. 8.39 VRRP Track

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.

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 Global	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 Global	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 Single IP Management

It is possible to manage several switches with a single IP address by using cascading. If there is a limitation for using IP addresses and there are too many switches, which you must manage, you can manage a number of switches with a single IP address using this cascading function.

It is named Single IP Management because you can easily manage various switches and subscribers connected to the switch with this cascading function. The V5812G provides the function.

The following is an example of the network where the cascading is configured.

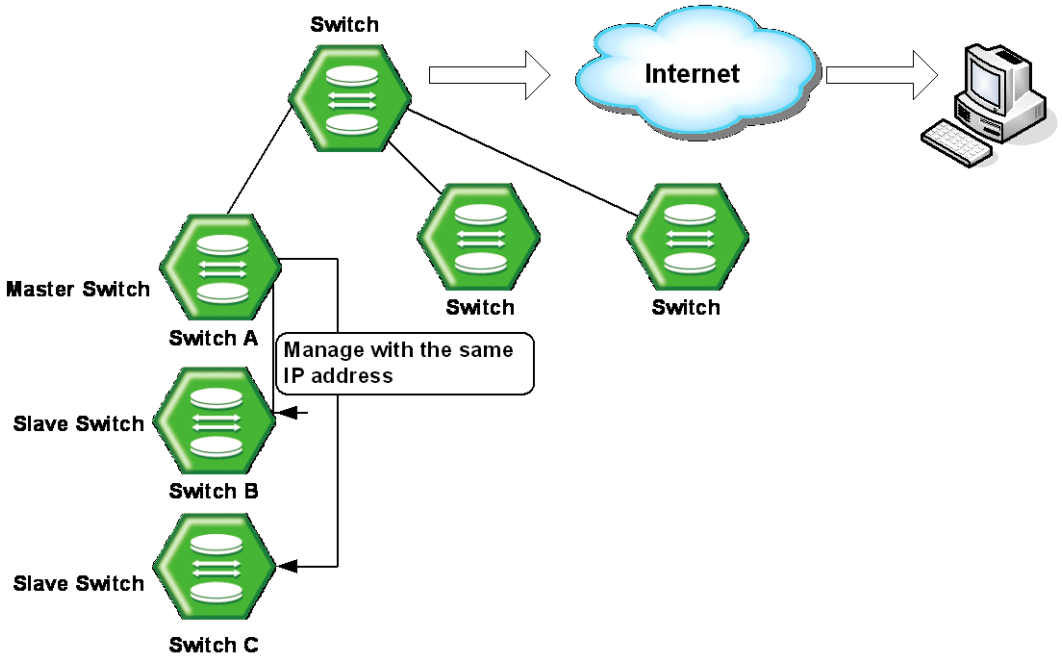


Fig. 8.40 Example of Cascading

A switch, which is supposed to manage the other cascaded switches is named as Master switch and the other switches managed by Master switch are named as Slave switch. Regardless of installed place or connection state, Master switch can check and manage all Slave switches.

i Up to 16 switches can be cascaded.

8.8.1 Switch Group

You should configure all the switches configured with stacking function to be in the same VLAN. To configure the switches as a switch group, which belongs to the same VLAN, use the following command.

Command	Mode	Description
stack device *NAME*	Global	Configures device name or VID.

i The port that connects Master and Slave switch must belong to the same VLAN.

8.8.2 Designating Master and Slave Switch

Designate Master switch using the following command.

Command	Mode	Description
stack master	Global	Sets the switch as a master switch.

After designating Master switch, register Slave switch for Master switch. To register Slave switch or delete the registered Slave switch, use the following command.

Command	Mode	Description
stack add *MAC-ADDR* [*DESCRIPTION*]	Global	Registers slave switch. MAC-ADDR: MAC address
stack del *MAC-ADDR*		Deletes slave switch.

i To make the cascading operate well, it is required to enable the interface of Slave switch. The switches in different VLANs cannot be added to the same switch group.

You should designate Slave switch registered in Master Switch as Slave Switch. To designate Slave switch, use the following command.

Command	Mode	Description
stack slave	Global	Sets the switch as a slave switch.

8.8.3 Disabling Cascading

To disable the cascading, use the following command.

Command	Mode	Description
no stack	Global	Disables the cascading.

8.8.4 Displaying Cascading Status

To display the cascading, use the following command.

Command	Mode	Description
show stack	Enable Global Bridge	Shows a configuration of the cascading.

8.8.5 Accessing to Slave Switch from Master Switch

After configuring all stacking configurations, it is possible to configure and mange by accessing to Slave switch from Master switch.

To access to Slave switch from Master switch, use the following command in *Bridge Configuration* mode.

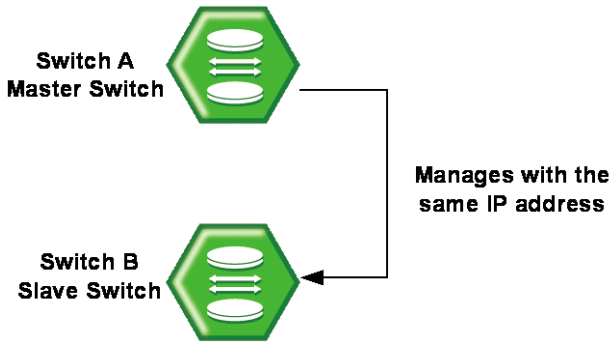
Command	Mode	Description
rcommand *NODE*	Enable	Accesses to a slave switch. NODE: node number

i NODE means node ID from configuring the cascading in Slave switch. If you enter the above command in Master switch, Telnet connected to Slave switch is displayed and it is possible to configure Slave switch using DSH command. If you use the exit command in Telnet, the connection to Slave switch is down.

8.8.6 Sample Configuration

Sample Configuration 1: Configuring the Cascading

The following is the cascading configuration by designating SWITCH A as a master and SWITCH B as a slave.



Step 1 Assign IP address in *Interface Configuration* mode of Switch and enable interface using the **no shutdown** command. To open *Interface Configuration* mode, you should open *Interface Configuration* mode of VLAN to register as a switch group for cascading.

The following is an example of configuring Interface of switch group as 1.

```
SWITCH_A# configure terminal
SWITCH_A(config)# interface 1
SWITCH_A(interface)# ip address 192.168.10.1/16
SWITCH_A(interface)# no shutdown
SWITCH_A(interface)#
```

i If there are several switches, rest of them are managed by IP address of Master switch. Therefore, you do not need to configure IP address in Slave switch.

Step 2 Configure Switch A as Master switch. Configure VLAN to belong to the same switch group and after registering Slave switch, configure it as a Master switch.

<Switch A – Master Switch>

```
SWITCH_A(config)# stack master
SWITCH_A(config)# stack device default
SWITCH_A(config)# stack add 00:d0:cb:22:00:11
```

Step 3 Configure VLAN in order to belong to the same switch group in Switch B registered in Master switch as Slave switch and configure as a Slave switch.

<Switch B – Slave Switch>

```
SWITCH_B(config)# stack slave
SWITCH_B(config)# stack device default
```

Step 4 Check the configuration. The information you can check in Master switch and Slave switch is different as below.

<Switch A – Master Switch>

```
SWITCH_A(config)# show stack
device  : default
node ID : 1
node   MAC address          status   type                name      port
   1   00:d0:cb:0a:00:aa    active   V5812G              SWITCH    26
   2   00:d0:cb:22:00:11    active   V5812G              SWITCH    26
SWITCH_A(config)#
```

<Switch B – Slave Switch>

```
SWITCH_B(config)# show stack
device  : default
node ID : 2
SWITCH_B(config)#
```

8.9 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 V5812G 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 5.2.5.

To display a configured rate limit, use the following command.

Command	Mode	Description
show rate-limit	Enable Global Bridge	Shows a configured rate limit.

8.10 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.

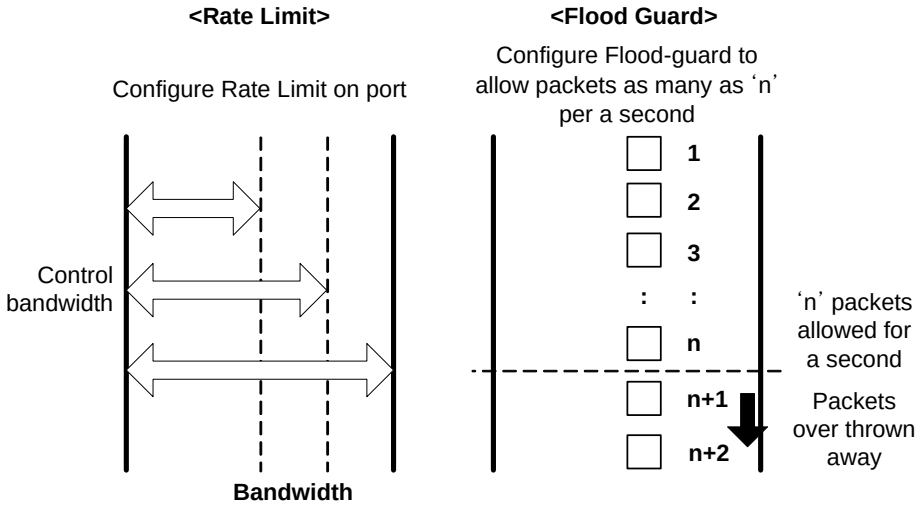


Fig. 8.41 Rate Limit and Flood Guard

8.10.1 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.

8.10.2 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.

8.10.3 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. V5812G 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.

8.11 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 V5812G 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.

8.12 Storm Control

The V5812G 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: 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.

8.13 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 V5812G 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* <1518-9216>	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.

8.14 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 <68-1500>	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, V5812G is supposed to block direct broadcast packet by default setting. However, you can enable or disable it in V5812G.

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.

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 V5812G 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 V5812G is configured only with IGMP snooping (L2 multicast forwarding feature) in the Layer 2 network.

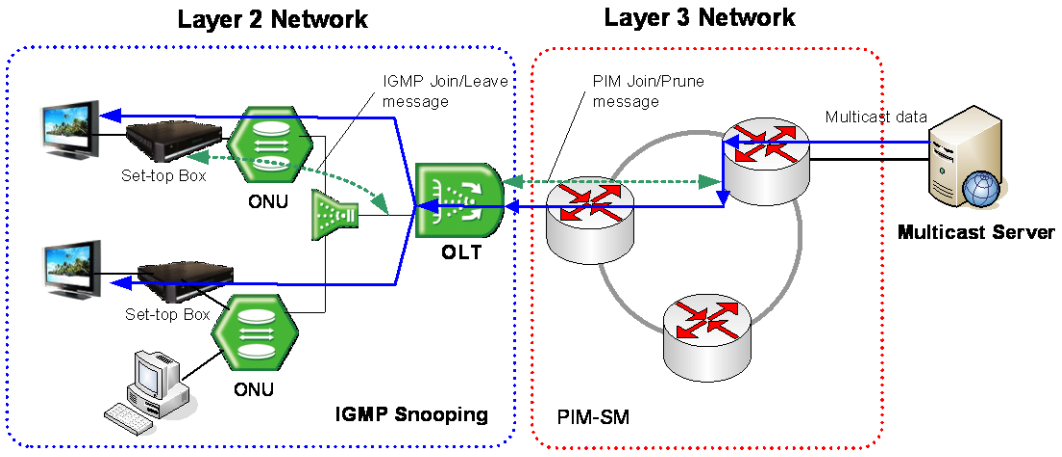


Fig. 9.1 The V5812G with IGMP Snooping

When installed within the Layer 3 network as a router, the V5812G should be configured with a multicast routing protocol. However, an additional switch performing IGMP snooping is needed for subscribers in the Layer 2 network. Fig. 9.2 shows an example of the V5812G with PIM-SM (L3 multicast routing protocol) in the Layer 3 network.

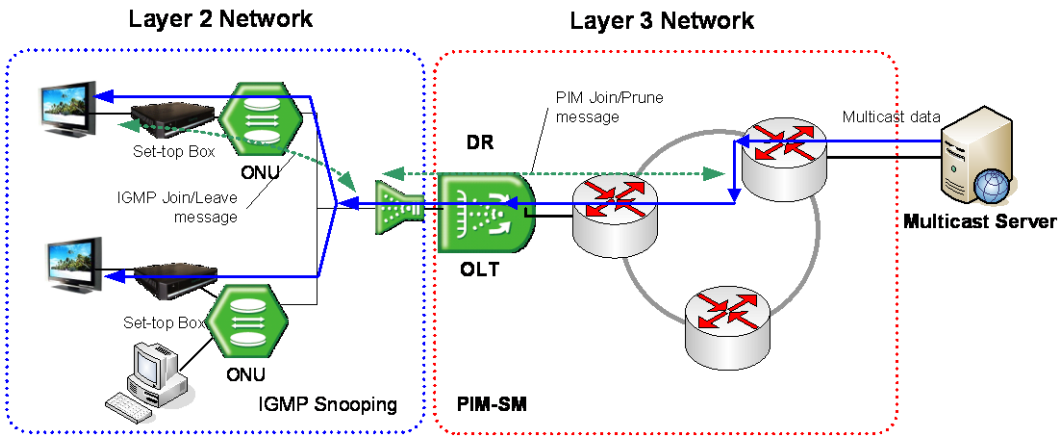


Fig. 9.2 The V5812G with PIM-SM

If more than one port are on the same Layer 2 interface and the V5812G is a border router of the Layer 3 network, you should configure the V5812G with both IGMP snooping and PIM-SM together.

Fig. 9.3 shows the example of the multicast network with the switch configured with both IGMP snooping and PIM-SM.

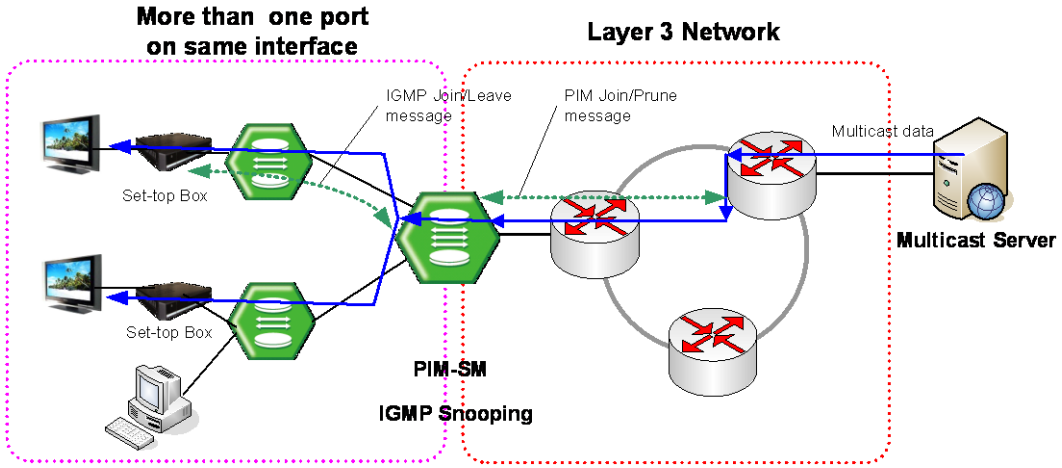


Fig. 9.3 The Switch with IGMP Snooping and PIM-SM

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 V5812G 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 V5812G 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: begin/end multicast group address

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*]		

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 V5812G 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, V5812G 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 <1-240>	Interface	Specifies a maximum query response time. 1-240: 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 V5812G 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 report may also contain multiple group records. Each group record has one of the fol-

lowing 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 V5812G provides various multicast functions including Layer 2 multicast forwarding, which allow you to achieve the fully effective and flexible multicast deployment.

This section describes the following features:

- Multicast Forwarding Database
- IGMP Snooping Basic
- IGMPv2 Snooping
- IGMPv3 Snooping
- Displaying IGMP Snooping Information
- Multicast VLAN Registration (MVR)
- IGMP Filtering and Throttling

9.2.1 Multicast Forwarding Database

Internally, the V5812G 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
no ip unknown-multicast [**port** *PORTS*] **block**		Configures the switch to flood unknown multicast traffic. (default)



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: 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: multicast group source: multicast source

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 V5812G dynamically forward multicast traffic only to those interfaces that want to receive it as nominal unicast forwarding does.

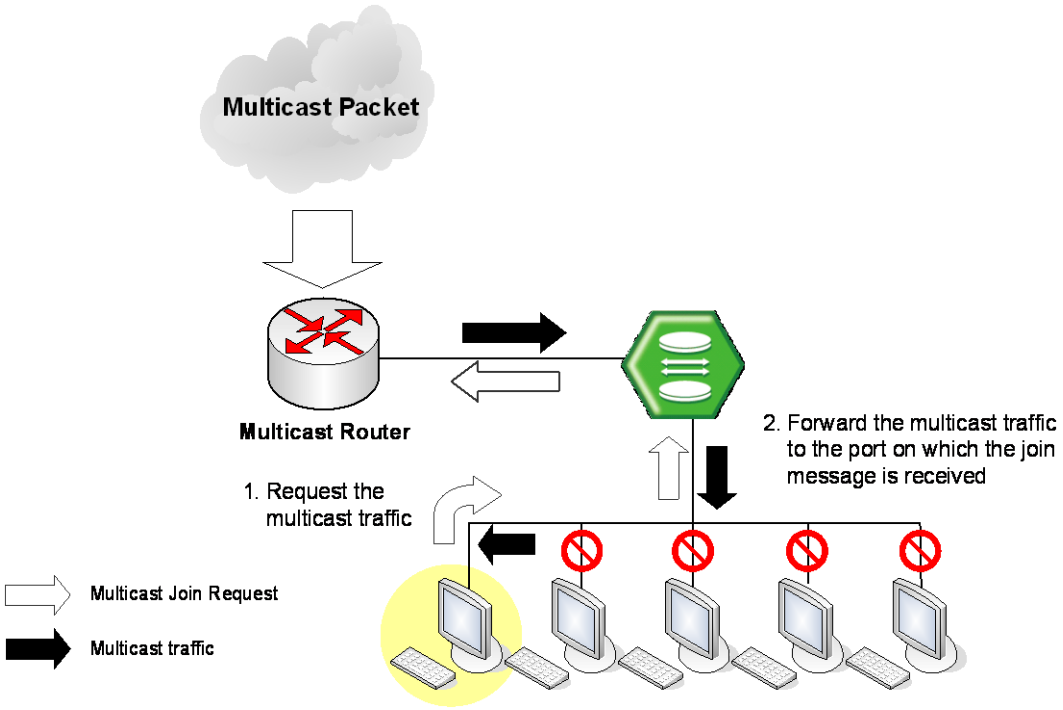


Fig. 9.4 IGMP Snooping

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 robustness-variable	Global	Deletes a specified 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* **immediate-leave**		Enables the IGMP snooping immediate leave on a port. 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-suppression	Global	Disables the IGMP snooping report 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, V5812G 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-tracking group *A.B.C.D*		Shows the explicit host tracking information per group. 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.

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 port {*PORTS* | **cpu**} [**mac-based**]		Shows the IGMP snooping table per port. 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 V5812G 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 untagged.
- 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*	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*		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, V5812G 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 V5812G 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.
- IGMP proxy and PIM on an interface cannot work together.
- 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, V5812G 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 V5812G 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	Disable the RPF check over IGMP packets.
ip igmp verify-sip		Enable the RPF check over IGMP packets (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.



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 V5812G 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

9.3 Multicast Routing

When receivers join a certain group, multicast routers must deliver the multicast traffic corresponding to the group to those receivers. To determine the appropriate forwarding path and to replicate the multicast traffic to multiple destinations, multicast routing protocols are needed.

The multicast routing protocols establish the distribution tree by building a forwarding table in its own way. The forwarding table contains the information of sources, groups, interfaces, and how to forward multicast packets. Note that the multicast has the different routing method from the unicast's.

Reverse Path Forwarding (RPF)

Routers typically forward unicast packets with the destination lookup. When unicast packets come to interfaces, routers forward the packets to the interfaces toward the destinations of those packets by referring to the routing table. If the routing table does not contain the information of the destinations, the routers forward the packets to the default gateway.

On the other hand, routers forward multicast packets based on the source of the packets. When multicast packets come to an interface, routers validate whether the interface on which the packets are received is directly toward the source of those packets by referring to the existing unicast routing table. This procedure is called the reverse path forwarding (RPF) check. If incoming multicast packets pass the RPF check, routers forward the packets to the outgoing interface. If not, routers drop the packets.

In the multicast routing, routers must forward packets away from the sources to prevent routing loops. Finally, the distribution tree established by RPF follows the shortest path tree (SPT) topology.

9.3.1 Multicast Routing

9.3.1.1 Enabling Multicast Routing

By default, multicast routing is disabled. To configure the V5812G to forward multicast traffic via Layer 3 network, you need to enable multicast routing.

To enable Layer 3 multicast routing, use the following command.

Command	Mode	Description
ip multicast-routing	Global	Enables multicast routing.
no ip multicast-routing		Disables multicast routing. (default)

9.3.1.2 TTL Threshold

You can specify a TTL threshold for multicast packets on an interface. This configuration is used on a border router which limits a multicast domain, since only the multicast packets with a TTL value greater than a TTL specified on an interface are forwarded to outgoing interfaces. If you intend the router to operate as a border router, the TTL threshold must be a very high value.

To specify a TTL threshold for multicast packets, use the following command.

Command	Mode	Description
ip multicast ttl-threshold <0-255>	Interface	Specifies a TTL threshold for multicast packets. 0-255: TTL value (default: 1)
no ip multicast ttl-threshold		Deletes a specified TTL threshold for multicast packets.

9.3.1.3 ECMP Load Splitting

Multicast routing protocols have different forwarding policies for the equal cost multipath (ECMP). In case of PIM, the interface with highest IP address is used to forward multicast traffic over the equal cost multipath.

The purpose of this feature is load splitting for forwarding multicast traffic over ECMP, allowing more efficient use of network resources and preventing traffic congestion. With this feature, multicast traffic is split across the equal cost multipath based on either its source address or its source and group address.

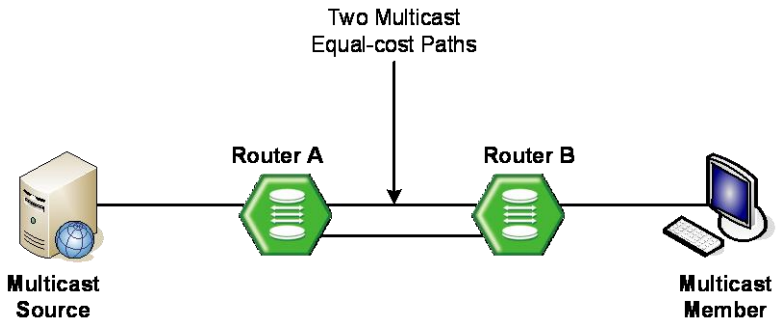


Fig. 9.5 Multicast Equal Cost Multipath (ECMP)

ECMP load splitting has two options for next hop decision:

- **srcip** selects next hop based on source address.
- **srcgrpip** selects next hop based on both source and group address.

To enable ECMP load splitting, use the following command.

Command	Mode	Description
ip multicast multipath [**srcip** | **srcgrpip**]	Global	Enables ECMP load splitting. srcip: source address (default) srcgrpip: source and group address
no ip multicast multipath		Disables ECMP load splitting.

9.3.1.4 MRIB Entry Limit

You can limit the maximum number of multicast routing entries in the multicast routing table in the multicast routing information base (MRIB), and then the system generates an error message when the number of the entries exceeds the limit. If the warning threshold is specified, the system generates a warning message when the number of the entries exceeds the threshold.

To specify the maximum number of multicast routing entries, use the following command.

Command	Mode	Description
ip multicast route-limit *LIMIT* [*THRESHOLD*]	Global	Specifies the limit of the maximum number of multicast routing entries. LIMIT: number of routing entries (1-214783647) THRESHOLD: warning threshold (1-214783647)
no ip multicast route-limit		Deletes a specified limit.



The warning threshold must not exceed the maximum number of multicast routing entries.

9.3.1.5 Displaying MRIB Entry

To display the multicast routing entries in the MRIB, use the following command.

Command	Mode	Description
show ip mroute [**summary**]	Enable Global Bridge	Shows all multicast routing entries. summary: abbreviated display
show ip mroute {**dense** | **sparse**} [**summary**]		Shows the multicast routing entries for a given PIM mode. dense: dense mode sparse: sparse mode
show ip mroute *A.B.C.D* [**dense** | **sparse**] [**summary**]		Shows the multicast routing entries for a given group. A.B.C.D: group address
show ip mroute *A.B.C.D A.B.C.D* [**dense** | **sparse**] [**summary**]		Shows the multicast routing entries for a given group and source. A.B.C.D: group/source address
show ip mroute *A.B.C.D/M* [**dense** | **sparse**] [**summary**]		Shows the multicast routing entries for a given group range. A.B.C.D/M: group address and prefix

If you use the **clear ip mroute** command, the MRIB clears the multicast routing entries in its multicast routing table, and removes the entries from the multicast forwarder.

To delete the multicast routing entries in the MRIB, use the following command.

Command	Mode	Description
clear ip mroute *	Enable Global Bridge	Deletes all multicast route entries.
clear ip mroute *A.B.C.D* [*A.B.C.D*]		Deletes a specified multicast route entry. A.B.C.D: group/source address

To clear the multicast forwarding cache (MFC) and tree information base (TIB) entries in the PIM-SM protocol level, use the following command.

Command	Mode	Description
clear ip mroute * [**pim sparse-mode**]	Enable Global Bridge	Deletes all MFC and TIB entries in the PIM-SM protocol.
clear ip mroute *A.B.C.D* [*A.B.C.D*] [**pim sparse-mode**]		Deletes a specified MFC and TIB entry in the PIM-SM protocol. A.B.C.D: group/source address



When clearing the MRIB entries, you must specify the group address prior to the source address.

9.3.1.6 Displaying MRIB Statistics

To display the multicast routing statistics entries in the MRIB, use the following command.

Command	Mode	Description
show ip mroute count	Enable Global Bridge	Shows all multicast routing statistics entries.
show ip mroute {**dense** | **sparse**} **count**		Shows the multicast routing statistics entries for a given PIM mode. dense: dense mode sparse: sparse mode
show ip mroute *A.B.C.D* [**dense** | **sparse**] **count**		Shows the multicast routing statistics entries for a given group. A.B.C.D: group address
show ip mroute *A.B.C.D A.B.C.D* [**dense** | **sparse**] **count**		Shows the multicast routing statistics entries for a given group and source. A.B.C.D: group/source address
show ip mroute *A.B.C.D/M* [**dense** | **sparse**] **count**		Shows the multicast routing statistics entries for a given group range. A.B.C.D/M: group address and prefix

To delete the multicast routing statistics entries from the multicast routing table, use the following command.

Command	Mode	Description
clear ip mroute statistics *	Enable Global Bridge	Deletes all multicast routing statistics entries.
clear ip mroute statistics *A.B.C.D* [*A.B.C.D*]		Deletes a specific multicast routing statistics entry. A.B.C.D: group/source address

9.3.1.7 Displaying MFIB Information

The multicast forwarding information base (MFIB) is the group of the information to forward multicast traffic in Layer 3, which is maintained by currently running multicast routing protocol. You can verify the forwarding entries in the MFIB with the **show ip mfib** command.

To display the multicast forwarding entries in the MFIB, use the following command.

Command	Mode	Description
show ip mfib [**vlan** *VLANS* | **group** *A.B.C.D*] [**detail**]	Enable Global Bridge	Shows the multicast forwarding entries in the MFIB. VLANS: VLAN ID (1-4094) A.B.C.D: multicast group address

9.3.1.8 MRIB Debug

To debug events in the MRIB, use the following command.

Command	Mode	Description
debug nsm mcast {**all** | **fib-msg** | **mrt** | **register** | **stats** | **vif**}	Enable	Debugs events in the MRIB. all: all multicast debugging fib-msg: MFIB messages mrt: multicast routes register: multicast PIM register messages stats: multicast statistics vif: multicast interface
no debug nsm mcast { **fib-msg** | **mrt** | **register** | **stats** | **vif**}		Disables the debug event.

9.3.2 PIM Basic

Protocol Independent Multicast (PIM) is the most widely deployed multicast routing protocol. It may use the underlying unicast routing information base, but is not dependent on any particular unicast routing protocol. PIM has two operation modes, which are called PIM Sparse Mode (PIM-SM) and PIM Dense Mode (PIM-DM), each optimized for a different environment.

PIM-SM is a multicast routing protocol efficient for multicast groups that may span wide-area (and inter-domain) internets. In the sparse mode, routers forward multicast packets only when they receives explicit join messages from neighboring routers that have downstream group members. PIM-SM uses a unidirectional shared tree per group to deliver multicast traffic, and optionally uses the shortest path tree per source.

PIM-DM is a multicast routing protocol efficient for multicast groups that are densely populated across a network. In the dense mode, routers initially flood multicast datagrams to all multicast routers, since they assume that all downstream systems want to receive multicast packets. Prune messages are then used to prevent from propagating to routers with no group members. Both PIM protocols use the same message formats.

i The V5812G currently support PIM-SM only.

PIM Messages

The followings are simple descriptions of PIM control messages:

- **Hello**
  PIM routers periodically send hello messages on all interfaces to discover neighboring PIM routers and to determine which router will be the DR for each subnet.

- **Register**
  Register messages are sent by the DR to the RP when a multicast packet needs to be transmitted on the RPT. These messages may contain the encapsulated multicast traffic. Both register and register-stop messages are unicast.
- **Register-stop**
  When receiving the register-stop message, routers stop sending register messages. These messages are sent from the RP to the sender of the register messages.
- **Join/prune**
  Join/prune messages are sent by routers towards upstream sources or RPs. Join messages are sent to receive the multicast traffic by building shared trees (RPT) or source trees (SPT). Prune messages are sent to prune established distribution trees when there are no more interests in the traffic.
- **Bootstrap**
  The bootstrap router (BSR) sends bootstrap messages to elect the Rendezvous Point (RP), which contain a set of the information for each candidate RP (RP-set).
- **Assert**
  Assert messages are used to resolve forwarding conflicts among routers.
- **Candidate RP advertisement**
  Each candidate RP unicasts these messages containing its own information to the BSR. The BSR then includes a set of that information in the bootstrap message.

9.3.2.1 PIM Mode

To enable PIM-SM on an interface, use the following command.

Command	Mode	Description
ip pim sparse-mode	Interface	Enables PIM-SM on an interface.
no ip pim sparse-mode		Disables PIM-SM on an interface.

You can also enable PIM-SM as the passive mode. The passive mode operation is for local members. The passive mode disables sending/receiving PIM packets on an interface, allowing only IGMP mechanism to be active.

To enable PIM-SM passive mode on an interface, use the following command.

Command	Mode	Description
ip pim sparse-mode passive	Interface	Enables PIM-SM passive mode on an interface.
no ip pim sparse-mode passive		Disables PIM-SM passive mode on an interface.

9.3.2.2 DR Priority

In PIM-SM, the designated router (DR) is normally the first-hop router of receivers (hosts), which is responsible to periodically send PIM join/prune messages toward the RP to inform it of the host group membership.

When there are multiple routers on the same subnet, one of them must be selected to act as the DR. To elect the DR, each PIM router examines PIM hello messages received from

other neighbor PIM routers and compares its DR priority in those from neighbors. The router with the highest priority then is elected as the DR. In case of more than one router with the same highest priority value, the one with the higher IP address is elected. If no PIM hello message is received from the DR for a certain period of time, another DR election is held.

In PIM-DM, however, the DR only plays a role of the alternative IGMP querier using this DR election when multiple routers exist with IGMPv1, since IGMPv1 does not define any IGMP querier election process.

To specify the DR priority on an interface, use the following command.

Command	Mode	Description
ip pim dr-priority <0-4294967294>	Interface	Specifies the DR priority on an interface. 0-4294967294: priority value (default: 1)
no ip pim dr-priority <0-4294967294>		Deletes the specified DR priority.
no ip pim dr-priority		

i The DR and the IGMP querier may be different routers in IGMPv2, while those are typically the same router in IGMPv1. In IGMPv2, the DR is the router with the highest IP address on the subnet, whereas the IGMP querier is the router with the lowest IP address.

9.3.2.3 Neighbor Filtering

If necessary, you can filter neighbor routers using access lists. When you enable this feature, PIM establishes adjacency without neighbor routers specified as deny in access lists.

To enable filtering neighbor routers in PIM, use the following command.

Command	Mode	Description
ip pim neighbor-filter {<1-99> | *WORD*}	Interface	Enables filtering neighbor routers in PIM. 1-99: IP standard access list WORD: access list name
no ip pim neighbor-filter {<1-99> | *WORD*}		Disables filtering neighbor routers in PIM.

To display the information of PIM neighbor routers, use the following command.

Command	Mode	Description
show ip pim neighbor [**detail**]	Enable Global Bridge	Shows the information for PIM neighbor routers.

9.3.2.4 PIM Join/Prune Message Group Filtering

If necessary, you can filter PIM join/prune messages from seperate group using access lists. When you enable this feature, a specifid PIM group of PIM join/prune messages from the trusted neighbor are denied by a specified range of access lists.

To enable PIM group filtering, use the following command.

Command	Mode	Description
ip pim group-filter {<1-99> | *WORD*}	Interface	Enables PIM group filtering to block PIM join/prune messages using a specified access list. 1-99: IP standard access list WORD: access list name
ip pim group-filter range {<1-1024> | *WORD*}		Enables PIM group filtering to block PIM join/prune messages using a specified range of access lists. 1-1024: IP standard access list range WORD: IP access-list-range name
no ip pim group-filter [**range**]		Disables PIM group filtering.



For more information of Standard Access List and Access List Range, see Section 7.18.1 and 7.18.4.

9.3.2.5 PIM Hello Message

PIM routers periodically send PIM hello messages to discover neighboring PIM routers and to determine which router will be the DR for each subnet. PIM hello messages are also the multicast packets using the group address 224.0.0.13 (all PIM routers group).

To specify an interval to send PIM hello messages, use the following command.

Command	Mode	Description
ip pim query-interval <1-18724>	Interface	Specifies an interval to send PIM hello messages. 1-18724: hello message interval (unit: second)
no ip pim query-interval		Deletes a specified interval to send PIM hello messages.

PIM hello messages may contain the hold time value in the option fields, which specifies how long the information is valid. The default hold time is 3.5 times of the interval of the PIM hello messages. If a hold time you specified is less than the current interval of those, the hold time will be ignored and return to the default value.

To specify a hold time of PIM hello messages, use the following command.

Command	Mode	Description
ip pim query-holdtime <1-65535>	Interface	Specifies a hold time of PIM hello messages. 1-65535: hello message hold time (unit: second)
no ip pim query-holdtime		Deletes a specified hold time of PIM hello messages.

9.3.2.6 PIM Join/Prune Interval

PIM routers periodically send PIM join/prune messages to a group. If a router does not send the join message during 3 times of the specified interval, it will be pruned from the group.

To specify an interval to send PIM join/prune messages, use the following command.

Command	Mode	Description
ip pim message-interval <1-65535>	Global	Specifies an interval to send join/prune messages. 1-65535: join/prune message interval (unit: second)
no ip pim message-interval		Deletes a specified interval to send join/prune messages.

9.3.2.7 PIM VIF Flap Discredit

PIM VIF is a PIM-specific virtual interface that is used to send or receive PIM control packets in the implementation level. It includes the methods for processing and composing PIM control messages, as well as various states per interface.

PIM routers are internally connected with PIM VIFs, and the equal cost multipath (ECMP) can also exist between them. Under the ECMP environment, a traffic flow is split across the multipath based on its source and group address as the physical interface's case. However, if a VIF flapping happens, the forwarding path for the flow must be recalculated, causing low multicast forwarding performance.

PIM VIF flap discredit function has been designed to minimize such a path recalculation caused by the VIF flapping, which can increase the stability and quality for multicast service. Using this function, the V5812G gives a discredit to a VIF for every flapping time, and then the VIF is not selected as a forwarding path until its credit is regenerated.

To enable/disable the PIM VIF flap discredit function, use the following command.

Command	Mode	Description
ip pim vif flap discredit	Global	Enables the PIM VIF flap discredit. (default)
no ip pim vif flap discredit		Disables the PIM VIF flap discredit.

To set the discredit value for the VIF flapping, use the following command.

Command	Mode	Description
ip pim vif flap discredit unit <10-50>	Global	Sets the discredit value for the VIF flapping. (default: 10)
no ip pim vif flap discredit unit		Deletes a configured discredit value.

To set the VIF credit regenerating rate, use the following command.

Command	Mode	Description
ip pim vif flap discredit half-recover-time <0-3600>	Global	Sets the VIF credit regenerating rate. (default: 10 seconds)
no ip pim vif flap discredit half-recover-time		Deletes a configured VIF credit regenerating rate.

If you configure this rate as 0, the VIF credit is not regenerated!

To set the current credit as the default (100), use the following command.

Command	Mode	Description
clear ip pim vif flap discredit [**vif** <0-127>]	Enable Global	Sets the current credit as the default (100). 0-127: VIF index

9.3.2.8 PIM Static Join

The IGMP static join feature supports an IGMPv2 host only. PIM static join has been also developed to reduce the zapping time by statically creating a virtual host that behaves like a real on a port. However, IGMP static join feature can not be used by Layer 3 device (Core switch) that is incapable of IGMP feature with no group member (host). In this case, you can use PIM static join instead of IGMP static join.

To configure the PIM static join, use the following command.

Command	Mode	Description
ip pim static-group *A.B.C.D*	Interface	Configures the PIM static join. A.B.C.D: Start/End multicast group address
ip pim static-group range *A.B.C.D A.B.C.D*		
no ip pim static-group [*A.B.C.D* | *]		Deletes the configured PIM static join. *: all addresses
no ip pim static-group range *A.B.C.D A.B.C.D*		

9.3.2.9 Displaying PIM Information

To display current PIM information, use the following command.

Command	Mode	Description
show ip pim interface [**detail**]	Enable Global Bridge	Shows PIM interface information. detail: includes VIF information
show ip pim local-members [*INTERFACE*]		Shows PIM local membership information.
show ip pim mroute *A.B.C.D* [*A.B.C.D*]		Shows the multicast routing table. A.B.C.D: multicast group or source address A.B.C.D/M: range of multicast group addresses static: static multicast route entry summary: summary of multicast route entry
show ip pim mroute [*A.B.C.D/M* | **static** | **summary**]		
show ip pim nexthop		Shows the next hop information. A.B.C.D | *: specific or any source address A.B.C.D: multicast group address
show ip pim nexthop {*A.B.C.D* | ***}** [*A.B.C.D*]		

9.3.3 PIM-SM

Rendezvous Point Tree (RPT)

PIM-SM mainly uses a shared tree to deliver multicast traffic, called the RP tree (RPT). As its name implies, it relies on a core router called the Rendezvous Point (RP) that receives all multicast traffic from the sources and forwards that traffic to the receivers. Other routers do not need to know the information of the sources. All they need to know is the address of the RP, because the RP surely knows the information of the sources for all multicast groups. Thus, receivers who are interested in a certain multicast group only send PIM join messages with (*, G) state toward the RP. That is, the RPT prevent each router from maintaining source and group (S, G) states for every multicast source. This mechanism shifts the burden of finding the multicast sources from each router to the network itself.

The shared tree is unidirectional, which means all multicast traffic flows only from the RP to the receivers. Thus, there is no guarantee that the shared tree (RPT) is the shortest path tree to the source, and most likely it is not, resulting in longer delays, but less forwarding states to maintain. Each multicast group has only one RP that may be different; each multicast group may have the different distribution tree.

Fig. 9.6 shows an example of the RPT network. The multicast traffic from the source A flows through the router B to the router D which is the RP. Note that, even in the RPT, RPs must receive multicast traffic from the sources via the shortest path. The RP then distributes the traffic to the receiver E and F that indicate the interest in the multicast group. Consequently, the distribution tree for the receiver E is **A→B→D→E**, and the one for the receiver F is **A→B→D→C→F**.

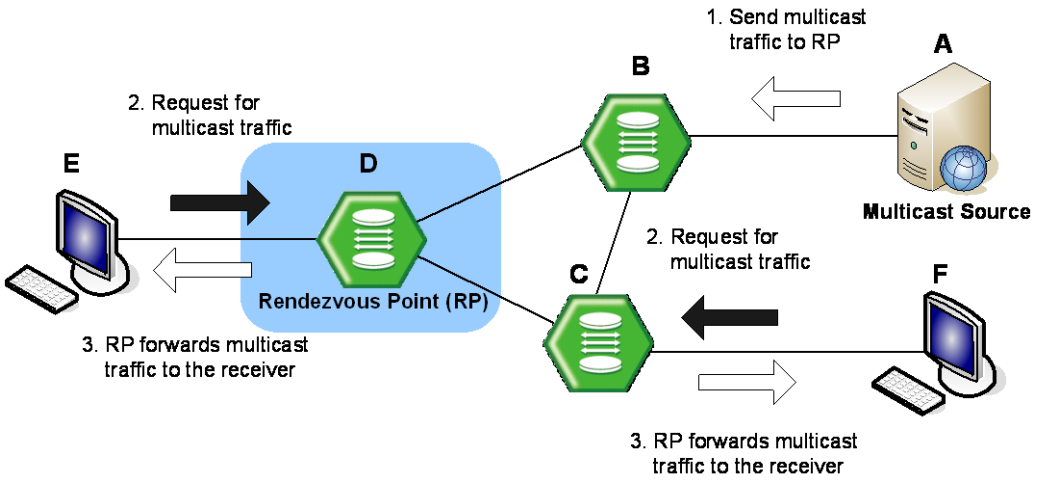


Fig. 9.6 Rendezvous Point Tree

Shortest Path Tree (SPT)

When the number of receivers increases, a shared tree may not be entirely efficient, so PIM-SM also provides the option to switch to receive multicast traffic on a shortest path tree (SPT). When this option is enabled, on receiving the first multicast packet from the RP in response to the PIM join message, the switchover to the SPT then occurs.

To establish the SPT to the multicast source, the DR sends the join message with (S, G) state toward that source. When the SPT between the receiver and source is established, and multicast traffic is sent via that distribution tree, the DR sends the prune message with (*, G) state toward the RP to prune the existing shared tree to receive the traffic.

SPT is established based on the existing unicast routing table by performing the RPF check. It has a different distribution tree for every multicast source, allowing the efficient network traffic flows, but more resources are needed for each multicast routers to maintain (S, G) states.

Fig. 9.7 shows an example of the SPT switchover. The multicast traffic from the source A initially attempts to flow through the router B and C to the receiver D that indicates the interest in the multicast group. Once the traffic arrives at the router C which is the DR, it sends the join message with (S, G) state toward the source A to build the SPT between the source and receiver. The source A then sends the multicast traffic to the receiver D via the SPT by deleting unnecessary hops. Finally, the distribution tree (SPT) built by the RPF check is **A→C→D**.

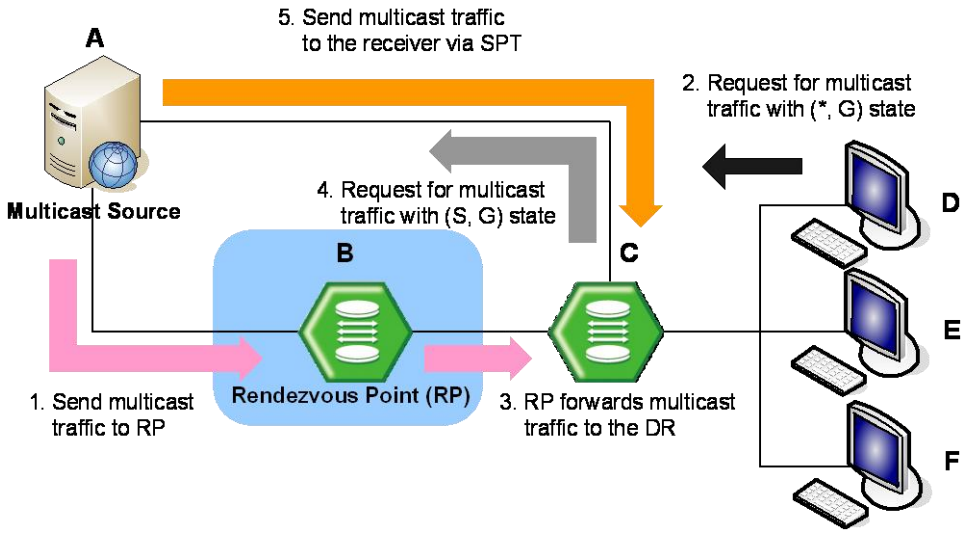


Fig. 9.7 Shortest Path Tree

PIM-SM Operation

When multicast receivers indicate their interests in certain multicast groups, the DR of the receivers sends PIM join messages with (*, G) state toward the RP for those groups. While the join messages flow hop-by-hop toward the RP, each PIM router along the path adds the interface on which the join messages are received to the outgoing interface (OIF) list with the join state, and sends the messages to the interface toward the RP.

If the RP has receivers interested in the group, the RP must receive the multicast traffic from the source of that group via the SPT to deliver the traffic to those receiver. The DR of the source encapsulates the multicast packets in the PIM register messages, and starts to unicast them to the RP. On receipt of the register messages, the RP sends the join message with (S, G) state toward the source to establish the SPT. When receiving the multicast traffic via the established SPT, the RP forwards the traffic toward those receivers.

Multicast traffic may be directly delivered from sources to receivers via the SPT using the switchover mechanism. For more information, see Section 9.3.3.4.

9.3.3.1 Rendezvous Point

In a shared tree, Rendezvous Point (RP) is a means for receivers to discover the sources that send to a particular multicast group. It is responsible to receive all multicast traffic from the sources and to forward that traffic to the receivers.

Static RP

To elect the RP among candidate RPs in the shared tree, the V5812G supports the BSR mechanism (see Section 9.3.3.2) and static RP, and also supports the simultaneous use of those. You can configure a router to use the static RP either for all the multicast groups (default) or for specific multicast groups (with access lists). If multiple static RPs are available for a single multicast group, the one with the highest IP address will be elected.

To statically specify an RP address for multicast groups, use the following command.

Command	Mode	Description
ip pim rp-address *A.B.C.D* [<1-99> | <1300-1999>] [**override**]	Global	Specifies an RP address for multicast groups. A.B.C.D: RP address 1-99: IP standard access list 1300-1999: IP standard access list (extended range)
no ip pim rp-address *A.B.C.D*		Deletes a specified RP address for multicast groups

i When the static RP and the RP elected through the BSR are both available for a multicast group, the one elected through the BSR is chosen by default. If you, however, want to choose the static RP for a multicast group in that situation, use the **override** option that gives the higher priority to the static RP.

Keep Alive Time

After a multicast source registers with the RP, the DR of the multicast source periodically sends the PIM null-register message to the RP to keep the (S, G) state between the router and RP. The null-register message is the one without encapsulated multicast traffic. If there is no null-register message during a given keep alive time (KAT), the multicast routing entry with (S, G) state is expired, and the source registration process will restart.

To specify the keep alive time for (S, G) states at the RP, use the following command.

Command	Mode	Description
ip pim rp-register-kat <1-65535>	Global	Specifies the KAT for (S, G) states at the RP. 1-65535: KAT value(unit: second)
no ip pim rp-register-kat		Deletes the specified KAT value.

Interface for Candidate RP

To elect the RP, each candidate RP sends its information to the BSR. This advertisement contains the IP address and priority of the candidate RP and the multicast groups that it can service. The BSR then periodically distributes the bootstrap message that includes a set of the information received from each candidate RP (RP-set) to all the routers in the PIM-SM domain.

To configure an interface to send the candidate RP advertisement to the BSR, use the following command.

Command	Mode	Description
ip pim rp-candidate *INTERFACE* [**group-list** <1-99>] [**interval** <1-16383>] [**priority** <0-255>]	Global	Configures an interface to send the candidate RP advertisement. INTERFACE: interface name 1-99: IP standard access list 1-16383: advertising interval (unit: second) 0-255: priority value
no ip pim rp-candidate *INTERFACE* **group-list** <1-99>		Deletes specified multicast groups which an interface can service.
no ip pim rp-candidate *INTERFACE*		Configures an interface not to send the candidate RP advertisement.
no ip pim rp-candidate		Configures an interface not to send the candidate RP advertisement as well as deletes specified candidate RP information.

i The access list with this command specifies the multicast groups that an advertising router can service. The candidate RP information without the access lists means that the router will service all the multicast groups.

Ignoring RP Priority

Normally, when choosing the RP among candidate RPs, routers examine the bootstrap messages sent from the BSR, and then choose the one has the highest priority among the RP-set. You can configure a router to only use the hash mechanism for the RP choice instead of the RP priority. This feature is used to interoperate with a router that cannot recognize the RP priority.

To configure a router to use the hash mechanism for the RP choice, use the following command.

Command	Mode	Description
ip pim ignore-rp-set-priority	Global	Enables ignoring the PR priority for the RP choice.
no ip pim ignore-rp-set-priority		Disables ignoring the PR priority for the RP choice.

Displaying RP Information

To display the RP information, use the following command.

Command	Mode	Description
show ip pim rp mapping	Enable Global Bridge	Shows group-to-RP mappings and the RP-set.
show ip pim rp-hash *A.B.C.D*		Shows the RP to be chosen for a specified group. A.B.C.D: multicast group address

9.3.3.2 Bootstrap Router

The bootstrap router (BSR) mechanism is one way that a multicast router can learn the set of group-to-RP mappings required in order to function.

All multicast routers in PIM-SM domain can be potentially the bootstrap router (BSR); they are all considered as candidate BSRs. To elect the BSR among the candidate BSRs, each candidate BSR floods the bootstrap messages with its information to the domain. When receiving the bootstrap messages, the candidate BSRs examine the messages, and then the one with the highest priority is elected as the BSR. If more than one candidate with the same highest priority, the one with the higher IP address is elected.

The elected BSR is responsible to periodically send out bootstrap messages including the RP-set, allowing all the routers in the PIM-SM domain determine which router is the RP that covers given multicast groups.

Interface for Candidate BSR

To configure an interface to flood the candidate BSR advertisement, use the following command.

Command	Mode	Description
ip pim bsr-candidate *INTERFACE*	Global	Configures an interface to flood the candidate BSR advertisement. INTERFACE: interface name 0-32: hash mask length for RP selection 0-255: priority for candidate BSR
ip pim bsr-candidate *INTERFACE* <0-32>		
ip pim bsr-candidate *INTERFACE* <0-32> <0-255>		
no ip pim bsr-candidate		Configures an interface not to flood the candidate BSR advertisement.

Clearing RP-Set

The BSR periodically distributes the bootstrap message that includes a set of the information received from each candidate RP (RP-set) to all the routers in the PIM-SM domain. You can also clear all RP-set to reset.

To clear all RP-set, use the following command.

Command	Mode	Description
clear ip pim sparse-mode bsr rp-set *	Global	Clears all RP-set.

Displaying BSR Configuration

To display the BSR information, use the following command.

Command	Mode	Description
show ip pim bsr-router	Enable Global Bridge	Shows the BSR information.

9.3.3.3 Source Registration

Multicast sources do not need any join process to send multicast traffic, since the DR of the multicast sources just receives the traffic from the sources without any information. Even in the RPT, RPs must receive multicast traffic from the sources via the shortest path while receivers receive multicast traffic via the shared tree. Thus, the DR needs to inform the RP about the information for the source, and the SPT must be established between the DR and RP via (S, G) states.

In case of the registration for a source, when receiving multicast traffic from the source, the DR encapsulates the multicast traffic in the PIM register message, and constantly unicasts it to the RP. The RP receives the register message, and then sends the PIM join message with (S, G) state back toward the DR to establish the SPT between them. Once the DR receives the join message, the SPT is then established, and the DR begins sending the multicast traffic without an encapsulation to the RP. When receiving the native multicast traffic, the RP unicasts the PIM register-stop message back to the DR. The DR then stops encapsulating the multicast traffic in the register message.

Registration Rate Limit

You can limit the maximum number of the PIM register message packets per second. If you enable this feature, both DR and RP will discard the register messages that exceed the limit.

To enable the rate limit for PIM register message, use the following command.

Command	Mode	Description
ip pim register-rate-limit <1-65535>	Global	Enables the rate limit for PIM register message. 1-65535: maximum number of packets that can be sent per second
no ip pim register-rate-limit		Disables the rate limit for PIM register message.

Registration Suppression Time

Once a multicast routing entry with (S, G) state is established by the source registration, the periodic reregistration is needed to keep the state for the entry. After the registration, the DR periodically sends the PIM null-register message that does not contain the encapsulated multicast traffic to the RP, and the RP returns the register-stop message. If there is no response to the null-register message during a given period, the multicast routing entry with (S, G) state is expired, and the source registration process will start again.

You can specify the interval to send the PIM null-register message which is also called the registration suppression time. When you specify this value at the RP, the configuration modifies the keep alive time (KAT) for the RP, if the **ip pim rp-register-kat** command is not used.

To specify the registration suppression time, use the following command.

Command	Mode	Description
ip pim register-suppression <1-65535>	Global	Specifies the registration suppression time. 1-65535: null-register message interval (unit: second)
no ip pim register-suppression		Deletes the specified the registration suppression time.

Register Message Filtering

You can enable the router to filter multicast sources specified in access lists at the RP. This filtering will permit/deny the PIM register messages for the specified sources. If unauthorized sources try to register with the RP, the RP then drops the PIM register messages from those sources. You can specify the either multicast source or source's DR address in access lists.

To enable the router to filter multicast sources, use the following command.

Command	Mode	Description
ip pim accept-register list {<100-199> | <2000-2699> | *WORD*}	Global	Enables the router to filter multicast sources. 100-199: IP extended access list 2000-2699: IP extended access list (extended range) WORD: access list name
no ip pim accept-register		Disables the router to filter multicast sources.

RP Reachability Validation

To enable the RP reachability validation for the source registration process at the first-hop router, use the following command.

Command	Mode	Description
ip pim register-rp-reachability	Global	Enables the RP reachability validation.
no ip pim register-rp-reachability		Disables the RP reachability validation. (default)

Source Address of Register Message

You can specify the source IP address of PIM register messages sent by the DR. This address is used to send corresponding PIM register-stop messages in response. By default, the source address of register messages is the IP address of the interface toward the RP. This address must be able to be learned by unicast routing protocols on the DR.

To specify the source IP address of PIM register messages, use the following command.

Command	Mode	Description
ip pim register-source {*A.B.C.D* | *INTERFACE*}	Global	Specifies the source IP address of register messages. A.B.C.D: source IP address INTERFACE: interface name
no ip pim register-source		Deletes a specified source IP address of register messages.

9.3.3.4 SPT Switchover

PIM-SM provides the switching option to deliver multicast traffic on the SPT. Multicasting over the SPT may be more efficient than multicasting over the RPT, since it can substantially reduce the network latency.

When the switching option is enabled, once multicast traffic from sources arrives at the DR, the switchover to the SPT then occurs. This option only provides the binary option, meaning that the switching to the SPT occurs either when receiving the first multicast packet, or not at all; it is not rate-based. You can enable this option only for specified multicast groups using access lists.

To enable the switchover to the SPT, use the following command.

Command	Mode	Description
ip pim spt-threshold	Global	Enables the switchover to SPT.
ip pim spt-threshold group-list {<1-99> | <1300-1999> | *WORD*}		Enables the switchover to SPT for specified multicast groups. 1-99: IP standard access list 1300-1999: IP standard access list (extended range) WORD: access list name

To disable the switchover to the SPT, use the following command.

Command	Mode	Description
no ip pim spt-threshold	Global	Disables the switchover to SPT.
no ip pim spt-threshold group-list {<1-99> | <1300-1999> | *WORD*}		

i The switchover to the SPT to deliver multicast traffic is disabled by default.

9.3.3.5 Cisco's Router Interoperability

Register Message Checksum

When a multicast source registers with the RP, the DR encapsulates the multicast traffic from the source in the PIM register message, and unicasts it to the RP. The standard PIM protocol specifies that the checksum field in the register message contains the checksum for the entire register message excluding the data portion, the encapsulated multicast traffic.

The Cisco's routers, however, validate the checksum for the whole register message including the data portion, resulting in incompatibility with the standard-based routers. To guarantee compatibility with the Cisco's routers, the V5812G provides the checksum option, which expands the range of the checksum calculation.

To enable the Cisco checksum option, use the following command.

Command	Mode	Description
ip pim cisco-register-checksum	Global	Enables the Cisco checksum option.
ip pim cisco-register-checksum group-list {<1-99> | <1300-1999> | *WORD*}		Enables the Cisco checksum option for specified multicast groups. 1-99: IP standard access list 1300-1999: IP standard access list (extended range) WORD: access list name

To disable the Cisco checksum option, use the following command.

Command	Mode	Description
no ip pim cisco-register-check-sum	Global	Disables the Cisco checksum option.

Candidate RP Message

Some Cisco's BSRs do not comply with the BSR standards; they do not accept candidate RPs with a group prefix number of zero. You can configure the router to send candidate RP messages with the option for the compatibility with the Cisco's BSR.

To enable the candidate RP message option for the Cisco compatibility, use the following command.

Command	Mode	Description
ip pim crp-cisco-prefix	Global	Enables the candidate RP message option for the Cisco compatibility.
no ip pim crp-cisco-prefix		Disables the candidate RP message option for the Cisco compatibility.

Excluding GenID Option

PIM hello messages may contain the generation ID (GenID) in the option fields, which is a random value for the interface on which the hello message is sent. The GenID is regenerated whenever PIM forwarding is started or restarted on the interface. It enables

neighbors to quickly detect a router's reboot and thus to synchronize RP-set information and forwarding states by triggering the bootstrap and join/prune messages to the rebooted router. The rebooted router then is able to quickly recover from the reboot.

Some older Cisco's routers cannot recognize the GenID option in the hello messages, so the V5812G provides the exclude-GenID option for the compatibility with the Cisco's routers.

To exclude the GenID option from the PIM hello messages, use the following command.

Command	Mode	Description
ip pim exclude-genid	Interface	Excludes the GenID from the hello messages.
no ip pim exclude-genid		Includes the GenID from the hello messages.

9.3.3.6 PIM Debug

To enable PIM-SM debugging, use the following command.

Command	Mode	Description
debug pim {**all** | **events** | **nexthop** | **mib** | **mfc** | **nsm** | **state** | **packet** [**in** | **out**]}	Enable	Enables PIM-SM debugging. all: all PIM-SM debugging events: events debugging nexthop: nexthop communications debugging mib: MIBs debugging mfc: MFC add/delete/update debugging nsm: NSM communications debugging state: debugging of state transition on all FSMs packet: incoming and/or outgoing packets debugging
no debug pim {**all** | **events** | **nexthop** | **mib** | **mfc** | **nsm** | **state** | **packet** [**in** | **out**]}		Disables PIM-SM debugging.

To enable PIM-SM timer debugging, use the following command.

Command	Mode	Description
debug pim timer	Enable	Enables PIM-SM timer debugging.
debug pim timer assert [**at**]		Enables PIM-SM assert timer debugging.
debug pim timer bsr [**bst** | **crp**]		Enables PIM-SM BSR timer debugging. bst: bootstrap debugging timer crp: candidate RP debugging timer
debug pim timer hello [**ht** | **nlt** | **tht**]		Enables PIM-SM hello timer debugging. ht: hello timer nlt: neighbor liveness timer tht: triggered hello timer
debug pim timer joinprune [**jt** | **et** | **ppt** | **kat** | **ot**]		Enables PIM-SM join/prune timer debugging. jt: join timer et: expiry timer ppt: prune pending timer kat: keep alive timer

		ot: override timer
debug pim timer register [**rst**]		Enables PIM-SM register timer debugging.

To disable PIM-SM timer debugging, use the following command.

Command	Mode	Description
no debug pim timer	Enable	Disables PIM-SM timer debugging.
no debug pim timer assert [**at**]		
no debug pim timer bsr [**bst** | **crp**]		
no debug pim timer hello [**ht** | **nlt** | **tht**]		
no debug pim timer joinprune [**jt** | **et** | **ppt** | **kat** | **ot**]		
no debug pim timer register [**rst**]		

9.3.4 Source Specific Multicast (SSM)

Multicast supports both many-to-many and one-to-many models, which are also known as Any Source Multicast (ASM). In this model, receivers may join and leave multicast groups with (*, G) state that indicates any source and group G. Since there is no means to specify the source's information, source discovery such as the RP mechanism in PIM-SM is needed, which is the key feature of ASM. Each group address is identified as 224.0.0.0 to 239.255.255.255 (224/4).

Source-Specific Multicast (SSM) is another multicast model especially for one-to-many. In the SSM service model, receivers can receive multicast traffic by subscribing to channel (S, G) that indicates specific source S and group G. Since SSM assumes that receivers already know the source's information, no further source discovery is provided. Thus, receivers need to know the source's information using an out of band mechanism. The SSM group address range is defined as 232.0.0.0 to 232.255.255.255 (232/8) by default.

9.3.4.1 PIM-SSM

PIM Source-Specific Multicast (PIM-SSM) is a subset of PIM-SM. It is much simpler than PIM-SM, because it only considers one-to-many multicast service model. PIM-SSM only use a shortest path tree (SPT) to deliver multicast traffic, so the PIM-SM's complex mechanisms such as RP, BSR, SPT switchover and a shared tree are not necessary any more. PIM-SSM uses the same PIM messages as PIM-SM's for its operation.

If all routers are configured with PIM-SM and IGMPv3, only by using the **ip pim ssm** command, PIM-SSM will be enabled. You can also define an additional SSM group other than the default SSM group range 232/8.

To enable PIM-SSM, use the following command.

Command	Mode	Description
ip pim ssm default	Global	Enables PIM-SSM for the group range 232/8.
ip pim ssm range {<1-99> | *WORD*}		Enables PIM-SSM for a specified group range. 1-99: standard access list WORD: access list name
no ip pim ssm		Disables PIM-SSM.

9.3.4.2 Static SSM Mapping

The purpose of static SSM mapping is to provide SSM service on IGMPv1 and IGMPv2 messages. It means that it enables a multicast host to signal to a router which groups it wants to receive multicast traffic from, and from which sources this traffic is expected. You can specify a source address of multicast server to receive the multicast traffic from specified sources. If V5812G receives IGMPv1 or IGMPv2 report message from the host when static SSM mapping is enabled, it handles as if it receives IGMPv3 report messages.

Static SSM mapping implemented for the V5812G has the following restriction, so you must keep it in mind, before configuring static SSM mapping.



IGMP proxy and static SSM mapping cannot be enabled together. It means that SSM mapping cannot be enabled when the system is already configured with upstream or downstream interface with IGMP proxy feature.

Before configuring static SSM mapping, you should first globally enable SSM mapping. To enable static SSM mapping, use the following command.

Command	Mode	Description
ip igmp ssm-map enable	Global	Enables SSM mapping for groups in a configured SSM range.
no ip igmp ssm-map enable		Disables SSM mapping for groups.

To configure the switch to statically map groups that match specified ACL to source address, use the following command.

Command	Mode	Description
ip igmp ssm-map static {<1-99> | <1300-1999> | *WORD*} *A.B.C.D*	Global	Enables a static SSM mapping for the group that matches specified ACL and source address. 1-99: standard access list number 1300-1999: extended range of standard access list WORD: IP named standard access list A.B.C.D: source address to use for static map group
no ip igmp ssm-map static {<1-99> | <1300-1999> | *WORD*} *A.B.C.D*		Disables a static SSM mapping for the group that matches specified ACL and source address.

To display the sources that SSM mapping uses for a particular group, use the following command.

Command	Mode	Description
show ip igmp ssm-map [*A.B.C.D*]	Enable Global Bridge	Shows a static SSM mapping information A.B.C.D: multicast group address

10 IP Routing Protocol

10.1 Border Gateway Protocol (BGP)

The Border Gateway Protocol (BGP) is an exterior gateway protocol (EGP) that is used to exchange routing information among routers in different autonomous systems (AS). BGP routing information includes the complete route to each destination. BGP uses the routing information to maintain a database of network reachability information, which it exchanges with other BGP systems. BGP uses the network reachability information to construct a graph of AS connectivity, thus allowing BGP to remove routing loops and enforce policy decisions at the AS level.

Multiprotocol BGP (MBGP) extensions enable BGP to support IPv6. MBGP defines the attributes MP_REACH_NLRI and MP_UNREACH_NLRI, which are used to carry IP v6 reachability information. Network layer reachability information (NLRI) update messages carry IPv6 address prefixes of feasible routes.

BGP allows for policy-based routing. You can use routing policies to choose among multiple paths to a destination and to control the redistribution of routing information.

BGP uses the Transmission Control Protocol (TCP) as its transport protocol, using port 179 for establishing connections. Running over a reliable transport protocol eliminates the need for BGP to implement update fragmentation, retransmission, acknowledgment, and sequencing.

The routing protocol software supports BGP version 4. This version of BGP adds support for classless interdomain routing (CIDR), which eliminates the concept of network classes. Instead of assuming which bits of an address represent the network by looking at the first octet, CIDR allows you to explicitly specify the number of bits in the network address, thus providing a means to decrease the size of the routing tables. BGP version 4 also supports aggregation of routes, including the aggregation of AS paths

An Autonomous System (AS) is a set of routers that are under a single technical administration and normally use a single interior gateway protocol and a common set of metrics to propagate routing information within the set of routers. To other ASs, an AS appears to have a single, coherent interior routing plan and presents a consistent picture of what destinations are reachable through it.

The two most important consequences are the need for interior routing protocols to reach one hop beyond the AS boundary, and for BGP sessions to be fully meshed within an AS. Since the next-hop contains the IP address of a router interface in the next autonomous system, and this IP address is used to perform routing, the interior routing protocol must be able to route to this address. This means that interior routing tables must include entries one hop beyond the AS boundary. When a BGP routing update is received from a neighboring AS, it must be relayed directly to all other BGP speakers in the AS. Do not expect to relay BGP paths from one router, through another, to a third, all within the same AS.

10.1.1 Basic Configuration

10.1.1.1 Configuration Type of BGP

When configuring BGP, you can select BGP configuration type between standard BGP and ZebOS BGP for the V5812G.

The standard BGP is one of the general BGP configuration type, which includes the following restrictions.

- **Manual transmission of community information**
  You should send the community information or message to neighbors directly using the **neighbor** {*A.B.C.D* | *WORD*} **send-community** command.
- **No synchronization**
  Standard configuration type does not support a synchronization between IGP and eBGP. In this type, BGP network disables IGP synchronization in BGP by default.
- **No auto-summary**
  Standard configuration type does not support auto summary feature. By default, the system disables the automatic network number summarization.



The ZebOS type requires no specific configuration for sending out BGP community and extended community attributes. ZebOS type is the default for the V5812G.

To select configuration type of the BGP router, use the following command.

Command	Mode	Description
bgp config-type {**standard** | **zebos**}	Global	Sets the BGP configuration type between standard and ZebOS.
no bgp config-type		Deletes the recent BGP configuration type and returns to default.

10.1.1.2 Enabling BGP Routing

Step 1 To define an AS number and open *Router Configuration* mode, use the following command.

Command	Mode	Description
router bgp <1-65535>	Global	Assigns AS number to configure BGP routing and opens *Router Configuration* mode. 1-65535: AS number

Step 2 To specify a network to operate with BGP, use the following command.

Command	Mode	Description
network *A.B.C.D/M*	Router	Adds BGP network to operate. A.B.C.D/M: network address with netmask A.B.C.D: network address NETMASK: subnet mask
network *A.B.C.D* **mask** *NETMASK*		

10.1.1.3 Disabling BGP Routing

Step 1 To delete a specified network to operate with BGP, use the following command.

Command	Mode	Description
no network *A.B.C.D/M*	Router	Deletes BGP network. A.B.C.D/M: network address with netmask A.B.C.D: network address NETMASK: subnet Mask
no network *A.B.C.D* **mask** *NETMASK*		

Step 2 Go back to *Global Configuration* mode using the **exit** command.

Step 3 To disable BGP routing of the chosen AS, use the following command.

Command	Mode	Description
no router bgp <1-65535>	Global	Deletes assigned AS number to configure BGP routing, enter the AS number. 1-65535: AS number

10.1.2 Advanced Configuration

The V5812G is possibly configured for the additional configurations related BGP.

10.1.2.1 Summary of Path

Aggregation combines the characteristics of several different routes and advertises a single route. In the example of 2 routes information of 172.16.0.0/24 and 172.16.1.0/24, the **as-set** parameter creates an aggregate entry advertising the path for a single route of 172.16.0.0/23, consisting of all elements contained in all paths being summarized. Use this feature to reduce the size of path information by listing the AS number only once, even if it was included in multiple paths that were aggregated. And it's useful when aggregation of information results in incomplete path information.

Using the **summary-only** parameter transmits the IP prefix only, suppressing the more-specific routes to all neighbors. Using the **as-set** parameter transmits a single AS path information only, one of AS numbers of each path.

To summarize route's information for the transmission, use the following command.

Command	Mode	Description
aggregate-address *A.B.C.D/M*	Router	Summarizes the information of routes and transmits it

as-set [**summary-only**]		to the other routers. A.B.C.D/M: network address summary-only: transmits IP prefix only. as-set: transmits one AS-path information.
aggregate-address *A.B.C.D/M* **summary-only** [**as-set**]		

To delete the route's information of specific network address, use the following command.

Command	Mode	Description
no aggregate-address *A.B.C.D/M* **as-set** [**summary-only**]	Router	Disables the summarization function of routes.
no aggregate-address *A.B.C.D/M* **summary-only** [**as-set**]		

10.1.2.2 Automatic Summarization of Path

Automatic summarization is new feature to expend the route information up to the class of specified IP address on interface connected directly to BGP router. For example, A class is fundamentally had "/8" as the subnet mask in case IP address assigned 100.1.1.1 in A class. It can generate route information of 100.0.0.0/8.

To enable/disable automatic summarization of the route, use the following command.

Command	Mode	Description
auto-summary	Router	Enables automatic network summarization of a route.
no auto-summary		Disables automatic network summarization of a route.



Please note that, use this feature when you use the basic classes in network.

10.1.2.3 BGP Next-Hop Address Tracking

BGP prefixes are automatically tracked as peering sessions are established. BGP next-hop address tracking feature significantly improves the response time of BGP to next-hop changes for routes installed in the RIB.

To enable/disable BGP next-hop address tracking, use the following command.

Command	Mode	Description
bgp nexthop trigger disable	Router	Enables BGP next-hop address tracking. (default)
bgp nexthop trigger enable		Disables BGP next-hop address tracking.

To set the delay interval between routing table walks for BGP next-hop address tracking, use the following command.

Command	Mode	Description
bgp nexthop trigger delay <2-30>	Router	Configures the delay interval between routing table walks for next-hop address tracking.
no bgp nexthop trigger delay		Deletes the configured delay interval.

10.1.2.4 Local Preference

The local preference indicates the preferred path when there are multiple paths to the same destination. The path having a higher preference is preferred.

To define preference of a particular path, use the following command.

Command	Mode	Description
bgp default local-preference <0-4294967295>	Router	Defines preference of a particular path and it is sent to all routers and access servers in the local AS. 0-4294967295: local preference value (default: 100)
no bgp default local-preference		Deletes the defined preference and reverts to the default setting.

10.1.2.5 Multi-Exit Discriminator (MED)

During the best-path selection process, the switch compares weight, local preference and as-path in turn among the similar parameters of BGP routers. Then, the MED is considered when selecting the best path among many alternative paths.

The V5812G, MED comparison is configured only among all paths from the autonomous system. You can configure the comparison of MEDs among all BGP routers within autonomous system. In addition, MED is used when comparing of routes from the neighboring routers placed within different AS.

To find the best route by comparing MED values, use the following command.

Command	Mode	Description
bgp always-compare-med	Router	Configures the router to consider the comparison of MEDs in choosing the best path from among paths.
no bgp always-compare-med		Chooses the best path regardless of the comparison of MEDs.

Meanwhile, when the best-path is selected among the neighbor routers within same Autonomous System, it doesn't compare MED values of them. However, in case the paths have same AS-path information, it does compare MED values. If there are two paths with different AS-path each other, the comparison of MED is unnecessary work. Other parameter's path information can be used to find the best path.

To compare MED values in order to choose the best path among lots of alternative paths included same AS-path value, use the following command.

Command	Mode	Description
bgp deterministic-med	Router	Configures the router to compare MEDs in choosing the best path when paths have same AS-path information.
no bgp deterministic-med		Configures the router not to compare MEDs even if the paths have same AS-path.

i During the best-path selection process, use the **bgp always-compare-med** command in case of comparing MED values regardless of AS-path. Otherwise, use the **bgp deterministic-med** command if it compares MED values of lots of paths contained same AS-path information.

10.1.2.6 Choosing Best Path

There are a lot of path parameters BGP protocol, which are IP address, AS, MED value and router ID. Even if two paths look same under the condition of IP address, they are actually different when other parameters are compared with each other.

To ignore AS-path for selecting the best path, use the following command.

Command	Mode	Description
bgp bestpath as-path ignore	Router	Ignores the information of AS-path as a factor in the algorithm for choosing the best route.
no bgp bestpath as-path ignore		Considers the information of AS-path as a factor in the algorithm for choosing the best route.

i If you would like to configure to select the best route by considering AS-path length of Confederation, you should configure the router first to ignore AS-path for choosing the best route using the **bgp bestpath as-path ignore** command before implementing the following command.

To consider AS-path length of Confederation during the best-path selection process, use the following command.

Command	Mode	Description
bgp bestpath compare-confed-aspath	Router	Considers the information of AS-path length of confederation as a factor in the algorithm for choosing the best route.
no bgp bestpath compare-confed-aspath		Ignores AS-path length of confederation as a factor in the algorithm for choosing the best route.

When comparing similar routes from more than 2 peers the BGP router does not consider router ID of the routes. It selects the first received route. The V5812G uses router ID in the selection process; similar routes are compared and the route with lowest router ID is selected as the best route. Router ID can be manually set by using the following command.

To select the best path by comparing router ID, use the following command. However, the default condition is that BGP receives routes with identical eBGP paths from eBGP peers.

Command	Mode	Description
bgp bestpath compare-routerid	Router	Selects the best path using the router ID for identical eBGP paths.
no bgp bestpath compare-routerid		Disables selecting the best path using the router ID.

The V5812G is basically configured not to compare MED values of the path information that exchanges between the Confederation Peers. But just in case, it can be configured to compare MED values of the path information that exchanges between Confederation Peers.

To compare MED values on the exchange of path information between Confederation Peers, use the following command.

Command	Mode	Description
bgp bestpath med confed [**missing-as-worst**]	Router	Configures the router to consider the MED in choosing a path from among the paths on the exchange of information between confederation peers.
bgp bestpath med missing-as-worst [**confed**]		

To ignore MED values of paths on the exchange of information between confederation peers, use the following command.

Command	Mode	Description
no bgp bestpath med confed [**missing-as-worst**]	Router	Ignores MEDs of paths on the exchange of their information between confederation peers.
no bgp bestpath med missing-as-worst [**confed**]		

If there are several equal paths, one of them has no MED value. Because this path is considered as “zero” without MED value, it will be chosen the best path. But the path would be the worst one if it has no MED value after **missing-as-worst** is set.

i After **missing-as-worst** parameter is configured in the system, the path will be recognized as the worst path without MED value.

10.1.2.7 Graceful Restart

Graceful restart allows a router undergoing a restart to inform its adjacent neighbors and peers of its condition. The restarting router requests a grace period from the neighbor or peer, which can then cooperate with the restarting router. With a graceful restart, the restarting router can still forward traffic during the restart period, and convergence in the network is not disrupted. The restart is not visible to the rest of the network, and the restarting router is not removed from the network topology.

The main benefits of graceful restart are uninterrupted packet forwarding and temporary suppression of all routing protocol updates. Graceful restart thus allows a router to exchange path information with the neighboring router.

To configure graceful restart specifically for BGP, use the following command.

Command	Mode	Description
bgp graceful-restart	Router	Sets to use graceful restart in BGP protocol.
no bgp graceful-restart		Disables the restart time value setting.

Therefore, 2 options of the time can be used to speed up routing convergence by its peer in case that BGP doesn't come back after a restart.

- **Restart Time**
  It's the waiting time for the restarting of Neighboring router's BGP process. Restart time allows BGP process time to restart and implement the internal connection (The session). However, if it's not working properly, it is considered as the router stops operating.
- **Stalepath Time**
  After BGP process of Neighboring router is restarted, it holds the time until BGP up dates the path information. In case that the information of BGP routes is not updated until the stalepath time, the switch discards this BGP routes information.

To set restart time or stalepath time on Graceful Restarting algorithm, use the following command.

Command	Mode	Description
bgp graceful-restart restart-time <1-3600>	Router	Sets the restart time of Graceful Restart configuration in the unit of second. 1-3600: restart time (default: 120)
bgp graceful-restart stalepath-time <1-3600>		Sets the stalepath-time of Graceful Restart configuration in the unit of second. 1-3600: stalepath time (default: 30)

If you don't use Graceful Restart feature or want to return the default value for restart time or stalepath time, use the following command.

Command	Mode	Description
no bgp graceful-restart restart-time [<1-3600>]	Router	Restores the default value for restart time.
no bgp graceful-restart stalepath-time [<1-3600>]		Restores the default value for stalepath time.

10.1.3 Administrative Distance for BGP

An administrative distance is a rating of the trustworthiness of a routing information source, such as an individual router or a group of routers. Numerically, an administrative distance is an integer between 1 and 255. In general, the higher the value is, the lower the trust rating is. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored.

To configure the administrative distance for BGP, use the following command.

Command	Mode	Description
distance <1-255> *A.B.C.D/M*	Router	Configures the administrative distance for BGP routes. 1-255: the administrative distance A.B.C.D/M: IP source prefix WORD: name of the access list
distance <1-255> *A.B.C.D/M WORD*		

distance bgp <1-255> <1-255> <1-255>		Specifies the administrative distance for BGP routes. 1-255: the administrative distance for BGP external routes (default: 20) 1-255: the administrative distance for BGP internal routes (default: 200) 1-255: the administrative distance for BGP local routes (default: 200)

To remove an administrative distance, use the following command.

Command	Mode	Description
no distance <1-255> *A.B.C.D/M*	Router	Removes the configured administrative distance.
no distance <1-255> *A.B.C.D/M WORD*		
no distance bgp		

10.1.4 IP Address Family

The V5812G recently supports both unicast and multicast as address-family. Use the following command in choosing either unicast or multicast to enter the *Address-Family Configuratio*n mode allowing configuration of address-family specific parameters.

Use the following command in order to enable address family routing process, which open you in *Address-Family Configuration* mode.

Command	Mode	Description
address-family ipv4 [**multicast** | **unicast**]	Router	Opens the *Address-Family Configuration* mode to configure sessions for IPv4 prefixes.
exit-address-family	Address-Family	Exits to *Router Configuration* mode.

10.1.5 BGP Neighbor

To assign IP address or peer group name for BGP Neighboring router within specified AS number, use the following command.

Command	Mode	Description
neighbor {*NEIGHBOR-IP* | *WORD*} **remote-as** <1-65535>	Router	Configures BGP neighboring router and specify AS number of BGP Neighbors. NEIGHBOR-IP: neighbor IP address WORD: peer group name or neighbor tag 1-65535: remote AS Number

10.1.5.1 Default Route

The V5812G can be configured that particular neighboring BGP routers or peer group is assigned by default route as 0.0.0.0. Then, neighboring router or member of peer group is able to receive the information of default route from the designated routers.

The following command allows neighboring BGP routers or Peer Group to transmit 0.0.0.0 as the default route.

To generate the default route to BGP neighbor or peer group, use the following command.

Command	Mode	Description
neighbor {*NEIGHBOR-IP* | *WORD*} **default-originate** [**route-map** *NAME*]	Router	Generates the default route to BGP Neighbor. NEIGHBOR-IP: neighbor IP address WORD: peer group name or neighbor tag 1-65535: remote AS number NAME: route map name
no neighbor {*NEIGHBOR-IP* | *WORD*} **default-originate** [**route-map** *NAME*]		Removes the default route for BGP Neighbor or peer group.

10.1.5.2 Peer Group

As the number of external BGP groups increases, the ability to support a large number of BGP sessions may become a scaling issue. In principle all members of BGP routers within a single AS must connect to other neighboring routers. The preferred way to configure a large number of BGP neighbors is to configure a few groups consisting of multiple neighbors per group. Supporting fewer BGP groups generally scales better than supporting a large number of BGP groups. This becomes more evident in the case of dozens of BGP neighboring groups when compared with a few BGP groups with multiple peers in each group. If the routers belong to same group, they can be applied by same configuration. This group is called as Peer Group.

After peer relationships have been established, the BGP peers exchange update message to advertise network reachability information. You can arrange BGP routers into groups of peers.

To create a BGP Peer Group, use the following command.

Command	Mode	Description
neighbor *NAME* **peer-group**	Router	Create a BGP peer group. NAME: peer group name
no neighbor *NAME* **peer-group**		Delete the BGP peer group created before.

To specify neighbor to the created peer group, use the following command.

Command	Mode	Description
neighbor *NEIGHBOR-IP* **peer-group** *NAME*	Router	Includes BGP neighbor to specified peer group using IP address. NEIGHBOR-IP: neighbor IP address NAME: peer group name
no neighbor *NEIGHBOR-IP* **peer-group** *NAME*		Removes BGP neighbor from the specified Peer Group.

10.1.5.3 Route Map

You can apply the specific route map on neighboring router that the exchange route information between routers or blocking the IP address range is configured on route map.

To make BGP Neighbor router exchange the routing information using Route-map, use the following command.

Command	Mode	Description
neighbor {*NEIGHBOR-IP* | *GROUP*} **route-map** *NAME* {**in** | **out**}	Router	Applies a route map to incoming or outgoing routes on neighboring router or peer group and exchange the route information. NEIGHBOR-IP: neighbor IP address GROUP: peer group name NAME: route map name
no neighbor {*NEIGHBOR-IP* | *GROUP*} **route-map** *NAME* {**in** | **out**}		Removes the connection with configured route-map.

10.1.5.4 Force Shutdown

The V5812G supports the feature to force to shutdown any active session for the specified BGP router or peer group and to delete the routing data between them. It shutdowns all connections and deletes the received path information from neighboring router or peer group.

To disable the exchange information with a specified router or peer group, use the following command.

Command	Mode	Description
neighbor {*NEIGHBOR-IP* | *WORD*} **shutdown**	Router	Shutdowns any active session for the specified router or peer group and delete all related routing data. NEIGHBOR-IP: neighbor IP address WORD: peer group name or neighbor tag
no neighbor {*NEIGHBOR-IP-ADDRESS* | *WORD*} **shutdown**		Enables the sessions with a previously existing neighbor or peer group that had been disabled.

10.1.5.5 Changing the Nexthop Information

When you use the command to change the nexthop information that is sent to the iBGP peer, the nexthop information is set the IP address of the interface used to communicate with the neighbor. To configure the router as the next hop for a BGP-speaking router or peer group, use the following command.

Command	Mode	Description
neighbor {*A.B.C.D* | *WORD*} **next-hop-self**	Router	Configures the router as the next hop for a BGP-speaking router or peer group. A.B.C.D: BGP neighbor IP address WORD: peer group name or neighbor tag
no neighbor {*A.B.C.D* | *WORD*} **next-hop-self**		Deletes the configured router as the next hop for a BGP-speaking router or peer group.

10.1.5.6 Neighbor Password

To enable/disable MD5 authentication on a TCP connection between BGP neighbors, use the following command.

Command	Mode	Description
neighbor {*A.B.C.D* | *WORD*} **password** *PASSWORD*	Router	Sets password to the neighbor. A.B.C.D: BGP neighbor IP address WORD: neighbor tag PASSWORD: password 0-7: encryption type LINE: alphanumeric string of characters
neighbor {*A.B.C.D* | *WORD*} **password** <0-7> *PASSWORD*		
no neighbor {*A.B.C.D* | *WORD*} **password** [*PASSWORD*]		Deletes a configured password.
no neighbor {*A.B.C.D* | *WORD*} **password** <0-7> *PASSWORD*		

10.1.5.7 Neighbor Description

A specific neighbor's description is useful for an ISP that has multiple neighbor relationships. To associate a description with a neighbor, use the following command.

Command	Mode	Description
neighbor {*A.B.C.D* | *WORD*} **description** *LINE*	Router	Specifies a description on a neighbor. A.B.C.D: BGP neighbor IP address WORD: neighbor tag LINE: 80-character text that describes the neighbor
no neighbor {*A.B.C.D* | *WORD*} **description** [*LINE*]		Deletes a specified description.

10.1.5.8 Source of Routing Updates

The loopback interface is that is most commonly used with the following command. The use of loopback interface eliminates a dependency and BGP doest not have to rely on the availability of a particular interface for making TCP connection. It is used in conjunction with any specified interface on the router

To allow internal BGP sessions to use any operation interface for TCP connection, use the following command.

Command	Mode	Description
neighbor {*A.B.C.D* | *WORD*} **update-source** *INTERFACE*	Router	Allows internal BGP sessions to use any operation interface for TCP connections. A.B.C.D: BGP neighbor IP address WORD: neighbor tag INTERFACE: loopback interface name or IP address
no neighbor {*A.B.C.D* | *WORD*} **update-source**		Restores the interface assignment to the closest interface.

10.1.5.9 Updates for Inbound Soft Reconfiguration

Soft-reconfiguration may be used in lieu of BGP route refresh capability. The V5812G can store updates for inbound soft reconfiguration. When a soft reset (inbound) is done on this neighbor, the locally stored routes are reprocessed according to the inbound policy.

To enable/disable local storage of all the received routes and their attributes, use the following command.

Command	Mode	Description
neighbor {*A.B.C.D* | *WORD*} **soft-reconfiguration inbound**	Router	Enables the local storage of updates. A.B.C.D: BGP neighbor IP address WORD: neighbor tag
no neighbor {*A.B.C.D* | *WORD*} **soft-reconfiguration inbound**		Disables the local storage of updates.

10.1.6 BGP Timers

BGP keepalive timer indicates that the frequency with which the keepalive messages are sent to the neighbors. And holdtime is the interval which the neighbor is considered dead if keepalive messages are not received.

To set the BGP keepalive and holdtime timer values for all the neighbors, use the following command.

Command	Mode	Description
timers bgp <0-65535> <0-65535>	Router	Configures the period of finding in the unit of second. 0-65535: keepalive timer value (default: 60 seconds) 0-65535: holdtime value (default: 180 seconds)

To reset the values, use the following command.

Command	Mode	Description
no timers bgp	Router	Resets timers to default value.

10.1.7 Route Flap Dampening

The route dampening minimizes the instability caused by route flapping. A penalty is added for every flap in a flapping route. As soon as the total penalty reaches the “suppress” limit the advertisement of the route is suppressed. This penalty is decayed according to the configured “half time” value. Once the penalty is lower than the “reuse” limit, the route advertisement is un-suppressed.

To enable the route-flap dampening, use the following command.

Command	Mode	Description
bgp dampening	Router	Enables the route-flap dampening.

To configure BGP dampening parameters, use the following command.

Command	Mode	Description
bgp dampening <1-45>	Router	Configures BGP dampening parameters. 1-45: reachability half-life time in minute (default: 15 minutes) 1-20000: reuse limit value (default: 750) 1-20000: suppress limit value (default: 2000) 1-255: max-suppress-time (default: 60 minutes) 1-45: un-reachability half-life time for penalty
bgp dampening <1-45> <1-20000> <1-20000> <1-255>		
bgp dampening <1-45> <1-20000> <1-20000> <1-255> <1-45>		
bgp dampening route-map *WORD*		Specifies the route-map criteria for dampening. WORD: route-map name

i When the penalty for a suppressed route decays below the “reuse value”, the routes become unsuppressed. When the penalty for a route exceeds the “suppress value”, the route is suppressed.

i The “reachability half-life time” is for the penalty to decrease to one-half of its current value. The “max-suppress-time is the maximum time that a dampened route is suppressed. This value is 4 times the half-life time.

To delete the configured BGP dampening parameters, use the following command.

Command	Mode	Description
no bgp dampening	Router	Deletes the configured BGP dampening parameter.

To display detailed information about dampening, use the following command.

Command	Mode	Description
show ip bgp dampening dampened-paths	Enable Global Bridge	Shows paths suppressed due to dampening.
show ip bgp dampening flap-statistics		Shows flap statistics of routes.
show ip bgp dampening parameters		Shows details of configured dampening parameters.

To reset all dampened BGP routes, use the following command.

Command	Mode	Description
clear ip bgp dampening	Enable Global Bridge	Resets all dampened BGP routes.
clear ip bgp dampening {*A.B.C.D* | *A.B.C.D/M*}		

To clear the flap count and history duration for all the prefixes under the specified address family, use the following command.

Command	Mode	Description
clear ip bgp flap-statistics	Enable Global Bridge	Clears the collected BGP flap statistics.
clear ip bgp flap-statistics {*A.B.C.D* | *A.B.C.D/M*}		

10.1.8 BGP Session Reset

When you manage BGP network, you can use the command to reset the session for all peers occasionally. Because the internal connections are re-established newly after resetting, the route information of the connected routers is restored by default.

You can reset the session in specified condition. The V5812G is available with several parameters to reset the BGP connections.

10.1.8.1 Session Reset of All Peers

To reset the sessions with all BGP peers, use the following command.

Command	Mode	Description
clear ip bgp *	Global	Resets all sessions with BGP peer groups.

When the route parameters restore to the default value by reset command, you can configure the specific parameters for its initialization. If you would like to reset/clear the outgoing advertised routes only, you should use **out** parameter. Otherwise, if you'd like to reset/clear the incoming advertised routes only, you should use **in** parameter.

Meanwhile, if **prefix-filter** is configured with **in** option, ORF (Outbound Route Filtering) and incoming route can be reset. By using **soft** option, you can configure the switch to update route information only when the session is still connected.

To reset the sessions of all peers and initialize the details of route configurations, use the following command.

Command	Mode	Description
clear ip bgp * in [**prefix-filter**]	Global	Resets the session of specific group under * condition. in: clears incoming advertised routes. prefix-filter: pushes out prefix-list ORF and does inbound soft reconfiguration. *: the conditional option (peer group name or AS number or IP address)
clear ip bgp * {**unicast** | **multicast**}**in** [**prefix-filter**]		
clear ip bgp out		Resets the session of specific group under * condition. *: the conditional option (peer group name or AS number or IP address) out: clears outgoing advertised routes. unicast | multicast: address family modifier
clear ip bgp * {**unicast** | **multicast**} **out**		
clear ip bgp * soft [**in** | **out**]		Updates the route information only while the session is possible for specific group under * condition. Apply the route either incoming or outgoing routes. *: the conditional option (peer group name or AS number or IP address)
clear ip bgp * {**unicast** | **multicast**} **soft** [**in** | **out**]		

10.1.8.2 Session Reset of Peers within Particular AS

To reset the session with all neighbor router which are connected to a particular AC, use the following command.

Command	Mode	Description
clear ip bgp <1-65535>	Global	Resets the session with all members of neighbor routers which are configured a particular AC number.

i See Section 10.1.8.1 when you configure the detail parameters.

To reset the sessions of BGP neighboring routers which are belong to specific AS number and initialize the details of route configurations, use the following command.

Command	Mode	Description
clear ip bgp <1-65535> **in** [**prefix-filter**]	Global	Resets the session of BGP neighboring routers which are configured a particular AC number. in: clears incoming advertised routes. prefix-filter: pushes out prefix-list ORF and does inbound soft reconfiguration. 1-65535: AS number
clear ip bgp <1-65535> {**unicast** | **multicast**} **in** [**prefix-filter**]		
clear ip bgp <1-65535> **out**		Resets the session of BGP neighboring routers which are configured a particular AC number. 1-65535: AS number out: clears outgoing advertised routes. unicast | multicast: address family modifier
clear ip bgp <1-65535> {**unicast** | **multicast**} **out**		

Command	Mode	Description
clear ip bgp <1-65535> **soft** [**in** | **out**]	Global	Updates the route information only while the session is possible of BGP neighboring routers which are configured a particular AC number. Apply the route either incoming or outgoing routes. 1-65535: AS number
clear ip bgp <1-65535> {**unicast** | **multicast**} **soft** [**in** | **out**]		

10.1.8.3 Session Reset of Specific Route

To reset the sessions of BGP neighboring router with specified IP address, use the following command.

Command	Mode	Description
clear ip bgp *ROUTE-IP-ADDRESS*	Global	Resets the sessions of BGP neighboring router with specified IP address.



See Section 10.1.8.1 when you configure the detail parameters.

To reset the sessions of BGP neighboring router with specified IP address and initialize the details of route configurations, use the following command.

Command	Mode	Description
clear ip bgp *A.B.C.D* **in** [**prefix-filter**]	Global	Resets the session of BGP neighboring router contained specified IP address. in: clears incoming advertised routes. prefix-filter: pushes out prefix-list ORF and does inbound soft reconfiguration. A.B.C.D: route IP address
clear ip bgp *A.B.C.D* {**unicast** | **multicast**} **in** [**prefix-filter**]		
clear ip bgp *A.B.C.D* **out**		Resets the session of BGP neighboring router with specified IP address. A.B.C.D: route IP address out: clears outgoing advertised routes. unicast | multicast: address family modifier
clear ip bgp *A.B.C.D* {**unicast** | **multicast**} **out**		
clear ip bgp *A.B.C.D* **soft** [**in** | **out**]		Updates the route information only while the session is possible of BGP neighboring router with specified IP address. Apply the route either incoming or outgoing routes. A.B.C.D: route IP address
clear ip bgp *A.B.C.D* {**unicast** | **multicast**} **soft** [**in** | **out**]		

10.1.8.4 Session Reset of External Peer

You can reset the session of BGP router connected to external AS. To reset a BGP connection for all external peers, use the following command.

Command	Mode	Description
clear ip bgp external	Global	Resets the session of all external AS peers.

i See Section 10.1.8.1 when you configure the detail parameters.

To reset the sessions of BGP router connected to external AS and initialize the details of route configurations, use the following command.

Command	Mode	Description
clear ip bgp external in [**prefix-filter**]	Global	Resets the session of BGP router connected to external AS. in: clears incoming advertised routes. prefix-filter: pushes out prefix-list ORF and does inbound soft reconfiguration. external: clears all external peers.
clear ip bgp external {**unicast** | **multicast**} **in** [**prefix-filter**]		
clear ip bgp external out		Resets the session of BGP router connected to external AS. external: clears all external peers. out: clears outgoing advertised routes. unicast | multicast : address family modifier
clear ip bgp external {**unicast** | **multicast**} **out**		
clear ip bgp external soft [**in** | **out**]		Updates the route information only while the session is possible of BGP router connected to external AS. Apply the route either incoming or outgoing routes. external: clears all external peers.
clear ip bgp external {**unicast** | **multicast**} **soft** [**in** | **out**]		

10.1.8.5 Session Reset of Peer Group

To reset the session for all members of a peer group, use the following command.

Command	Mode	Description
clear ip bgp peer-group *GROUP*	Global	To reset the session for all configured routers of specified peer group. GROUP: peer group name

i See Section 10.1.8.1 when you configure the detail parameters.

To reset the sessions of BGP routers which are members of specified peer group and initialize the details of route configurations, use the following command.

Command	Mode	Description
clear ip bgp peer-group *GROUP* **in** [**prefix-filter**]	Global	Resets the session for all members of specified peer group. in: clears incoming advertised routes. prefix-filter: pushes out prefix-list ORF and does inbound soft reconfiguration. GROUP: peer group name
clear ip bgp peer-group *GROUP* {**unicast** | **multicast**} **in** [**prefix-filter**]		
clear ip bgp peer-group *GROUP* **out**		Resets the session for all members of specified peer group. GROUP: peer group name out: clears outgoing advertised routes. unicast | multicast: address family modifier
clear ip bgp peer-group *GROUP* {**unicast** | **multicast**} **out**		

clear ip bgp peer-group *GROUP* **soft** [**in** | **out**]		Resets the route information only while the session is possible for all members of specified peer group. Apply the route either incoming or outgoing routes. GROUP: peer group name
clear ip bgp peer-group *GROUP* {**unicast** | **multicast**} **soft** [**in** | **out**]		

10.1.9 Displaying and Managing BGP

BGP network information or configurations provided can be used to determine resource utilization and enable BGP troubleshooting functions to solve network problems.

To see the configurations involved in BGP routing protocol, use the following command.

Command	Mode	Description
show ip bgp summary	Enable Global	Shows the summarized network status of BGP neighboring routers.
show ip bgp [**ipv4** {**unicast** | **multicast**}] **summary**		

10.1.9.1 BGP Neighbor

To show detailed information on BGP neighbor router's session, use the following command.

Command	Mode	Description
show ip bgp neighbors	Enable Global Bridge	Shows general information on BGP neighbor connections of all neighboring routers.
show ip bgp {**unicast** | **multicast**} **neighbors**		
show ip bgp neighbors *NEIGHBOR-IP*		Shows information of a specified neighbor router by its IP address. NEIGHBOR-IP: neighbor router' s IP address
show ip bgp {**unicast** | **multicast**} **neighbors** *NEIGHBOR-IP*		
show ip bgp neighbors *NEIGHBOR-IP* **advertised-routes**		The **advertised-routes** option displays all the routes the router has advertised to the neighbor.
show ip bgp ipv4 {**unicast** | **multicast**} **neighbors** *NEIGHBOR-IP* **advertised-routes**		
show ip bgp neighbors *NEIGHBOR-IP* **received prefix-filter**		Displays all received routes from neighbor router, both accepted and rejected.
show ip bgp ipv4 {**unicast** | **multicast**} **neighbors** *NEIGHBOR-IP* **received prefix-filter**		
show ip bgp neighbors *NEIGHBOR-IP* **received-routes**		The **received-routes** option displays all received routes (both accepted and rejected) from the specified neighbor. To implement this feature, BGP soft reconfiguration is set.
show ip bgp ipv4 {**unicast** | **multicast**} **neighbors** *NEIGHBOR-IP* **received-routes**		
show ip bgp neighbors *NEIGHBOR-IP* **routes**		The **routes** option displays the available routes only that are received and accepted.
show ip bgp ipv4 {**unicast** | **multicast**} **neighbors** *NEIGHBOR-IP* **routes**		

10.1.9.2 Logging Neighbor Changes

To enable/disable logging of status change messages without turning on BGP debugging, use the following command.

Command	Mode	Description
bgp log-neighbor-changes	Router	Enables logging of BGP neighbor status changes
no bgp log-neighbor-changes		Disables logging of BGP neighbor status changes

The V5812G logs the following events using the above command.

- BGP notification received
- Erroneous BGP update received
- User reset request
- Peer time-out / Peer closing down the session / Member added to peer group
- Interface flap
- Router ID changed
- Neighbor deleted
- Remote AS changed
- Administrative shutdown

10.1.9.3 Checking the BGP Network Route

To check that the BGP network route is reachable through IGP, use the following command.

Command	Mode	Description
bgp network import-check	Router	Checks BGP network route exists in IGP.
no bgp network import-check		Disables the function.

10.1.9.4 Sending SNMP Trap

To enable/disable the system to send SNMP trap message of BGP routing information, use the following command.

Command	Mode	Description
bgp snmp-notification enable	Router	Configures the system to send SNMP trap of routing information while BGP is running.
bgp snmp-notification disable		Disables the system to send SNMP trap of routing information while BGP is running.

10.1.10 BGP Debug

To enable BGP debugging, use the following command.

Command	Mode	Description
debug bgp	Enable Global	Enables BGP debugging.
debug bgp { **all** | **dampening** | **events** | **filters** | **fsm** | **keepalives** | **nsm** | **updates** [**in** | **out**] }		Enables BGP debugging. all: all BGP debugging dampening: BGP dampening debugging events: events debugging filters: BGP filters debugging fsm: BGP finite state machine debugging keepalives: BGP deepalives debugging nsm: NSM message debugging updates in/out: inbound/outbound updates debugging

To disable BGP debugging, use the following command.

Command	Mode	Description
no debug bgp	Enable Global	Disables BGP debugging.
no debug bgp { **all** | **dampening** | **events** | **filters** | **fsm** | **keepalives** | **nsm** | **updates** }		

To display the debugging information, use the following command.

Command	Mode	Description
show debugging bgp	Enable Global Bridge	Shows the debugging information of BGP.

10.2 Open Shortest Path First (OSPF)

Open shortest path first (OSPF) is an interior gateway protocol developed by the OSPF working group of Internet Engineering Task Force (IETF). OSPF designed for IP network supports IP subnetting and marks on information from exterior network. Moreover, it supports packet authorization and transmits/receives routing information through IP multicast. It is most convenient to operate OSPF on layered network.

OSPF is the most compatible routing protocol in layer network environment. The first setting in OSPF network is planning network organized with router and configures border router faced with multiple section.

After that, sets up the basic configuration for OSPF router operation and assigns interface to Area. To make compatible OSPF router configuration for user environment, each router configuration must be accorded by verification.

This section provides configurations for OSPF routing protocol. Lists are as follows.

- Enabling OSPF
- ABR Type Configuration
- Compatibility Support
- OSPF Interface
- Non-Broadcast Network
- OSPF Area
- Default Metric
- Graceful Restart Support
- Opaque-LSA Support
- Default Route
- Finding Period
- External Routes to OSPF Network
- OSPF Distance
- Host Route
- Passive Interface
- Blocking Routing Information
- Summary Routing Information
- OSPF Monitoring and Management

10.2.1 Enabling OSPF

To use OSPF routing protocol, it must be activated as other routing protocols. After activation, configures network address and ID which is operated by OSPF.

The following command shows steps of activating OSPF.

Step1

Open *Router Configuration* mode from *Global Configuration* mode.

Command	Mode	Description
router ospf [<1-65535>]	Global	Opens *Router Configuration* mode with enabling OSPF.
no router ospf [<1-65535>]		Disables OSPF routing protocol.

In case that more than 2 OSPF processes are operated, a process number should be assigned. Normally, there is one OSPF which is operating in one router.

If OSPF routing protocol is disabled, all related configuration will be lost.

Step2

Configure a network ID of OSPF. Network ID decides IP v4 address of this network.

Command	Mode	Description
router-id *A.B.C.D*	Router	Assigns a router ID with enabling OSPF.
no router-id *A.B.C.D*		Deletes a configured router ID.

In case if using **router-id** command to apply new router ID on OSPF process, OSPF process must be restarted to apply. Use the **clear ip ospf process** command to restart OSPF process.

If there is changing router ID while OSPF process is operating, configuration must be processed from the first. In this case, the V5812G can change only router ID without changing related configurations.

Command	Mode	Description
ospf router-id *A.B.C.D*	Router	Changes only a router ID without changing related configurations.
no ospf router-id *A.B.C.D*		Deletes a changed router ID.

To transfer above configuration to other routers, Use the **clear ip ospf process** command to restart OSPF process.

Step 3

Use the **network** command to specify a network to operate with OSPF.

There are two ways to show network information configurations. Firstly, shows IP address with bitmask like “10.0.0.0/8”. Secondly, shows IP address with wildcard bit information like “10.0.0.0 0.0.0.255”. The variable option after **area** must be IP address or OSPF area ID.

To configure a network, use the following command.

Command	Mode	Description
network *A.B.C.D/M* **area** {<0-4294967295> | *A.B.C.D*}	Router	Specifies a network with OSPF area ID. 0-4294967295: OSPF area ID
network *A.B.C.D A.B.C.D* **area** {<0-4294967295> | *A.B.C.D*}		

10.2.2 ABR Type Configuration

The V5812G supports 4 types of OSPF ABR which are Cisco type ABR (RFC 3509), IBM type ABR (RFC 3509), IETF Draft type and RFC 2328 type.

To configure ABR type of OSPF, use the following command.

Command	Mode	Description
ospf abr-type {**cisco** | **ibm** | **shortcut** | **standard**}	Router	Selects an ABR type. cisco: cisco type ABR, RFC 3509 (default) ibm: IBM type ABR, RFC 3509 shortcut: IETF draft type standard: RFC 2328 type
no ospf abr-type {**cisco** | **ibm** | **shortcut** | **standard**}		Deletes a configured ABR type.

10.2.3 Compatibility Support

OSPF protocol in the V5812G uses RFC 2328 which is finding shorten path. However, Compatibility configuration enables the switch to be compatible with a variety of RFCs that deal with OSPF. Perform the following task to support many different features within the OSPF protocol.

Use the following command to configure compatibility with RFC 1583.

Command	Mode	Description
compatible rfc1583	Router	Supports compatibility with RFC 1583.
no compatible rfc1583		Disables configured compatibility.

10.2.4 OSPF Interface

OSPF configuration can be changed. Users are not required to alter all of these parameters, but some interface parameters must be consistent across all routers in an attached network.

10.2.4.1 Authentication Type

Authentication encodes communications among the routers. This function is for security of information in OSPF router.

To configure authentication of OSPF router for security, use the following command.

Command	Mode	Description
ip ospf authentication [**message-digest** | **null**]	Interface	Enables authentication on OSPF interface. message-digest: MD5 encoding null: no encoding A.B.C.D: IP address for authentication
ip ospf *A.B.C.D* **authentication** [**message-digest** | **null**]		

If there is no choice of authentication type, the code communication will be based on text.

To delete comfigured authentication, use the following command.

Command	Mode	Description
no ip ospf authentication	Interface	Deletes configured authentication.
no ip ospf *A.B.C.D* **authentication**		

10.2.4.2 Authentication Key

If authentication enables on OSPF router interface, the password is needed for authentication. The authentication key works as a password. The authentication key must be consistent across all routers in an attached network.

There are two ways of authentication by user selection, one is type based on text, and another is MD5 type.

The authentication key must be consistent across all routers in an attached network.

To configure an authentication key which is based on text encoding, use the following command.

Command	Mode	Description
ip ospf authentication-key *KEY*	Interface	Configures the authentication which is based on text encoding. KEY: maximum 16 alphanumeric characters
ip ospf authentication-key *KEY* {**first** | **second**} [**active**]		
ip ospf *A.B.C.D* **authentication-key** *KEY*		
ip ospf *A.B.C.D* **authentication-key** *KEY* {**first** | **second**} [**active**]		

To configure an authentication key which is based on MD5 encoding, use the following command.

Command	Mode	Description
ip ospf message-digest-key <1-255> **md5** *KEY* [**active**]	Interface	Configures the authentication which is based on md5 type. 1-255: key ID KEY: maximum 16 alphanumeric characters
ip ospf message-digest-key <1-255> **md5** [**active**]		
ip ospf *A.B.C.D* **message-digest-key** <1-255> **md5** *KEY* [**active**]		
ip ospf *A.B.C.D* **message-digest-key** <1-255> **md5** [**active**]		

To delete a configured authentication key, use the following command.

Command	Mode	Description
no ip ospf authentication-key	Interface	Deletes a configured authentication key.
no ip ospf authentication-key {**first** | **second**}		
no ip ospf *A.B.C.D* **authentication-key**		
no ip ospf *A.B.C.D* **authentication-key** {**first** | **second**}		
no ip ospf message-digest-key <1-255>		
no ip ospf *A.B.C.D* **message-digest-key** <1-255>		

10.2.4.3 Interface Cost

OSPF protocol assigns suitable cost according to the bandwidth on the each interface to find the shortest route. Cost is used for packet routing, and routers are using the Cost to communicate.

To configure an interface cost for OSPF, use the following command.

Command	Mode	Description
ip ospf cost <1-65535>	Interface	Configures an interface cost for OSPF.
ip ospf *A.B.C.D* **cost** <1-65535>		

To delete a configured interface cost for OSPF, use the following command.

Command	Mode	Description
no ip ospf cost	Interface	Deletes a configured an interface cost for OSPF.
no ip ospf *A.B.C.D* **cost**		

10.2.4.4 Blocking Transmission of Route Information Database

OSPF routing communicates through the LAS. Each routing information is saved internal router as a datebase, but user can configure the specific interface to block the transmission of routing information saved in database to other router.

To block the transmission of routing information to other router, use the following command.

Command	Mode	Description
ip ospf database-filter all out	Interface	Blocks the transmission of routing information to other router.
ip ospf *A.B.C.D* **database-filter all out**		

To release a blocked interface, use the following command.

Command	Mode	Description
no ip ospf database-filter	Interface	Releases a blocked interface.
no ip ospf *A.B.C.D* **database-filter**		

10.2.4.5 Routing Protocol Interval

Routers on OSPF network exchange various packets, about that packet transmission, time interval can be configured in several ways

The following lists are sort of time interval which can be configured by user:

- **Hello Interval**
  OSPF router sends Hello packet to notify existence of itself. Hello interval is that packet transmission interval.
- **Retransmit Interval**
  When router transmits LSA, it is waiting for approval information come from receiver. In this time, if there is no answer from receiver for configured time, the router transmits LSA again. Retransmit-interval is configuration of the time interval between transmission and retransmission.
- **Dead Interval**
  If there is no hello packet for the configured time. The router perceives other router is stopped working. Dead interval is configuration of the time interval which perceives other router is stopped operating.
- **Transmit Delay**
  When a router transmits LSA, the traffic can be delayed by status of communications. Transmit delay is considering of the configuration for LSA transmission time.

i The interval explained as above must be consistent across all routers in an attached network.

To configure a Hello interval, use the following command.

Command	Mode	Description
ip ospf hello-interval <1-65535>	Interface	Configures a Hello interval in the unit of second. 1-65535: interval value (default: 10)
ip ospf *A.B.C.D* **hello-interval** <1-65535>		
no ip ospf hello-interval		Sets a Hello interval to the default value.
no ip ospf *A.B.C.D* **hello-interval**		

To configure a retransmit interval, use the following command.

Command	Mode	Description
ip ospf retransmit-interval <1-65535>	Interface	Configures a retransmit interval in the unit of second. 1-65535: interval value (default: 5)
ip ospf *A.B.C.D* **retransmit-interval** <1-65535>		
no ip ospf retransmit-interval		Sets a retransmit interval to the default value.
no ip ospf *A.B.C.D* **retransmit-interval**		

To configure a dead interval, use the following command.

Command	Mode	Description
ip ospf dead-interval <1-65535>	Interface	Configures a dead interval in the unit of second. 1-65535: interval value (default: 40)
ip ospf *A.B.C.D* **dead-interval** <1-65535>		
no ip ospf dead-interval		Sets a dead interval to the default value.
no ip ospf *A.B.C.D* **dead-interval**		

To configure a transmit delay, use the following command.

Command	Mode	Description
ip ospf transmit-delay <1-65535>	Interface	Configures a transmit delay in the unit of second. 1-65535: interval value (default: 1)
ip ospf *A.B.C.D* **transmit-delay** <1-65535>		
no ip ospf transmit-delay		Sets a transmit delay to the default value.
no ip ospf *A.B.C.D* **transmit-delay**		

10.2.4.6 OSPF Maximum Transmission Unit (MTU)

Router verifies MTU when DD (Database Description) is exchanging among the routers on OSPF networks. Basically, OSPF network can not be organized if there are different sizes of MTUs between routers. Therefore MTU value must be consistent. Generally MTU value is 1500 bytes on Ethernet interface.

To configure MTU on OSPF interface, use the following command.

Command	Mode	Description
ip ospf mtu <576-65535>	Interface	Configures an MTU on OSPF interface.
no ip ospf mtu		Deletes a configured MTU on OSPF interface.

i Configuration as above makes MTU consistently on same OSPF network; actual MTU value on interface itself will not be changed.

On the other hands, if there are two routers which have different MTU, it can be participated with OSPF network through the configuration that skips the verification of MTU value when there is DD exchanging.

To configure the switch to skip the MTU verification in DD process, use the following command.

Command	Mode	Description
ip ospf mtu-ignore	Interface	Configures the switch to skip the MTU verification in DD process.
ip ospf *A.B.C.D* **mtu-ignore**		

To configure the switch not to skip the MTU verification in DD process, use the following command.

Command	Mode	Description
no ip ospf mtu-ignore	Interface	Configures the switch not to skip the MTU verification in DD process.
no ip ospf *A.B.C.D* **mtu-ignore**		

10.2.4.7 OSPF Priority

Routers have each role to exchange the information on OSPF network. DR (Designated Router) is one of essential role to get and transmit the route information in the same area.

The router having the highest priority becomes DR (Designated Router). If there are routers which have same priority, the highest router ID will be DR.

Normally, router has priority 1, but it can be changed to make DR through the configuration of priority.

To configure a priority of OSPF router, use the following command.

Command	Mode	Description
ip ospf priority <0-255>	Interface	Configures a priority of OSPF router.
ip ospf *A.B.C.D* **priority** <0-255>		

To delete a configured priority of OSPF router, use the following command.

Command	Mode	Description
no ip ospf priority	Interface	Deletes a configured priority of OSPF router.
no ip ospf *A.B.C.D* **priority**		

10.2.4.8 OSPF Network Type

There are 4 types of OSPF network. Broadcast network, NBMA (Non-broadcast-multiple-access) network, Point-to-multipoint network and Point-to-point network.

User can configure OSPF network as a Broadcast network or Non-broadcast network type. For example, if the network does not support multicasing it can be configured Non-broadcast type from Broadcast type, and NBMA network as a Frame relay can be

broadcast network type.

NBMA type network need virtual circuit to connect routers. But Point-to-multipoint type uses virtual circuit on part of network to save the management expenses. It does not to need to configure Neighbor router to connect routers which are not directly connected. It also saves IP resources and no need to configure the process for destination router. It supports those benefits for stable network services.

Generally, the routers and Layer 3 switches are using Broadcast type network.

To select an OSPF network type, use the following command.

Command	Mode	Description
ip ospf network {**broadcast** | **non-broadcast** | **point-to-multipoint** [**non-broadcast**] | **point-to-point**}	Interface	Selects an OSPF network type.

10.2.5 Non-Broadcast Network

To operate NBMA type network, neighbor router configuration is needed. And IP address, Priority, Poll-interval configuration as well. Priority is information for designate router selection and it configured [0] as a default. Poll-interval is the waiting time to re-get the hello packet from dead Neighbor router. It configured 120 seconds as a default.

To configure a router communicated by non-broadcast type, use the following command.

Command	Mode	Description
neighbor *A.B.C.D* [**cost** <1-65535>]	Router	Configures a neighbor router of NBMA type.
neighbor *A.B.C.D* **priority** <0-255>		
neighbor *A.B.C.D* **priority** <0-255> **poll-interval** <1-65535>		
neighbor *A.B.C.D* **poll-interval** <1-65535>		
neighbor *A.B.C.D* **poll-interval** <1-65535> **priority** <0-255>		

To delete a configured router communicated by non-broadcast type, use the following command.

Command	Mode	Description
no neighbor *A.B.C.D*	Router	Deletes a configured neighbor router of NBMA type.
no neighbor *A.B.C.D* **cost** [<1-65535>]		
no neighbor *A.B.C.D* **priority** [<0-255>]		
no neighbor *A.B.C.D* **priority poll-interval** [<1-65535>]		
no neighbor *A.B.C.D* **poll-interval** [<1-65535>]		
no neighbor *A.B.C.D* **poll-interval priority** [<0-255>]		

10.2.6 OSPF Area

Router configuration on OSPF network includes Area configuration with each interface, network. Area has various and special features. It needs to be configured pertinently to make effective management on whole of OSPF network.

OSPF network defines several router types to manage the Area. ABR (Area Border Router) is one of the router types to transmit information between Areas.

ASBR (Autonomous System Border Router) is using OSPF on oneside and using other routing protocol except for OSPF on other interface or Area. ASBR exchanges area information between different routing protocols.

Area types are various. The most principle Area types are Stub Area and NSSA (Not So Stubby Area).

10.2.6.1 Area Authentication

OSPF routers in specific Area can configure authentication for security of routing information. Encoding uses password based on text or MD5. To set password on interface assigned Area, use the **ip ospf authentication-key** and **ip ospf message-digest-key** commands in interface mode, see Section 10.2.4.1 for more information.

To configure authentication information for encoding, use the following command.

Command	Mode	Description
area {<0-4294967295> | *A.B.C.D*} **authentication**	Router	Configures authentication information which is based on text encoding in the Area.
area {<0-4294967295> | *A.B.C.D*} **authentication message-digest**		Configures authentication information which is based on MD5 encoding in the Area.

To delete configured authentication information for encoding, use the following command.

Command	Mode	Description
no area {<0-4294967295> | *A.B.C.D*} **authentication**	Router	Deletes configured authentication information.

10.2.6.2 Default Cost of Area

The default cost of Area is configured only in ABR. ABR function is for delivering the summary default route to stub area or NSSA, in that cases the default cost of area must be required. However, ABR which does not have stub area or NSSA can not use the following command.

To configure a default cost of Area, use the following command.

Command	Mode	Description
area {<0-4294967295> | *A.B.C.D*} **default-cost** <1-16777215>	Router	Configures a default cost of Area.

To delete a configured default cost of Area, use the following command.

Command	Mode	Description
area {<0-4294967295> | *A.B.C.D*} **default-cost** <1-16777215>	Router	Deletes a configured default cost of Area.



This command is only for ABR which is delivering summary default route to stub or NSSA.

10.2.6.3 Blocking the Transmission of Routing Information Between Area

ABR transmits routing information between Areas. In case of not to transmit router information to other area, the V5812G can configure it as a blocking.

First of all, use the **access-list** or **prefix-list** command to assign LIST-NAME. And use the following command to block the routing information on LIST-NAME. This configuration only available in case of OSPF router is ABR.

To block routing information on LIST-NAME, use the following command.

Command	Mode	Description
area {<0-4294967295> | *A.B.C.D*} **filter-list access** *LIST-NAME* {**in** | **out**}	Router	Blocks routing information on LIST-NAME.
area {<0-4294967295> | *A.B.C.D*} **filter-list prefix** *LIST-NAME* {**in** | **out**}		

To delete configured blocking information, use the following command.

Command	Mode	Description
no area {<0-4294967295> | *A.B.C.D*} **filter-list access** *LIST-NAME* {**in** | **out**}	Router	Deletes configured blocking information.
no area {<0-4294967295> | *A.B.C.D*} **filter-list prefix** *LIST-NAME* {**in** | **out**}		



This command is only available for ABR.

10.2.6.4 Not So Stubby Area (NSSA)

NSSA (Not So Stubby Area) is stub Area which can transmit the routing information to Area by ASBR. On the other hand, Stub Area cannot transmit the routing information to area. To configure NSSA, use the following command.

Command	Mode	Description
area {<0-4294967295> | *A.B.C.D*} **nssa**	Router	Configures NSSA.

The following options are configurable for NSSA:

- **default-information-originate**
  This option is configuration for allowing default path of Type-7 in NSSA. It means routing path without routing information will use the interface which is allowed in default type-7 path. **metric** is for metric value, **metric-type** is for type of finding the path. **metric-type 1** uses internal path cost with external path cost as a cost, **metric type 2** always uses external cost value only.
- **no-redistribution**
  This option is configuration in NSSA for restriction to retransmit the routing information which is from outside.
- **no-summary**
  This option is for restriction to exchange routing information between OSPF areas.
- **translator-role**
  NSSA-LSA (Link State Advertisement) has three types according to the way of process type. **always** changes all NSSA-LSA into Type-5 LSA. **candidate** changes NSSA-LSA into Type-5 LSA when it is translator. **never** does not change NSSA-LSA.

NSSA uses ASBR when it transmits Stub Area or other routing protocol Area into OSPF. In this case, if other routing protocol has default path, use **default-information-originate** command to configure the all of default path is using the assigned ASBR

To configure **NSSA** with various features, use command with options. **area** <0-4294967295> **NSSA** command has 4 options as **default-information-originate**, **no-redistribution**, **no-summary**, **translator-role** and it can be selected more than 2 options without order. **default-information-originate** has **metric** <0-16777214> and **metric-type** <1-2> as an option, **translator-role** must choose one of **candidate**, **never**, **always as an options**.

The following is explaining options of command:

- **default-information-originate** or
  default-information-originate metric <0-16777214> or
  default-information-originate metric-type <1-2>
- **no-redistribution**
- **no-summary**
- **translator-role** {**candidate** | **never** | **always**}

To configure NSSA with one option, use the following command.

Command	Mode	Description
area {<0-4294967295> | *A.B.C.D*} **nssa default-information-originate**	Router	Configures NSSA with one option.
area {<0-4294967295> | *A.B.C.D*} **nssa default-information-originate metric** <0-16777214>		
area {<0-4294967295> | *A.B.C.D*} **nssa default-information-originate metric-type** <1-2>		
area {<0-4294967295> | *A.B.C.D*} **nssa no-redistribution**		
area {<0-4294967295> | *A.B.C.D*} **nssa no-redistribution default-information-originate** [**metric** <0-16777214>]		
area {<0-4294967295> | *A.B.C.D*} **nssa no-redistribution default-information-originate metric-type** <1-2>		
area {<0-4294967295> | *A.B.C.D*} **nssa no-redistribution default-information-originate no-summary** [**translator-role** { **always** | **candidate** | **never** }]		
area <0-4294967295> **nssa no-redistribution default-information-originate translator-role** { **always** | **candidate** | **never** }		
area <0-4294967295> **nssa no-summary**		
area {<0-4294967295> | *A.B.C.D*} **nssa no-summary** [**no-redistribution]** **default-information-originate** [**metric** <0-16777214>]		
area {<0-4294967295> | *A.B.C.D*} **nssa no-summary** [**no-redistribution**] **default-information-originate metric-type** <1-2>		
area {<0-4294967295> | *A.B.C.D*} **nssa no-summary default-information-originate [no-redistribution]** [**translator-role** { **always** | **candidate** | **never** }]		
area {<0-4294967295> | *A.B.C.D*} **nssa no-summary no-redistribution** [**translator-role** { **always** | **candidate** | **never** }]		
area <0-4294967295> **nssa translator-role** {**candidate** | **never** | **always**}		

The following example shows how to configure NAAS with more than 2 options:

- **area** <0-4294967295> **nssa no-summary no-redistribution**
- **area** <0-4294967295> **nssa translator-role** {**candidate** | **never** | **always**} **default-information-originate metric-type** <1-2> **no-redistribution**

To delete configured NSSA, use the following command.

Command	Mode	Description
no area {<0-4294967295> | *A.B.C.D*} **nssa**	Router	Deletes configured NSSA.
no area {<0-4294967295> | *A.B.C.D*} **nssa default-information-originate**		
no area {<0-4294967295> | *A.B.C.D*} **nssa default-information-originate no-redistribution** [**no summary**]		
no area {<0-4294967295> | *A.B.C.D*} **nssa default-information-originate no-redistribution no-summary** [**translator-role** {**candidate** | **never** | **always**}]		
no area {<0-4294967295> | *A.B.C.D*} **nssa default-information-originate no-redistribution translator-role** {**candidate** | **never** | **always**}		
no area {<0-4294967295> | *A.B.C.D*} **nssa no-redistribution** [**default-information-originate**]		
no area {<0-4294967295> | *A.B.C.D*} **nssa no-redistribution default-information-originate no-summary** [**translator-role** {**candidate** | **never** | **always**}]		
no area {<0-4294967295> | *A.B.C.D*} **nssa no-redistribution** [**no-summary**] **default-information-originate translator-role** {**candidate** | **never** | **always**}		
no area {<0-4294967295> | *A.B.C.D*} **nssa no-redistribution no-summary** [**translator-role** {**candidate** | **never** | **always**}]		
no area {<0-4294967295> | *A.B.C.D*} **nssa no-redistribution translator-role default-information-originate** [**no-summary**]		
no area {<0-4294967295> | *A.B.C.D*} **nssa no-redistribution translator-role** [**no-summary**] [**default-information-originate**]		
no area {<0-4294967295> | *A.B.C.D*} **nssa no-summary** [**default-information-originate**]		
no area {<0-4294967295> | *A.B.C.D*} **nssa no-summary default-information-originate no-redistribution** [**translator-role** {**candidate** | **never** | **always**}]		
no area {<0-4294967295> | *A.B.C.D*} **nssa no-summary default-information-originate translator-role** [**no-redistribution**]		
no area {<0-4294967295> | *A.B.C.D*} **nssa no-summary no-redistribution** [**default-information-originate**]		
no area {<0-4294967295> | *A.B.C.D*} **nssa no-summary no-redistribution** [**default-information-originate**] [**translator-role**]		
no area {<0-4294967295> | *A.B.C.D*} **nssa no-summary translator-role** [**default-information-originate**] [**no-redistribution**]		
no area {<0-4294967295> | *A.B.C.D*} **nssa no-summary translator-role no-redistribution**		
no area {<0-4294967295> | *A.B.C.D*} **nssa translator-role** [**default-information-originate**]		

no area {<0-4294967295> | *A.B.C.D*} **nssa translator-role default-information-originate** [**no-redistribution**] [**no-summary**]		
no area {<0-4294967295> | *A.B.C.D*} **nssa translator-role no-redistribution** [**default-information-originate**] [**no-summary**]		
no area {<0-4294967295> | *A.B.C.D*} **nssa translator-role no-summary** [**no-redistribution**] [**default-information-originate**]		

10.2.6.5 Area Range

In case of OSPF belongs to several Areas, Area routing information can be shown in one routing path. Like as above, various routing information of Area can be combined and summarized to transmit to outside.

To summarize and combine the routing information, use the following command.

Command	Mode	Description
area {<0-4294967295> | *A.B.C.D*} **range** *A.B.C.D/M*	Router	Configures to use summarized information for assigned path.
area {<0-4294967295> | *A.B.C.D*} **range** *A.B.C.D/M* {**advertise** | **not-advertise**}		

Use **advertise** option to transmit summarized routing information with using summarized information. And use the **not-advertise** option to block the transmission of summarized routing information to outside.

To release the configuration, use the following command.

Command	Mode	Description
no area {<0-4294967295> | *A.B.C.D*} **range** *A.B.C.D/M*	Router	Releases the configuration to use summarized information for assigned path
no area {<0-4294967295> | *A.B.C.D*} **range** *A.B.C.D/M* {**advertise** | **not-advertise**}		

10.2.6.6 Shortcut Area

Backbone Area is the default Area among the Areas of OSPF. All traffic should pass the Backbone Area and OSPF network must be planned for that, but there is some efficiency way which is not to pass the Backbone Area. That is Shortcut, and it must be configured for efficient traffic in every ABR type, see Section 10.2.2.

To configure the shortcut option, use the following command.

Command	Mode	Description
area {<0-4294967295> | *A.B.C.D*} **shortcut** {**default** | **disable** | **enable**}	Router	Configures the shortcut option.

To releases the configured shortcut option, use the following command.

Command	Mode	Description
no area {<0-4294967295> | *A.B.C.D*} **shortcut** {**default** | **disable** | **enable**}	Router	Releases the configured shortcut option.

10.2.6.7 Stub Area

Stub Area is that ABR is connected to Backbone Area. If it is assigned as Stub Area, ABR will notify the default path to Stub Area and other routing protocol information will not transmit to Stub Area.

To create Stub Area, use the following command.

Command	Mode	Description
area {<0-4294967295> | *A.B.C.D*} **stub** [**no-summary**]	Router	Creates a Stub Area.

If **no-summary** option adds to Stub Area, other Area OSPF routing information also can not come to Stub Area, However, it only goes to default route from ABR router. That is Totally Stubby Area.

To delete a created Stub Area, use the following command.

Command	Mode	Description
no area {<0-4294967295> | *A.B.C.D*} **stub** [**no-summary**]	Router	Deletes a created Stub Area.

10.2.6.8 Maximum Area

User can set the maximum number of OSPF area that the router can belong to.

To specify the maximum number of OSPF area, use the following command.

Command	Mode	Description
maximum-area <1-4294967294>	Router	Specifies the maximum number of OSPF area.

To remove the configured maximum area value, use the following command.

Command	Mode	Description
no maximum-area	Router	Removes the configured maximum area value.

10.2.6.9 Virtual Link

In OSPF, all areas must be connected to a backbone area. If there is a break in backbone continuity, or the backbone is purposefully portioned, you can establish a virtual link. The virtual link must be configured in both routers.

OSPF network regards virtual link routers as Point-to-point router. Therefore, the Hello-interval, Retransmit-interval, Transmit-delay must be consistent across all routers in an attached network.

User can configure Authentication for security, Authentication key for password, and time period for Hello-interval, Retransmit-interval, Transmit-delay and Dead-interval to operate virtual link.

The following items describe 7 configurations for virtual link:

- **Authentication**
  This is configuration for security of routing information. **message-digest** uses MD5 to encode for authentication, **null** means not using any of authentication.
- **Authentication-key**
  Configures the authentication which is based on text encoding.
- **Message-digest-key**
  Configures the authentication which is based on md5 type.
- **Hello-interval**
  OSPF router sends Hello packet to notify existence of itself. Hello-interval is that packet transmission interval.
- **Retransmit-interval**
  When router transmits LSA, it is waiting for approval information come from receiver. In this time, if there is no answer from receiver for configured time, the router transmits LSA again. Retransmit-interval is configuration of the time interval between transmission and retransmission
- **Dead-interval**
  If there is no hello packet for the configured time. The router perceives other router is stopped working. Dead-interval is configuration of the time interval which perceives other router is stopped operating.
- **Transmit-delay**
  When a router transmits LSA, the traffic can be delayed by status of communications. Transmit-delay is considering of the configuration for LSA transmission time.

Configuration for virtual link can be selected more than 2 options without order. The following is explaining options of command:

- **authentication** [**message-digest** | **null**]
- **authentication-key** *KEY*
- **message-digest-key** *KEY* **md5** *KEY*
- **hello-interval** <1-65535>
- **retransmit-interval** <1-65535>
- **dead-interval** <1-65535>
- **transmit-delay** <1-65535>

To configure a virtual link with one option, use the following command.

Command	Mode	Description
area {<0-4294967295> | *A.B.C.D*} **virtual-link** *A.B.C.D* **authentication** [**message-digest** | **null**]	Router	Configures a virtual link.
area {<0-4294967295> | *A.B.C.D*} **virtual-link** *A.B.C.D* **authentication-key** *KEY*		
area {<0-4294967295> | *A.B.C.D*} **virtual-link** *A.B.C.D* **message-digest-key** *KEY* **md5** *KEY*		
area {<0-4294967295> | *A.B.C.D*} **virtual-link** *A.B.C.D* **hello-interval** <1-65535>		
area {<0-4294967295> | *A.B.C.D*} **virtual-link** *A.B.C.D* **retransmit-interval** <1-65535>		
area {<0-4294967295> | *A.B.C.D*} **virtual-link** *A.B.C.D* **dead-interval** <1-65535>		
area {<0-4294967295> | *A.B.C.D*} **virtual-link** *A.B.C.D* **transmit-delay** <1-65535>		

The following example shows how to configure virtual link with more than 2 options:

- **area** <0-4294967295> **virtual-link** *A.B.C.D* **authentication-key** *KEY* **authentication** [**message-digest** | **null**]
- **area** <0-4294967295> **virtual-link** *A.B.C.D* **hello-interval** <1-65,535> **dead-interval** <1-65535>

To delete a configured virtual link, use the following command.

Command	Mode	Description
no area {<0-4294967295> | *A.B.C.D*} **virtual-link** *A.B.C.D* **authentication** [**message-digest** | **null**]	Router	Deletes a configured virtual link.
no area {<0-4294967295> | *A.B.C.D*} **virtual-link** *A.B.C.D* **authentication-key** *KEY*		
no area {<0-4294967295> | *A.B.C.D*} **virtual-link** *A.B.C.D* **message-digest-key** *KEY* **md5** *KEY*		
no area {<0-4294967295> | *A.B.C.D*} **virtual-link** *A.B.C.D* **hello-interval** <1-65535>		
no area {<0-4294967295> | *A.B.C.D*} **virtual-link** *A.B.C.D* **retransmit-interval** <1-65535>		
no area {<0-4294967295> | *A.B.C.D*} **virtual-link** *A.B.C.D* **dead-interval** <1-65535>		
no area {<0-4294967295> | *A.B.C.D*} **virtual-link** *A.B.C.D* **transmit-delay** <1-65535>		

10.2.7 Default Metric

OSPF finds metric based on interface bandwidth. For example, default metric of T1 link is 64, but default metric of 64K line is 1562. If there are plural lines in the bandwidth, you can view costs to use line by assigning metric to each line.

To classify costs to use line, use the following command.

Command	Mode	Description
auto-cost reference-bandwidth <1-4294967>	Router	Configures default metric in the unit of Mbps. (default: 100)

To delete the configuration, use the following command.

Command	Mode	Description
no auto-cost reference-bandwidth	Router	Deletes the configuration.

10.2.8 Graceful Restart Support

You need to restart OSPF protocol processor when there is network problem. In this case, it takes long time to restarts OSPF and there is no packet transmission. Other routers are also need to delete routing information and register it again. Graceful Restart improves those inconveniences. Although OSPF is restarting, Graceful Restart makes the transmission of a packet with routing information.

To configure the Graceful Restart, use the following command.

Command	Mode	Description
capability restart {**graceful** | **signaling** | **reliable-graceful**}	Router	Configures the Graceful Restart.
no capability restart		Releases the configuration.

The following items are additional options for the Graceful Restart:

- **grace-period**
  When OSPF restarts, process is keeping status in graceful for the time configured as **grace-period**. After the configured time, OSPF operates in normal.
- **helper**
  This is functions that helps other routers around the restarting router. It makes re starting router as a working and transmitting to other routers. **only-reload** is for the case of OSPF router is restarting, **only-upgrade** is for the OSPF router which is up-grading software, and **max-grace-period** works when **grace-period** from other routers has less value than it. Configuration for Helper can be selected more than 2 options without order.

To configure the additional options for Graceful Restart, use the following command.

Command	Mode	Description
ospf restart grace-period <1-1800>	Global	Configures the additional options for Graceful Restart.
ospf restart helper max-grace-period <1-1800>		
ospf restart helper max-grace-period <1-1800> **only-reload** [**only-upgrade**]		
ospf restart helper max-grace-period <1-1800> **only-upgrade** [**only-reload**]		
ospf restart helper only-reload [**only-upgrade**]		
ospf restart helper only-reload only-upgrade max-grace-period <1-1800>		
ospf restart helper only-reload max-grace-period <1-1800> [**only-upgrade**]		
ospf restart helper only-upgrade [**only-reload**]		
ospf restart helper only-upgrade only-reload max-grace-period <1-1800>		
ospf restart helper only-upgrade max-grace-period <1-1800> [**only-reload**]		

To release the configuration, use the following command.

Command	Mode	Description
no ospf restart grace-period <1-1800>	Global	Releases the configuration.
ospf restart helper never		
no ospf restart helper max-grace-period <1-1800>		

10.2.9 Opaque-LSA Support

Opaque-LSA is LSA Type-9, Type-10, Type-11. The V5812G enables Opaque-LSA as a default but it can be released by user.

To release the enabled Opaque-LSA management, use the following command.

Command	Mode	Description
no capability opaque	Router	Releases the enabled Opaque-LSA management.

To enable Opaque-LSA management, use the following command.

Command	Mode	Description
capability opaque	Router	Enables Opaque-LSA management.

10.2.10 Default Route

You can configure ASBR (Autonomous System Boundary Router) to transmit default route to OSPF network. Autonomous System Boundary router transmits route created externally to OSPF network. However, it does not create system default route.

To have autonomous System Boundary router create system default route, use the following command.

Command	Mode	Description
default-information originate	Router	Configures the default route.

The following items are detail options for the Default Route configuration.

- **metric**
  Configures Metric value of the default route.
- **metric-type**
  metric-type is for type of finding the path. **metric-type 1** uses internal path cost with external path cost as a cost, **metric type 2** always uses external cost value only.
- **always**
  Transmits the default route to outside.
- **no-summary**
  Restricts to exchange routing information between OSPF area in NSSA.
- **route-map**
  Transmits specific routing information to assigned route which has MAP-NAME.

The detail options for default route configuration are classified in 4 as above, and those configurations can be selected more than 2 options without order.

The following is explaining options of command:

- **metric** <0-16777214>
- **metric-type** <1-2>
- **always**
- **route-map** *MAP-NAME*

To configure the default route with an option, use the following command.

Command	Mode	Description
default-information originate metric <0-16777214>	Router	Configures the default route with one option.
default-information originate metric-type <1-2>		
default-information originate always		
default-information originate route-map *MAP-NAME*		

The following example shows how to configure default route with more than 2 options:

- **default-information originate metric-type** <1-2> **always**
- **default-information originate route-map** *MAP-NAME* **metric** <0-16777214>

To delete the configuration, use the following command.

Command	Mode	Description
no default-information originate	Router	Deletes the configuration.
no default-information originate metric <0-16777214>		
no default-information originate metric-type <1-2>		
no default-information originate always		
no default-information originate route-map *MAP-NAME*		

10.2.11 Finding Period

OSFP start to find the shortest path as soon as got a notification of changing the network component. You can configure the period to find the path.

To configure the period of finding, use the following command.

Command	Mode	Description
timers spf *SPF-DELAY SPF-HOLD*	Router	Configures the period of finding in the unit of second. SPF-DELAY: 0-4294967295 (default: 5) SPF-HOLD: 0-4294967295 (default: 10)

To release the configuration, use the following command.

Command	Mode	Description
no timers spf	Router	Release the configuration.

10.2.12 External Routes to OSPF Network

If other routing protocol redistribute into OSPF network, these routes become OSPF external routes. Other routing protocols are RIP and BGP. And static route, connected route, kernel route are also external route. Those routing information can distribute into OSPF network.

There are 4 kinds of additional configuration about external routes to OSPF network. **metric** is configures Metric value of the default route, **metric-type** is for type of finding the path. **metric-type 1** uses internal path cost with external path cost as a cost, metric type 2 always uses external cost value. **route-map** is transmission of specific routing information to assigned route which has MAP-NAME, and, **tag** is using the assign tag number on the specific MAP-NAME.

Those 4 kinds of additional configuration can be selected more than 2 options without order, and it applies to consistent across all external routes in an attached network.

The following is explaining 4 options of command:

- **metric** <0-16777214>
- **metric-type** <1-2>
- **route-map** *MAP-NAME*
- **tag** <0-4294967295>

To configure the external route transmission, use the following command.

Command	Mode	Description
redistribute {**bgp** | **connected** | **kernel** | **rip** | **static**} **metric** <0-16777214>	Router	Configures the external route transmission.
redistribute {**bgp** | **connected** | **kernel** | **rip** | **static**} **metric-type** <1-2>		
redistribute {**bgp** | **connected** | **kernel** | **rip** | **static**} **route-map** *MAP-NAME*		
redistribute {**bgp** | **connected** | **kernel** | **rip** | **static**} **tag** <0-4294967295>		

The following example shows how to configure it with more than 2 options:

- **redistribute** {**bgp** | **connected** | **kernel** | **rip** | **static**} **metric** <0-16777214> **tag** <0-4294967295>
- **redistribute** {**bgp** | **connected** | **kernel** | **rip** | **static**} **tag** <0-4294967295> **metric-type** <1-2>

For efficient transmission of routing information, and to avoid non-matching between metric and OSPF routing protocol, use the **default matric** command to assign metric about redistribute route.

To configure the default metric, use the following command.

Command	Mode	Description
default-metric <0-16777214>	Router	Configures the default metric.

To delete the default metric, use the following command.

Command	Mode	Description
no default-metric [<0-16777214>]	Router	Deletes the default metric.

10.2.13 OSPF Distance

An administrative distance is a rating of the trustworthiness of a routing information source, such as an individual router or a group of routers. Numerically, an administrative distance is an integer between 0 and 255. In general, the higher the value is, the lower the trust rating is. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored.

OSPF uses three different administrative distances: intra-area, inter-area, and external. Routes learned through other domain are external, routes to another area in OSPF domain are inter-area, and routes inside an area are intra-area. The default distance for each type of route is 110. In order to change any of the OSPF distance values, use the following commands.

The following is explaining 3 options of command.

- **external** <1-255>
- **inter-area** <1-255>
- **intra-area** <1-255>

To configure the distance with 1 option, use the following command.

Command	Mode	Description
distance <1-255>	Router	Configures the distance of OSPF route. (default: 110)
distance ospf external <1-255>		
distance ospf inter-area <1-255>		
distance ospf intra-area <1-255>		

The following example shows how to configure the distance with more than 2 options:

- **distance ospf external** <1-255> **inter-area** <1-255>
- **distance ospf inter-area** <1-255> **intra-area** <1-255>

To make it as a default, use the following command.

Command	Mode	Description
no distance ospf	Router	Restores it as the default.
no distance <1-255>		Deletes a configured distance of OSPF route.

10.2.14 Host Route

OSPF regards routing information of specific host as stub link information. Routing information can be assigned to each host which is connected with one router.

To configure the routing information to each host, use the following command.

Command	Mode	Description
host *A.B.C.D* **area** {*A.B.C.D* | <1-4294967295>}	Router	Configures the routing information to each host.
host *A.B.C.D* **area** {*A.B.C.D* | <1-4294967295>} **cost** <0-65535>		

To delete the routing information of specific host, use the following command.

Command	Mode	Description
no host *A.B.C.D* **area** { *A.B.C.D* | <1-4294967295>}	Router	Deletes the routing information to each host.
no host *A.B.C.D* **area** { *A.B.C.D* | <1-4294967295>} **cost** <0-65535>		

10.2.15 Passive Interface

The passive interface which is configured by OSPF network operate as stub area. Therefore passive interface can not exchange the OSPF routing information.

To configure the passive interface, use the following command.

Command	Mode	Description
passive-interface *INTERFACE* [*A.B.C.D*]	Router	Configures the passive interface.

To release the configured as passive interface, use the following command.

Command	Mode	Description
no passive-interface *INTERFACE* [*A.B.C.D*]	Router	Releases the configured as passive interface.

10.2.16 Blocking Routing Information

The V5812G can classify and restrict the routing information. To configure this function, sort the specific routing information in **access-list** first, and block the routing information in **access-list.**

To block the routing information in access-list, use the following command.

Command	Mode	Description
distribute-list *ACCESS-LIST* **out** {**bgp** | **connected** | **kernel** | **rip** | **static**}	Router	Blocks the routing information in access-list

To release the configuration, use the following command.

Command	Mode	Description
no distribute-list *ACCESS-LIST* **out** {**bgp** | **connected** | **kernel** | **rip** | **static**}	Router	Releases the configuration.

10.2.17 Summary Routing Information

In case of external routing protocol transmits to OSPF network, more than 2 routing information can be summarized as one. For example, 192.168.1.0/24 and 192.168.2.0/24 can become 192.168.0.0/16 to transmit to OSPF network. This summary reduces the number of routing information and it improves a stability of OSPF protocol

And you can use **no-advertise** option command to block the transmission of summarized routing information to outside. Or assign the specific **tag** number to configure.

To configure the summary routing information, use the following command.

Command	Mode	Description
summary-address *A.B.C.D/M*	Router	Configures the summary routing information.
summary-address *A.B.C.D/M* **not-advertise**		Blocks the transmission of summarized routing information to outside
summary-address *A.B.C.D/M* **tag** <0-4294967295>		Configures the summary routing information with a specific tag

To delete the configured summary routing information, use the following command.

Command	Mode	Description
no summary-address *A.B.C.D/M*	Router	Deletes the summary routing information.
no summary-address *A.B.C.D/M* **not-advertise**		Blocks the transmission of summarized routing information to outside
no summary-address *A.B.C.D/M* **tag** [<0-4294967295>]		Configures the summary routing information with a specific tag

10.2.18 OSPF Monitoring and Management

You can view all kinds of statistics and database recorded in IP routing table. These 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.

10.2.18.1 Displaying OSPF Protocol Information

You can verify the information of OSPF protocol. To display the information about OSPF protocol, use the following command.

Command	Mode	Description
show ip ospf	Enable Global Bridge	Shows the information about OSPF protocol.
show ip ospf <0-65535>		Shows the information about a specific process ID in OSPF protocol.

To display OSPF routing table to ABR and ASBR, use the following command.

Command	Mode	Description
show ip ospf [<0-65535>] **border-routers**	Enable Global Bridge	Shows OSPF routing table to ABR and ASBR.

To display the OSPF database, use the following command.

Command	Mode	Description
show ip ospf [<0-65535>] **database** {**self-originate** | **max-age** | **adv-router** *A.B.C.D* }	Enable Global Bridge	Shows the OSPF database.
show ip ospf [<0-65535>] **database** {**asbr-summary** | **external** | **network** | **router** | **summary** | **nssa-external** | **opaque-link** | **opaque-area** | **opaque-as**}		
show ip ospf [<0-65535>] **database** {**asbr-summary** | **external** | **network** | **router** | **summary** | **nssa-external** | **opaque-link** | **opaque-area** | **opaque-as**} **self-originate**		
show ip ospf [<0-65535>] **database** {**asbr-summary** | **external** | **network** | **router** | **summary** | **nssa-external** | **opaque-link** | **opaque-area** | **opaque-as**} **adv-router** *A.B.C.D*		
show ip ospf [<0-65535>] **database** {**asbr-summary** | **external** | **network** | **router** | **summary** | **nssa-external** | **opaque-link** | **opaque-area** | **opaque-as**} *A.B.C.D*		
show ip ospf [<0-65535>] **database** {**asbr-summary** | **external** | **network** | **router** | **summary** | **nssa-external** | **opaque-link** | **opaque-area** | **opaque-as**} *A.B.C.D* **self-originate**		
show ip ospf [<0-65535>] **database** {**asbr-summary** | **external** | **network** | **router** | **summary** | **nssa-external** | **opaque-link** | **opaque-area** | **opaque-as**} *A.B.C.D* **adv-router** *A.B.C.D*		

To display the interface information of OSPF, use the following command.

Command	Mode	Description
show ip ospf interface [*INTERFACE*]	Enable Global Bridge	Shows the interface information of OSPF.

To display the information of neighbor route, use the following command.

Command	Mode	Description
show ip ospf [<0-65535>] **neighbor**	Enable Global Bridge	Shows the information of neighbor router.
show ip ospf [<0-65535>] **neighbor** *A.B.C.D* [**detail**]		
show ip ospf [<0-65535>] **neighbor interface** *A.B.C.D*		
show ip ospf [<0-65535>] **neighbor detail** [**all**]		
show ip ospf [<0-65535>] **neighbor all**		

To display the routing information registered in routing table, use the following command.

Command	Mode	Description
show ip ospf [<0-65535>] **route**	Enable Global Bridge	Shows the routing information which is registered in routing table.

To display the information of virtual link, use the following command.

Command	Mode	Description
show ip ospf [<0-65535>] **virtual-links**	Enable Global Bridge	Shows the information of virtual link.

10.2.18.2 Sending SNMP Trap

To enable/disable the system to send SNMP trap message of OSPF routing information, use the following command.

Command	Mode	Description
ospf snmp-notification enable	Router	Configures the system to send SNMP trap of routing information while OSPF is running.
ospf snmp-notification disable		Disables the system to send SNMP trap of routing information while OSPF is running.

10.2.18.3 Logging Neighbor Changes

To enable/disable the system to log changes in OSFP neighbors' state such as system up/down and reset, use the following command.

Command	Mode	Description
ospf log-neighbor-changes	Router	Enables logging of OSPF neighbor state changes
no ospf log-neighbor-changes		Disables logging of OSPF neighbor state changes

10.2.18.4 Limiting Number of Database

The V5812G can limit the Number of Database to process in OSPF. For example, if a router connected with many of routers, it carries overload to process the database. Therefore, Limiting the Number of Database reduces the overload on system.

To configure the limiting Number of Database, use the following command.

Command	Mode	Description
max-concurrent-dd <1-65535>	Router	Configures the limiting Number of Database.

To delete the configuration, use the following command.

Command	Mode	Description
no max-concurrent-dd <1-65535>	Router	Deletes the configuration.

10.2.18.5 Maximum Process of LSA

The V5812G can configure maximum number of LSA to process. LSA is classified as internal route LSA and external route LSA, maximum number of LSA can configure on each class.

And also, if the process of LSA is over the configured number, you can configure it to stop the process or send the caution message. When the outer route of LSA is overflowed the assigned value, you can configure it to restart OSPF after the waiting time. If the waiting time is 0, OSPF keeps the process before the administrator reboots the system.

To assign the maximum number of LSA to process in OSPF, use the following command.

Command	Mode	Description
overflow database <1-4294967294> [**hard** | **soft**]	Router	Assigns the number of LSA for internal route.
overflow database external <0-2147483647> <0-65535>		Assigns the number of LSA for external route.

When there is an overflow, **hard** configuration will stop the process, and **soft** configuration will send a caution message.

To release the configuration, use the following command.

Command	Mode	Description
no overflow database	Router	Releases the configuration for OSPF internal route.
no overflow database external [<0-2147483647>]		Releases the configuration for OSPF external route.
no overflow database external <0-2147483647> [<0-65535>]		

10.2.19 OSPF Debug

To enable OSPF debugging, use the following command.

Command	Mode	Description
debug ospf [**all**]	Enable Global	Enables OSPF debugging.
debug ospf events [**abr** | **asbr** | **lsa** | **nssa** | **os** | **router** | **vlink**]		Enables debugging about OSPF operation such as OSPF neighbor router, transmitted information, deciding destination router, calculating the shortest route, and so on.
debug ospf ifsm [**events** | **status** | **timers**]		Enables debugging about OSPF interface.
debug ospf lsa [**flooding** | **generate** | **install** | **maxage** | **refresh**]		Enables debugging about information transmitted by OSPF and calculating the shortest route.
debug ospf nfsm [**events** | **status** | **timers**]		Enables debugging about OSPF Neighbor router.
debug ospf nsm [**interface** | **redistribute**]		Enables debugging between OSPF process and NSM (Network Services Module).
debug ospf packet [**hello** | **dd** | **ls-ack** | **ls-request** | **ls-update** | **send** | **recv** | **detail**]		Enables debugging about each packet.
debug ospf route [**ase** | **ia** | **install** | **spf**]		Enables debugging about OSPF routing.

To disable OSPF debugging, use the following command.

Command	Mode	Description
no debug ospf [**all**]	Enable Global	Disables OSPF debugging.
no debug ospf events [**abr** | **asbr** | **lsa** | **nssa** | **os** | **router** | **vlink**]		
no debug ospf ifsm [**events** | **status** | **timers**]		
no debug ospf lsa [**flooding** | **generate** | **install** | **maxage** | **refresh**]		
no debug ospf nfsm [**events** | **status** | **timers**]		
no debug ospf nsm [**interface** | **redistribute**]		
no debug ospf packet [**hello** | **dd** | **ls-ack** | **ls-request** | **ls-update** | **send** | **recv** | **detail**]		
no debug ospf route [**ase** | **ia** | **install** | **spf**]		

To display the OSPF debugging information, use the following command.

Command	Mode	Description
show debugging ospf	Enable Global Bridge	Shows the debugging information of OSPF.

10.3 Routing Information Protocol (RIP)

Routing Information Protocol (RIP), as it is more commonly used than any other Routing Protocols, for use in small, homogeneous networks. It is a classical distance-vector routing protocol with using hop count. RIP is formally defined in documents in Request For Comments (RFC) 1058 and Internet Standard (STD) 56. As IP-based networks became both more numerous and greater in size, it became apparent to the Internet Engineeing Task Force (IETF) that RIP needed to be updated. Consequently, the IETF released RFC 1388, RFC 1723 and RFC 2453, which described RIP v2 (the second version of RIP).

RIP v2 uses broadcast User Datagram Protocol (UDP) data packets to exchange routing information. The V5812G sends routing information and updates it every 30 seconds. This process is termed advertised. If a router does not receive an update from another router for 180 seconds or more, it marks the routes served by the non-updating router as being unusable. If there is still no update after 120 seconds, the router removes all routing table entries for the non-updating router.

The metric that RIP uses to rate the value of different routes is hop count. The hop count is the number of routers that should be traversed through the network to reach the destination. A directly connected network has a metric of zero; an unreachable network has a metric of 16. This short range of metrics makes RIP an unsuitable routing protocol for large networks.

A router that is running RIP can receive a default network via an update from another router that is running RIP, or the router can source (generate) the default network itself with RIP. In both cases, the default network is advertised through RIP to other RIP neighbors. RIP sends updates to the interfaces in the specified networks.

If an interface's network is not specified, it will not be advertised in any RIP update. The V5812G supports RIP version 1 and 2.

10.3.1 Enabling RIP

To use RIP protocol, you should enable RIP.

Step 1 To open *Router Configuration* mode, use the following command on *Global Configuration* mode.

Command	Mode	Description
router rip	Global	Opens *Router Configuration* mode and operates RIP routing protocol.
no router rip		Restores all configurations involved in RIP to the default.

Step 2 Configure the network to operate as RIP.

Command	Mode	Description
network {*A.B.C.D/M* | *INTERFACE* }	Router	Establishes the network to operate as RIP. A.B.C.D/M: IP prefix (e.g. 35.0.0.0/8) INTERFACE: interface name
no network {*A.B.C.D/M* | *INTERFACE* }		Removes a specified network to operate as RIP.

The command **network** enables RIP interfaces between certain numbers of a special network address. For example, if the network for 10.0.0.0/24 is RIP enabled, this would result in all the addresses from 10.0.0.0 to 10.0.0.255 being enabled for RIP.

By the way, it's not possible to exchange the RIP routing information if it hasn't been established RIP network using **network** command even though interface belongs to RIP network. RIP packets with RIP routing information is transmitted to port specified with the **network** command.

After RIP is enabled, you can configure RIP with the following items:

- RIP Neighbor Router
- RIP Version
- Creating available Static Route only for RIP
- Redistributing Routing Information
- Metrics for Redistributed Routes
- Administrative Distance
- Originating Default Information
- Routing Information Filtering
- Maximum Number of RIP Routes
- RIP Network Timer
- Split Horizon
- Authentication Key
- Restarting RIP
- UDP Buffer Size of RIP
- Monitoring and Managing RIP

10.3.2 RIP Neighbor Router

Since RIP is broadcast protocol, routers should be connected each other to transmit the routing information of RIP to non-broadcast network.

To configure neighbor router to transmit RIP information, use the following command on *Router Configuration* mode.

Command	Mode	Description
neighbor *A.B.C.D*	Router	Configures a neighbor router to exchange routing information. A.B.C.D: neighbor address
no neighbor *A.B.C.D*		Deletes the neighbor router.

i You can block the routing information to specific interface by using the **passive-interface** command.

10.3.3 RIP Version

Basically, the V5812G supports RIP version 1 and 2. However, you can configure to receive either RIP v1 type packets only or RIP v2 type packets only.

To configure RIP version, use the following command.

Command	Mode	Description
version {**1** | **2**}	Router	Selects one type of RIP packets to transmit either RIP v1 or RIP v2 type packet
no version {**1** | **2**}		Restores the default of specified RIP version type

The preceding task controls default RIP version settings. You can override the routers RIP version by configuring a particular interface to behave differently.

To control which RIP version an interface sends, perform one of the following tasks after opening *Interface Configuration* mode.

Command	Mode	Description
ip rip send version 1	Interface	Sends RIP v1 type packet only to this interface.
ip rip send version 2		Sends RIP v2 type packet only to this interface.
ip rip send version 1 2		Sends RIP v1 and RIP v2 type packets both.

To delete the configuration that sends RIP version packet to interface, use the following command.

Command	Mode	Description
no ip rip send version 1	Interface	Deletes the configuration of RIP v1 type packet for helping them to be sent to the interface.
no ip rip send version 2		Deletes the configuration of RIP v2 type packet for helping them to be sent to the interface.
no ip rip send version 1 2		Deletes the configuration of both RIP v1 and v2 type packets for helping them to be sent to the interface.

Similarly, to control how packets received from an interface are processed, perform one of the following tasks.

Command	Mode	Description
ip rip receive version 1	Interface	Receives RIP v1 type packet only from the interface.
ip rip receive version 2		Receives RIP v2 type packet only from the interface.
ip rip receive version 1 2		Receives both RIP v1 and RIP v2 type packets from the interface.

To delete the configuration that receives RIP version packet from the interface, use the following command.

Command	Mode	Description
no ip rip receive version 1	Interface	Deletes the configuration of RIP v1 type packet for helping them be received from the interface.
no ip rip receive version 2		Deletes the configuration of RIP v2 type packet for helping them to be received from interface.
no ip rip receive version 1 2		Deletes the configuration of both RIP v1 and RIP v2 type packets for helping them to be received from the interface.

10.3.4 Creating available Static Route only for RIP

This feature is provided only by Dasan Networks' **route** command creates static route available only for RIP. If you are not familiar with RIP protocol, you would better use **redistribute static** command.

Command	Mode	Description
route *A.B.C.D/M*	Router	Creates suitable static route within RIP environment only. A.B.C.D/M: IP prefix
no route *A.B.C.D/M*		Deletes this static route established by route command.

10.3.5 Redistributing Routing Information

The V5812G can redistribute the routing information from a source route entry into the RIP tables. For example, you can instruct the router to re-advertise connected, kernel, or static routes as well as other routes established by routing protocol. This capability applies to all the IP-based routing protocols.

To redistribute routing information from a source route entry into the RIP table, use the following command.

Command	Mode	Description
redistribute {**kernel** | **connected** | **static** | **ospf** | **bgp**}	Router	Registers transmitted routing information in another router's RIP table. 1-16: metric value WORD: pointer to route-map entries
redistribute {**kernel** | **connected** | **static** | **ospf** | **bgp** } **metric** <0-16>		
redistribute {**kernel** | **connected** | **static** | **ospf** | **bgp** } **route-map** *WORD*		

To delete the configuration for redistributing routing information in another router's RIP table, use the following command.

Command	Mode	Description
no redistribute {**kernel** | **connected** | **static** | **ospf** | **bgp**}	Router	Removes the configuration of transmitted routing information in another router's RIP table.
no redistribute {**kernel** | **connected** | **static** | **ospf** | **bgp** } **metric** <0-16>		
no redistribute {**kernel** | **connected** | **static** | **ospf** | **bgp**} **route-map** *WORD*		

As the needs of the case demand, you may also conditionally restrict the routing information between the two networks using **route-map** command.

To permit or deny the specific information, open the *Route-map Configuration* mode using the following command in *Global Configuration* mode.

Command	Mode	Description
route-map *TAG* {**deny** | **permit**} <0-65535>	Global	Creates the route map. TAG: route map tag 0-65535: sequence number

One or more **match** and **set** commands typically follow **route-map** command. If there are no **match** commands, then everything matches. If there are no set commands, nothing is done. Therefore, you need at least one **match** or **set** command.

Use the following command on *Route-map Configuration* mode to limit the routing information for transmitting to other routers' RIP table.

Command	Mode	Description
match interface *INTERFACE*	Route-map	Transmits the information to specified interface only. INTERFACE: interface name
match ip address {<1-199> | <1300-2699> | *NAME*}		Transmits the information matched with access-list. 1-199: IP access list number 1300-2699: IP access list number (extended range) NAME: IP access list name
match ip address prefix-list *NAME*		Transmits the information matched with prefix-list. NAME: IP prefix list name
match ip next-hop {<1-199> | <1300-2699> | N*AME*}		Transmits information to only neighbor router in access-list. 1-199: IP access list number 1300-2699: IP access list number (extended range) NAME: IP access list name
match ip next-hop prefix-list *NAME*		Transmits information to only neighbor router in prefix-list. NAME: IP prefix list name

Command	Mode	Description
match metric <0-4294967295>	Route-map	Transmits information matched with specified metric, enter the metric value.
set ip next-hop *A.B.C.D*		Configures Neighbor router's address. A.B.C.D: IP address of next hop
set metric <1-2147483647>		Sets the metric value for destination routing protocol. 1-2147483647: metric value

10.3.6 Metrics for Redistributed Routes

The metrics of one routing protocol do not necessarily translate into the metrics of another. For example, the RIP metric is a hop count and the OSPF metric is a combination of five quantities. In such situations, an artificial metric is assigned to the redistributed route. Because of this unavoidable tampering with dynamic information, carelessly exchanging routing information between different routing protocols can create routing loops, which can seriously degrade network operation. To prevent this situation, we configure metrics

To set metrics for redistributed routes, use the following command.

Command	Mode	Description
default-metric <1-16>	Router	Configures the equal metric of all routes transmitted by routing protocol, enter the value. 1-16: default metric value
no default-metric <1-16>		Removes the equal metric of all routes transmitted by routing protocol.

i The metric of all protocol can be configured from 0 to 4294967295. It can be configured from 1 to 16 for RIP.

10.3.7 Administrative Distance

Administrative distance is a measure of the trustworthiness of the source of the routing information.

In large scaled network, Administrative distance is the feature that routers use in order to select the best path when there are two or more different routes to the same destination from two different routing protocols. Administrative distance defines the reliability of a routing protocol. Each routing protocol is prioritized in order of most to least reliable (believable) with the help of an administrative distance value.

Remember that administrative distance has only local significance, and is not advertised in routing updates. Most routing protocols have metric structures and algorithms that are not compatible with other protocols. In a network with multiple routing protocols, the exchange of route information and the capability to select the best path across the multiple protocols are critical. Administrator should set the distance value based on whole routing networks.

To configure the administrative distance value, use the following command.

Command	Mode	Description
distance <1-255> [*A.B.C.D/M* [*ACCESS-LIST*]]	Router	Sets the administrative distance value for routes. 1-255: distance value A.B.C.D/M: IP source prefix ACCESS-LIST: access list name
no distance <1-255> [*A.B.C.D/M* [*ACCESS-LIST*]]		Deletes the administrative distance value.

10.3.8 Originating Default Information

You can set an autonomous system boundary router to generate and transmit a default route into an RIP routing domain. If you specifically set to generate a default routes into an RIP network, this router becomes an autonomous system (AS) boundary router. However, an AS boundary router does not generate a default route automatically into the RIP network.

To generate a default route into RIP by the AS boundary router, use the following command on *Router Configuration* mode.

Command	Mode	Description
default-information originate	Router	Generates a default route into RIP by the AS boundary router.
no default-information originate		Disables a default route feature.

10.3.9 Routing Information Filtering

You can limit the routing protocol information by performing the following tasks.

- Block the transmission of routing information to a particular interface. This is to prevent other systems on an interface from learning about routes dynamically.
- Provides a local mechanism for increasing the value of routing metrics.

10.3.9.1 Filtering Access List and Prefix List

The V5812G switch is able to permit and deny conditions that you can use to filter inbound or outbound routes by access-list or prefix-list. Use the **distribute-list** command to apply the access list to routes received from or forwarded to a neighbor.

User should configure the route information for a set of deny conditions based on matching each access list or prefix list. In addition, this configuration is able to be applied on the specific interface as well as the whole routes information of switch.

To block the route information based on matching access list or prefix list, use the following command.

Command	Mode	Description
distribute-list *ACCESS-LIST* {**in** | **out**} [*INTERFACE*]	Router	Apply a specific access list or prefix list to incoming or outgoing RIP route updates on interface in order to block the route. INTERFACE: interface name ACCESS-LIST: access list name PREFIX-LIST: prefix list name
distribute-list prefix *PREFIX-LIST* {**in** | **out**} [*INTERFACE*]		

To remove the filtering access list or prefix-list to incoming or outgoing RIP route

Command	Mode	Description
no distribute-list *ACCESS-LIST* {**in** | **out**} [*INTERFACE*]	Router	Removes the application of a specific access list or prefix list to incoming or outgoing RIP route updates on interface in order to block the route.
no distribute-list prefix *PREFIX-LIST* {**in** | **out**} [*INTERFACE*]		

10.3.9.2 Disabling the transmission to Interface

To prevent other routers on a local network from learning about routes dynamically, you can keep routing update messages from being sent through a router interface. This feature applies to all IP-based routing protocols except for BGP.

Disable the routing information to transmit on this interface of router, use the following command.

Command	Mode	Description
passive-interface *INTERFACE*	Router	Disables the transmission of multicast RIP messages on the interface. INTERFACE: interface name
no passive-interface *INTERFACE*		Re-enables the transmission of RIP multicast messages on the specified interface.

10.3.9.3 Offset List

An offset list is the mechanism for increasing incoming and outgoing metrics to routes learned via RIP. You can limit the offset list with an access list. To add the value of routing metrics, use the following command.

Command	Mode	Description
offset-list *ACCESS-LIST* {**in** | **out**} <0-16> [*INTERFACE*]	Router	Add an offset to incoming or outgoing metrics to routes learned via RIP. ACCESS-LIST: access list name 0-16: type number
no offset-list *ACCESS-LIST* {**in** | **out**} <0-16> [*INTERFACE*]		Removes an offset list.

10.3.10 Maximum Number of RIP Routes

You can set the maximum number of RIP routes for using on RIP protocol. To set the maximum number of routes, use the following command.

Command	Mode	Description
maximum prefix <1-65535> [1-100]	Router	Sets the maximum number of routes of RIP. 1-65535: maximum number of RIP routes 1-100: percentage of maximum routes to generate a warning (default: 75)
no maximum prefix <1-65535> [1-100]		Removes the maximum number of routes of RIP which are set before.

10.3.11 RIP Network Timer

Routing protocols use several timers that determine such variables as the frequency of routing updates, the length of time before a route becomes invalid, and other parameters. You can adjust these timers to tune routing protocol performance to better your internet needs. The default settings for the timers are as follows.

- **Update**
  The routing information is updated once every 30 seconds. This is the fundamental timing parameter of the routing protocol. Every update timer seconds, the RIP process is supposed to send the routing table to all neighboring RIP routers.
- **Timeout**
  The default is 180 seconds. It's the interval of time in seconds after which a route is declared invalid. However, this information will be still written in routing table until the neighbor routers are notified that this route is removed from the routing table.
- **Garbage**
  The invalid information of route is deleted on the routing table every 120 seconds. Once the information of route is classified as "invalid", it's eventually removed from the routing table after 120 seconds.

To adjust the timers, use the following command.

Command	Mode	Description
timers basic *UPDATE TIMEOUT GARBAGE*	Router	Adjusts RIP network timers.
no timers basic *UPDATE TIMEOUT GARBAGE*		Restores the default timers.

10.3.12 Split Horizon

Normally, routers that are connected to broadcast type IP networks and that use distance-vector routing protocols employ the split horizon mechanism to reduce the possibility of routing loops. Split horizon blocks information about routes from being advertised by a router out any interface from which that information originated. This behavior usually optimizes communications among multiple routers, particularly when links are broken.

However, with non-broadcast networks, such as Frame Relay, situations can arise for which this behavior is less than ideal. For these situations, you might want to disable split horizon.

If the interface is configured with secondary IP address and split horizon is enabled, updates might not be sourced by every secondary address. One routing update is sourced per network number unless split horizon is disabled.

To enable or disable split horizon mechanism, use the following command in *Interface Configuration* mode.

Command	Mode	Description
ip rip split-horizon [**poisoned**]	Interface	Enables the split horizon mechanism. poisoned: performs poisoned reverse.
no rip ip split-horizon [**poisoned**]		Disables the split horizon mechanism.

10.3.13 Authentication Key

RIP v1 does not support authentication. If you are sending and receiving RIP v2 packets, you can enable RIP authentication on an interface. The key chain determines the set of keys that can be used on the interface. If a key chain is not configured, plain text authentication can be performed using string command.

The V5812G supports two modes of authentication on an interface for which RIP authentication is enabled: plain text authentication and MD5 authentication. The default authentication in every RIP v2 packet is plain text authentication.



Do not use plain text authentication in RIP packets for security purposes, because the unencrypted authentication key is sent in every RIP v2 packet. Use plain text authentication when security is not an issue, for example, to ensure that misconfigured hosts do not participate in routing.

To configure RIP authentication, use the following command.

Command	Mode	Description
ip rip authentication key-chain *NAME*	Interface	Enables authentication for RIP v2 packets and to specify the set of keys that can be used on an interface. NAME: name of key chain
ip rip authentication mode {**text** | **md5**}		Specifies the authentication mode. text: sends a simple text password to neighbors. If a neighbor does not have the same password, request and updates from this system are rejected. md5: sends an MD5 hash to neighbors. Neighbors must share the MD5 key to decrypt the message and encrypt the response.
ip rip authentication string *STRING*	Interface	Configures RIP authentication string which will be using on interface without Key chain. The string must be shorter than 16 characters. STRING: RIP authentication string

To disable RIP authentication, use the following command.

Command	Mode	Description
no ip rip authentication key-chain *NAME*	Interface	Disables authentication keys that can be used on an interface.
no ip rip authentication mode {**text** | **md5**}		Disables specified authentication mode.
no ip rip authentication string *STRING*		Removes RIP authentication string which will be using on interface without Key chain.

10.3.14 Restarting RIP

Occasionally, you should restart RIP system only when the switch is still operating while you manage and configure RIP. At this time, the switch reports the neighbors that RIP system is being restarting. It keeps previous route information until the restarting is complete in timer.

To restart RIP system only, use the following command.

Command	Mode	Description
rip restart grace-period <1-65535>	Global	Restarts RIP system and set the period.
no rip restart grace-period [<1-65535>]		Removes a configured period.

10.3.15 UDP Buffer Size of RIP

RIP protocol exchanges the routing information between routers using UDP packets. The V5812G can be configured theses UDP packets buffer size, use the following command.

Command	Mode	Description
recv-buffer size <8196-2147483647>	Router	Sets the UDP Buffer size value for using RIP. 8196-2147483647: UDP buffer size value
no recv-buffer size <8196-2147483647>		Restore the default value of UDP buffer size.

10.3.16 Monitoring and Managing RIP

You can display specific router information such as the contents of IP routing tables, and databases. Information provided can be used to determine resource utilization and solve network problems. You can also discover the routing path your router’s packets are taking through the network.

10.3.16.1 Displaying RIP Protocol Information

To display RIP information, use the following command.

Command	Mode	Description
show ip rip [**database**]	Enable Global Bridge	Shows RIP information being used in router.
show ip route [**database**] **rip**		Shows a routing table information involved in RIP.
show ip protocols [**rip**]		Shows a current status of RIP protocol and its information.
show ip rip interface [*INTERFACE*]	Enable	Shows RIP information of specified interface.

To clear RIP information being used in router, use the following command.

Command	Mode	Description
clear ip rip route [**bgp** | **connected** | **kernel** | **ospf** | **rip** | **static** | **all** | *A.B.C.D/M*]	Enable Global Bridge	Deletes RIP information being used in router.

10.3.16.2 Displaying Debugging Information

To quickly diagnose problems, the **debug** command is useful for customers. To enable debugging of RIP routing transactions, use the following command.

Command	Mode	Description
debug rip [**all**]	Enable	Turns on all debugging options of changed RIP information.
debug rip events		Enables a debugging of RIP event such as packet transmit and sending and changed RIP information.
debug rip nsm		Enables RIP nsm debugging.
debug rip packet [**recv** | **send**]		Shows more detailed information about RIP packet. The information includes address of packet transmission and port number.
debug rip packet [**recv** | **send**] **detail**		

To disable debugging of RIP routing transactions, use the following command.

Command	Mode	Description
no debug rip [**all**]	Enable	Turns off all debugging options of changed RIP information.
no debug rip events		Disables a debugging of RIP event such as packet transmit and sending and changed RIP information.
no debug rip nsm		Disables RIP nsm debugging.
no debug rip packet [**recv** | **send**]		Disables a debugging of RIP packets.
no debug rip packet [**recv** | **send**] **detail**		

To display the debugging information, use the following command.

Command	Mode	Description
show debugging rip	Enable Global Bridge	Shows the debugging information of RIP.

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. Optionally, FEC coding and AES encryption are applied to the user data.

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.

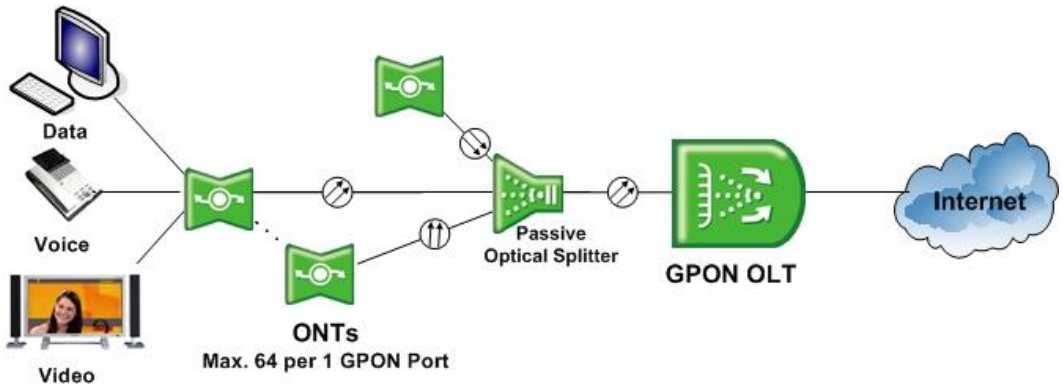


Fig. 11.1 Example of GPON Network

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* such as **1**, **2**, **3**, **4**. 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 64. Multiple input for the ONU ID is the same as the ONU ID, e.g. **1-3**, **8-22**.

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 Profile Configuration* mode to configure an ONU profile or *GPON-OLT Configuration* mode to configure OLT.

Fig. 11.2 shows the CLI structure of *GPON Configuration* mode.

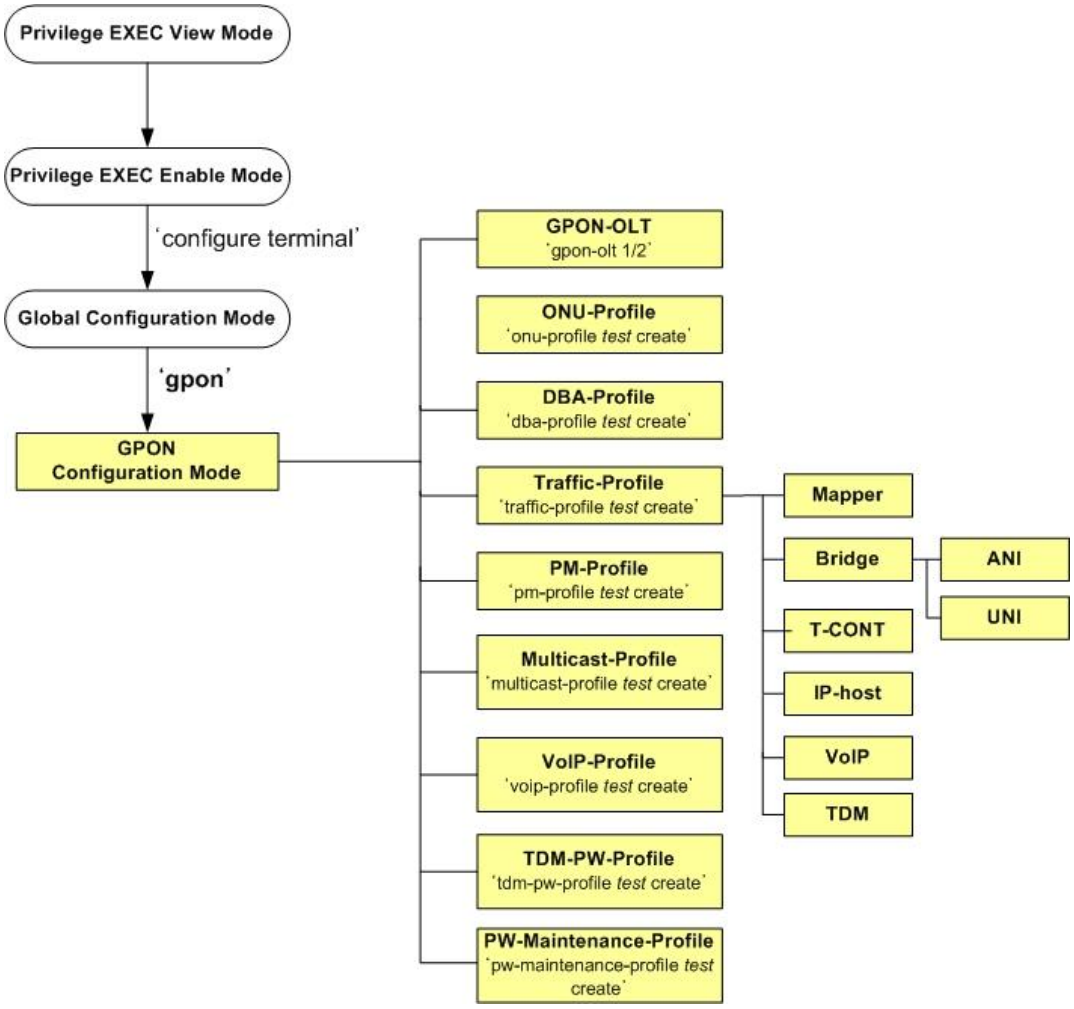


Fig. 11.2 CLI Structure of *GPON Configuration* Mode

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
  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

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	GPON-OLT	Shows the OLT's description.

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

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.

Encryption of downstream data uses AES algorithm with a key generated by each ONU (ONT) and configured by GPON OLT. 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 64) 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 <10-86400>	GPON-OLT	Starts an encryption key exchange process between OLT and ONU and specifies an exchange interval. 10-86400: 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 [*ONU-ID*]	GPON-OLT	Shows the status of encryption mode. ONU-ID: ONU ID (1 to 64) or ONU serial number
show olt key-exchange		Shows the configured interval and the encryption key exchange process information.

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	GPON-OLT	Shows the total upstream bandwidth of 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*]	GPON	Shows the status of OLT's bandwidth scheduler.
show olt bw-scheduler	GPON-OLT	

11.1.4 OLT Optical Transceiver Parameter

To set an optical transceiver parameter, use the following command.

Command	Mode	Description
olt optic-param default	GPON-OLT	Set a default optic module parameter.
olt optic-param user1		Set an user1 optic module parameter.

To display the status of OLT's optic module parameter, use the following command.

Command	Mode	Description
show olt optic-param [*OLT-ID*]	GPON GPON-OLT	Shows the status of OLT's optic module parameter.

11.1.5 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 V5812G 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 V5812G 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 V5812G 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 it tries to enable its laser, the V5812G 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	GPON-OLT	Shows a current configuration of the auto ONU (ONT) fault detection.

11.1.6 Maximal Distance between OLT and ONU (ONT)

PON systems distribute the bandwidth of each fiber core among up to 64 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>		

11.1.7 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.

11.1.8 MAC Aging Time

To manage a MAC table in the OLT system, use the following command.

Command	Mode	Description
olt mac aging-time <30-2147480>	GPON-OLT	Specifies MAC aging time. 30-2147480: aging time (default: 300s)

11.1.9 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 V5812G 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	GPON	Shows the configuration of GPON link down detection.

11.1.10 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 <1-64>	GPON-OLT	Sets the maximum number of ONU connections. 1-64: maximum number of ONUs connected to a specified OLT (default: 64)
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*]	GPON	Shows the configured maximum number of ONUs.
show olt max-onu-count	GPON-OLT	

11.1.11 OLT Anti-Spoofing

When the V5812G 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 V5812G 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. ONU-ID: ONU ID (1-64) or serial number MAC: MAC address VID: VID
clear olt anti-spoofing *ONU-ID* [*MAC VID*]		

To display the user configuration of the OLT anti-spoofing, use the following command.

Command	Mode	Description
show olt anti-spoofing [*OLT-ID*]	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	GPON-OLT	Shows the current anti-spoofing MAC filtering status per ONU, MAC and VID.

11.1.12 Displaying OLT Information

To display GPON OLT information, use the following command.

Command	Mode	Description
show olt status [*OLT-ID*]	GPON GPON-OLT	Shows the information of active/inactive GPON OLT IDs.

The following is an example of displaying active/inactive OLT IDs of V5812G.

```
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)#
```

11.1.12.1 OLT Traffic Statistics

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

Command	Mode	Description
show olt statistics	GPON-OLT	Shows traffic statistics of an OLT.
show olt statistics onu *ONU-IDs*		Shows traffic statistics of a specified ONU (ONT) collected by an OLT.
show olt statistics activation		Shows traffic statistics of GPON activation data.

The following is an example of displaying traffic statistics of the OLT 2.

```
SWITCH(config-gpon-olt[2])# show olt statistics
--------------------------------------------------------------------------------
 OLT :   2                              Downstream            Upstream
--------------------------------------------------------------------------------
 (Pon counter)
 Pon valid eth packets                       0                N/A
 Pon CPU packets                             0                N/A
 Pon ploams                                  0                  0
 Pon invalid packets                       N/A                  0
 (perfomance monitoring counter)
 Rx valid packets                        17823                N/A
 Rx error packets                            0                N/A
 CPU valid packets                           0                  0
 CPU dropped packets                         0                    0
 MAC lookup miss                             0                N/A
 Priority Q0 forwarded packets           17823                  0
 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
 Priority Q3 dropped packets                 0                  0
 Priority Q4 forwarded packets               0                  0
 Priority Q4 dropped packets                 0                  0
 Priority Q5 forwarded packets               0                  0
 Priority Q5 dropped packets                 0                  0
 Priority Q6 forwarded packets               0                  0
 Priority Q6 dropped packets                 0                  0
 Priority Q7 forwarded packets               0                  0
 Priority Q7 dropped packets                 0                  0
 CRC dropped packets                       N/A                  0
 security dropped packets                  N/A                  0
 security learn failures                   N/A                  0

 header modifier forwarded packets           0                N/A
 header modifier dropped packets         17823                N/A
SWITCH(config-gpon-olt[2])#
```

To clear collected statistics, use the following command.

Command	Mode	Description
clear olt statistics	GPON-OLT	Clears collected traffic statistics of an OLT.
clear olt statistics activation		Clears the collected traffic statistics of GPON activation data.

11.1.12.2 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	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 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 (1-64) or serial number
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

11.1.12.3 OLT Slot Information

To display the slot information of running SIUs as GPON OLT, use the following command.

Command	Mode	Description
show gpon slot-status	GPON	Shows GPON slot information in a chassis.

11.1.12.4 GPON Daemon Memory Usage

To display the memory usage of GPON or GPON OLT daemon, use the following command.

Command	Mode	Description
show memory gpon	Enable	Shows the memory usage of GPON daemon.
show memory gpon-olt		Shows the memory usage of GPON OLT daemon.

11.1.12.5 OLT Rx Power

Even if ONU's transmitting power is constant, the Rx power on OLT may be not even for a certain reason.

To display the OLT Rx power, use the following command.

Command	Mode	Description
show olt rxpower [*ONU-ID*]	GPON-OLT	Shows OLT Rx power. ONU-ID: ONU ID (1-64) or serial number

11.2 ONU Management

This section describes how to manage an ONU (ONT). The V5812G provides the centralized remote ONU (ONT) management concept, so you can manage every remote ONU (ONT) connected to the V5812G 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 V5812G is able to register ONU (ONT) automatically and manually.

- By default, the V5812G 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 Serial Number-based ONU (ONT) 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. V5812G 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		Shows the configured interval for requesting ONU's serial number.

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 64) 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*]	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 64) or ONU serial number

11.2.1.6 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 64) 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 [*ONU-ID*]	GPON-OLT	Shows the ONU's description.

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 64) 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.

i For the details of how to create and configure the IP host service, see 11.5.5 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 assigned IP address on ONU, use the following command.

Command	Mode	Description
show onu ip-host *ONU-ID*	GPON-OLT	Shows the assigned IP address on ONU. ONU-ID: ONU ID (1 to 64) or ONU serial number

The **show onu ip-host** command is useful when you check the assigned IP address on ONU especially in case of DHCP assignment.

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**} *UNI-PORTs* {**enable** | **disable**}	GPON-OLT	Enables/disables the administration of UNI port on the specified ONU. ONU-ID: ONU ID (1 to 64) or ONU serial number eth/pots/ces/virtual-eth/video: Ethernet / POTS / CES / virtual Ethernet / video UNI-PORT: UNI port number

To see the admin status of the ONU (ONT) UNI, use **show onu uni-status** command. (See 11.2.11 Displaying ONU Information)

11.2.4 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-ID*	GPON-OLT	Resets a specified ONU. ONU-ID: ONU ID (1 to 64) or ONU serial number

11.2.5 Forward Error Correction (FEC) Mode

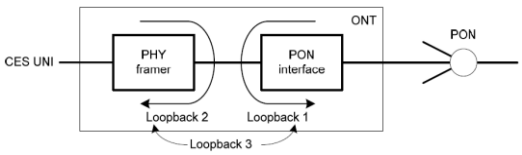
To enable/disable FEC mode for ONU ID, use the following command.

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.

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 11.1.7 Forward Error Correction (FEC) Mode.

11.2.6 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 64) 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 64) 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) 

To see the status of the ONU (ONT) UNI, use **show onu uni-status** command. (See 11.2.11 Displaying ONU Information)

11.2.7 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: 1-64 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.

11.2.8 Source MAC address Monitoring

The V5812G 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*]	GPON	Shows the configured source MAC address monitoring for OLT.
show olt srcmac-monitor	GPON-OLT	

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: 1-64 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 V5812G 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: 1-64 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.

To display VoIP service and VoIP line status information, use the following command.

Command	Mode	Description
show onu voip line *ONU-ID*	GPON-OLT	Shows the information of VoIP service and line status. ONU-ID: 1-64 or ONU serial number

11.2.10 ONU Firmware Upgrade

The V5812G 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.

11.2.10.1 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**	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 (1-64) or ONU serial number FILE_NAME: ONU firmware name

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 (1-64) or ONU serial number
show onu firmware version [*ONU-IDs*]	GPON-OLT	Shows the status of ONU firmware. ONU-ID: ONU ID (1-64) 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 (1-64) or ONU serial number
show onu firmware version [*ONU-IDs*]	GPON-OLT	Shows the status of ONU firmware. ONU-ID: ONU ID (1-64) 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 64) or ONU serial number

11.2.10.2 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*	GPON-OLT	Upgrades an ONU (ONT) with a specified firmware. ONU-ID: ONU ID (1-64) or ONU serial number FILENAME: firmware file name

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.

It may take about 10 minutes to upgrade the firmware of ONU (ONT).

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 (1-64) or ONU serial number
show onu firmware version [*ONU-IDs*]	GPON-OLT	Shows the status of ONU firmware. ONU-ID: ONU ID (1-64) 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 64) or ONU serial number

11.2.10.3 Auto Upgrade

For efficient system maintenance, the V5812G 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	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_DALLAS_22_0_8_33.bin |  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	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 11.2.11 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 {<0-23> | **immediately**}	GPON	Specifies the time that the upgrade-completed ONU restarts. 0-23: restart time (unit: o'clock)
onu auto-upgrade reboot-time 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**}	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	GPON GPON-OLT	Shows a progress of ONU auto-upgrade.
show onu auto-upgrade model-list [*NAME*]	GPON-OLT	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
 ------------------------------------------------------------------------------
   1  |  enable |    Upgrade ONU Progress |      enable  |    enable
   2  | disable |    Upgrade ONU Progress |      enable  |    enable


SWITCH(config-gpon-olt[1])# 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
 ------------------------------------------------------------------------------
   1  |  enable |    Upgrade ONU Progress |      enable  |    enable


SWITCH(config-gpon-olt[1])# show onu auto-upgrade model-list
 ------------------------------------------------------------------------------
  OLT | ONU |     Model    |   Upgrade Status     | Fail-CNT |        Active
 ------------------------------------------------------------------------------
```

```
  1  |  1 |       H645 |              -     |       0 |          22.0.8.26
SWITCH(config-gpon-olt[1])#
```

To display the firmware for ONU auto-upgrade, use the following command.

Command	Mode	Description
show onu auto-upgrade firmware	GPON	Shows the firmware information of auto-upgraded ONU.
show onu auto-upgrade current-fw	GPON-OLT	Shows the firmware to be auto-upgraded currently.

The following is an example of displaying the firmware for ONU auto-upgrade.

```
SWITCH(config-gpon-olt[1])# show onu auto-upgrade current-fw
Current Firmware : G_ONU_DALLAS_22_0_8_33.bin

SWITCH(gpon)# show onu auto-upgrade firmware
 ------------------------------------------------------------------------------
      Model    |         Firmware Name        |    Version    |      Status
 ------------------------------------------------------------------------------
      H645     |    G_ONU_DALLAS_22_0_8_33.bin |  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 (1-64) or ONU serial number
show onu firmware version [*ONU-IDs*]	GPON-OLT	Shows the status of ONU firmware. ONU-ID: ONU ID (1-64) 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 64) or ONU serial number

11.2.11 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*]	GPON	Shows the ONU (ONT) information in detail. OLT-ID: GPON OLT port number ONU-ID: ONU ID (1 to 64) or ONU serial number
show onu detail-info [*ONU-ID*]	GPON-OLT	
show onu info [*ONU-ID*]		Shows the ONU (ONT) information.

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 [*ONU-ID*]	GPON-OLT	Shows the registered ONU (ONT) information. ONU-ID: ONU ID (1 to 64) or ONU serial number
show onu active count		Show the number of active ONUs.

The following is the sample output of displaying the ONUs connected to the OLT 2.

```
SWITCH(config-gpon-olt[2])# show onu active
-------------------------------------------------------------------------------
 OLT | ONU |  STATUS  |  MODE  |  Serial No.  |      Password      |  Link uptime
-------------------------------------------------------------------------------
 2   |   1 | Inactive | manual | CIGG09140025 | 00000000000000000000 | 00:00:00
 2   |   2 | Inactive | manual | DSNWcb002829 | 00000000000000000000 | 00:00:00
 2   |   3 | Inactive | manual | CIGG09140017 | 00000000000000000000 | 00:00:00
 2   |   4 | Inactive | manual | CIGG92500094 | 00000000000000000000 | 00:00:00
 2   |   5 |   Active |   auto | DSNWcb00282d | 00000000000000000000 | 00:03:34
SWITCH(config-gpon-olt[2])#
```

To display the link status of ONUs, use the following command.

Command	Mode	Description
show onu block status *OLT-ID* [*ONU-ID*]	GPON	Shows the link status of ONUs OLT-ID: GPON port number ONU-ID: ONU ID (1 to 64) 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	GPON-OLT	Shows the reason of inactive ONUs. ONU-ID: ONU ID (1 to 64) or ONU serial number

To display the model names of the ONUs connected to a specified OLT, use the following command.

Command	Mode	Description
show onu model-name [*ONU-ID*]	GPON-OLT	Shows the model names of the ONUs. ONU-ID: ONU ID (1 to 64) or ONU serial number

To display the number of MAC addresses currently learned in an ONU, use the following command.

Command	Mode	Description
show onu mac-address [*ONU-ID*]	GPON-OLT	Shows the number of MAC addresses currently learned in ONUs connected to a current OLT.

The following is the sample output of displaying the MAC addresses of ONUs connected to the OLT 2.

```
SWITCH(config-gpon-olt[2])# show onu mac-address
--------------------------------
 OLT | ONU |       MAC
--------------------------------
  2  |   1 | 00:00:00:00:00:00
  2  |   2 | 00:19:c7:03:2c:d7
SWITCH(config-gpon-olt[2])#
```

To display a host name of the specified ONU, use the following command.

Command	Mode	Description
show onu hostname [*ONU-IDs*]	GPON-OLT	Shows a host name of the specified ONU.

To display the IGMP group list of ONU (ONT), use the following command.

Command	Mode	Description
show onu igmp-group-list *ONU-ID*	GPON-OLT	Shows the current IGMP group list of the ONU. ONU-ID: ONU ID (1 to 64) or ONU serial number

To display the status of the ONU (ONT) UNI, use the following command.

Command	Mode	Description
show onu uni-status [*OLT-ID*]	GPON	Shows the status of the ONU UNI. ONU-ID: ONU ID (1 to 64) or ONU serial number
show onu uni-status [*ONU-IDs*]	GPON-OLT	

To display the assigned IP address on ONU, use the following command.

Command	Mode	Description
show onu ip-host *ONU-ID*	GPON-OLT	Shows the assigned IP address on ONU. ONU-ID: ONU ID (1 to 64) or ONU serial number

The **show onu ip-host** command is useful when you check the assigned IP address on ONU especially in case of DHCP assignment.

11.3 ONU Profile

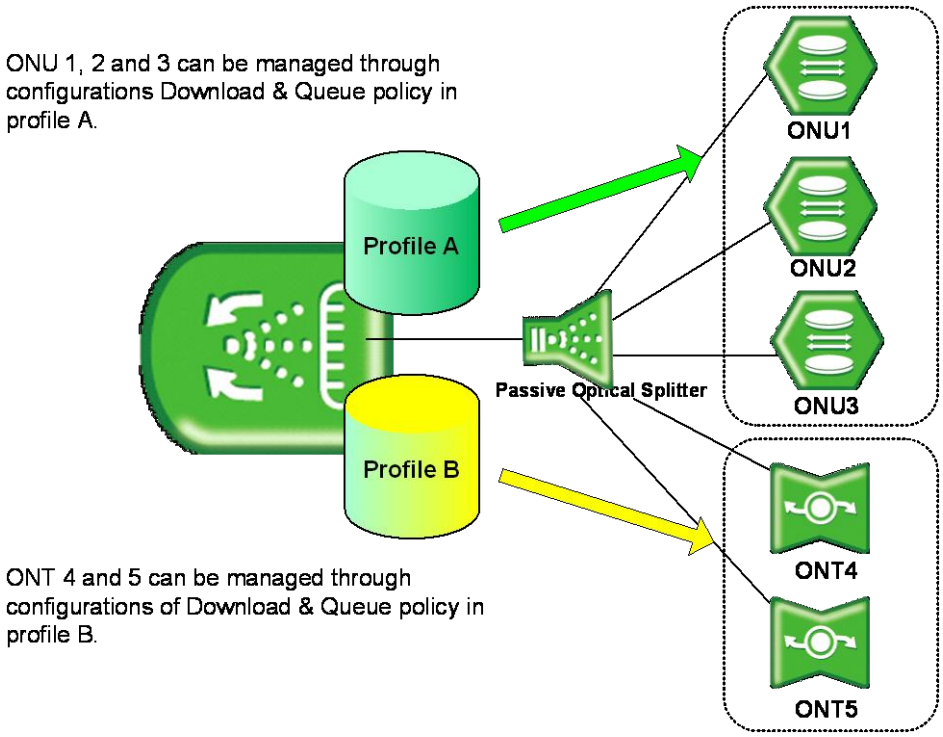


Fig. 11.3 ONU Profile

The V5812G 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 the 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*	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* }	ONU-Profile	Sets the RX optical power threshold and sends RX power high/low alarm to OLT when the RX power exeeds 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 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.



For the details of how to create and configure the traffic profile, see 11.5 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 *NAME*		Removes the PM profile from ONU profile.



For the details of how to create and configure the PM profile, see 11.9 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** *SIR_BANDWIDTH* [*PIR_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 11.2.11 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.

i If you modify a running ONU profile, you also need to use the **apply** command to apply the changes to ONUs (ONTs). If you do not, it will not be applied.

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.

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 64) 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 64) 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 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 cofiguration 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[2])# show onu status
------------------------------------------------------------------------
  OLT | ONU |  ACTIVE  |    Fail Reason     | Profile Name
------------------------------------------------------------------------
   2  |  1  |  Active  |          Success | H640V
```

11.3.7 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*	GPON	Shows the list of ONUs (ONTs) where an ONU profile is applied. NAME: ONU profile name

11.4 DBA Profile

You need to open *DBA Profile Configuration* mode to set the bandwidth allocation and ONU status reporting mode.

11.4.1 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*		Deletes a DBA profile.
dba-profile *PROFILE* **modify**		Modifies the configured DBA profile.

11.4.2 Configuring DBA Profile

If the V5812G 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 <128-1031616>		Sets a bandwidth. 128-1031616: 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.

$$\text{Maximum B/W} \geq \text{fixed B/W} + \text{assured B/W}$$

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.

11.4.3 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.

11.4.4 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.

11.5 Traffic Profile

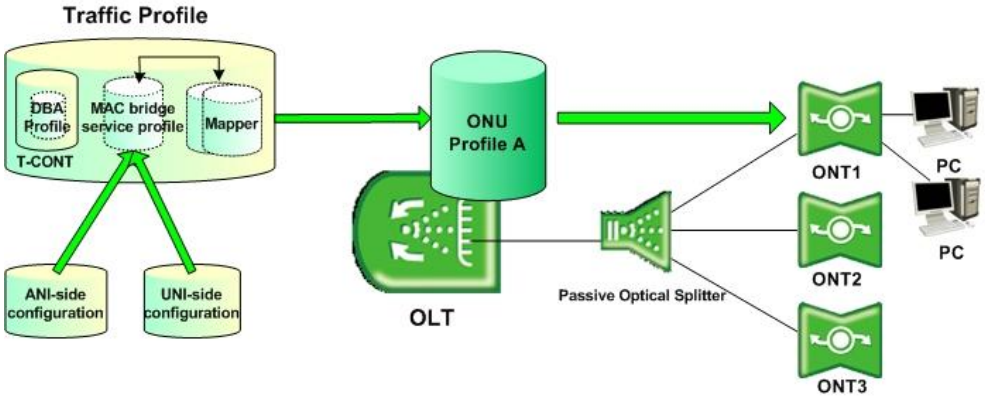


Fig. 11.4 Traffic Profile

The V5812G 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 V5812G 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.

11.5.1 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*	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).

11.5.2 Creating a Mapper

A mapper provides support for upstream flow routing based on 802.1p priority bits. The V5812G 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 4, 802.1p mapper ID
no mapper *MAPPER_ID*		Removes the created mapper from the traffic profile

i V5812G 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.

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.

11.5.3 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 4, 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

11.5.3.1 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.

11.5.3.2 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)

11.5.3.3 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.

11.5.3.4 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 4
no ani mapper *MAPPER_ID*		Disconnects a mapper 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)
no vlan-filter		Disables the VLAN tagging filtering function.

11.5.3.5 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 the UNI-side port discard: blocks the untagged frames to the UNI-side port 1-4094: VLAN ID(s)
no vlan-filter		Disables the VLAN tagging filtering function.

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**} *SIR_BANDWIDTH PIR_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.

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.

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.

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.

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.



To see the admin status of the ONU (ONT) UNI, use **show onu uni-status** command. (See 11.2.11 Displaying ONU Information)

11.5.3.6 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
no link ip-host-config *SERVICE-ID*		Disconnects the linked IP-host service.

For the details of how to create and configure the IP-host service, see 11.5.5 IP Host Service Configuration.

11.5.3.7 TDM Service Link

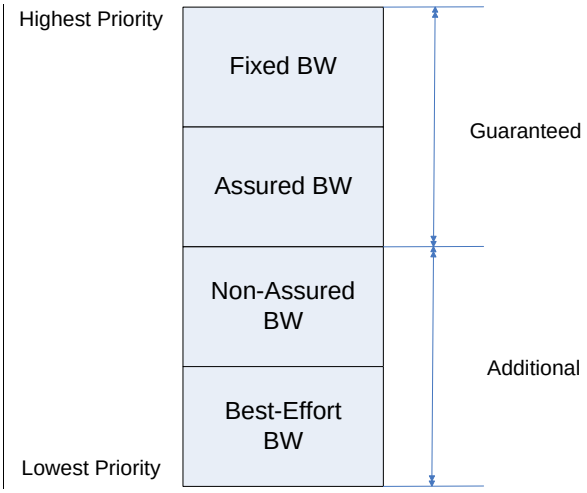
To link a TDM service to MAC bridge service profile, use the following command.

Command	Mode	Description
link tdm-service *SERVICE_ID*	Traffic-Bridge	Links a TDM service to MAC bridge service profile. SERVICE_ID: TDM service ID
no link tdm-service *SERVICE_ID*		Disconnects the linked TDM service.

For the details of how to create and configure the TDM service, see 11.5.7 TDM Service Configuration (CES UNI).

11.5.4 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. The mechanism of T-CONT is shown in Fig. 11.5.



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. 11.5 Priority of T-CONT types

The V5812G 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 16

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.

11.5.4.1 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.

11.5.4.2 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*]	GPON	Shows the information of T-CONT ID of OLT.
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 being currently configured for the profile. The user can see the current profile configuration before applying it by **apply** command.

11.5.5 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.
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*])#.

11.5.5.1 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.

11.5.5.2 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.
no dns		Deletes the configured DNS IP address.

11.5.5.3 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.

11.5.5.4 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 *VLANS* **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 VLANS: VLAN ID(s) (1-4094)
no vlan-filter		Disables the VLAN tagging filtering function.

11.5.5.5 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
no link voip-service *SERVICE_ID*		Disconnects the linked VoIP service.



For the details of how to create and configure the VoIP service, see 11.5.6 VoIP Service Configuration (POTS UNI).

11.5.5.6 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
no link tdm-service *SERVICE_ID*		Disconnects the linked TDM service.



For the details of how to create and configure the TDM service, see 11.5.7 TDM Service Configuration (CES UNI).

11.5.6 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.
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*])#.

11.5.6.1 VoIP Service Management Mode

The V5812G 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.

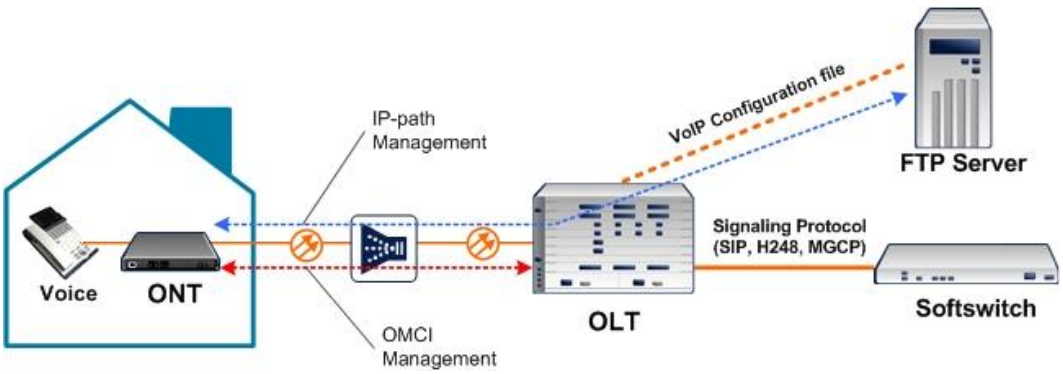


Fig. 11.6 VoIP Service Architecture

V5812G 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.

11.5.6.2 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.



For the details of how to create and configure the VoIP profile, see 11.6 VoIP Profile.

11.5.6.3 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.



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 V5812G 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** }	Traffic VoIP-IP-path	Specifies the protocol on the current VoIP service. sip: Session Initiation Protocol h248: Media Gateway Control protocol (MEGACO) (future release)

11.5.6.4 POTS UNI Configuration

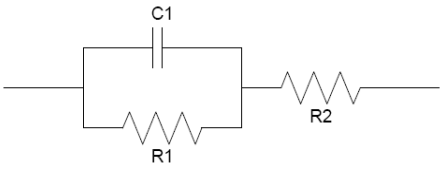
To configure the user network interface, use the following command.

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))

11.5.6.5 UDP/TOS Configuration

To perform the configuration for UDP-based service that are 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 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)

11.5.7 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: TDM port number
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*])#.

11.5.7.1 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")

11.5.7.2 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)

11.5.7.3 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

11.5.7.4 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)
line-length power-feed ds1-power-short line-length { **133** | **266** | **399** | **533** | **655** }		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)
line-length power-feed ds1-power-long line-length { **0** | **7_5** | **15** | **22_5** }		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 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.

11.5.7.5 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.

11.5.7.6 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)

11.5.7.7 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 11.7 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 UDP-based service that are 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 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)

11.5.7.8 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 *ONU-ID*	GPON-OLT	Shows the list of source MAC addresses for TDM pseudowire of the specified ONU.

11.5.8 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.

11.5.9 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.

11.5.10 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	All modes of Traffic-profile	Shows the information being currently configured for the profile. The user can see the current profile configuration before applying it by **apply** command.

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 64)

11.5.11 Sample Configuration

For the sample configuration, see “Configuration Example 1” in 11.13 Sample Configuration.

11.6 VoIP Profile

11.6.1 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 V5812G if the ONT has POTS terminations and if OLT is to be used to remotely manage and provide the VoIP service.

11.6.1.1 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

11.6.1.2 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.

11.6.1.3 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.

11.6.1.4 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 11.6.1.2 VoIP Media Configuration.)

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)

11.6.1.5 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.

11.6.1.6 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.

11.6.1.7 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.

11.6.2 OMCI-based SIP Configuration

If the ONUs are fully provisioned and managed from the V5812G 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.



To enter the H248 protocol mode, use **protocol h248** command. However, the configuration for the H248 protocol is not yet supported.

11.6.2.1 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.

11.6.2.2 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.

11.6.2.3 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		

11.6.2.4 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)

11.6.2.5 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.

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.

In order to see the configured dial plan, use **show voip-profile** command.

11.6.3 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.

Whenever you modify a VoIP profile, you should apply the changes again using the **apply** command. If not, the changes will not be applied.

11.6.4 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*]	GPON	Shows the information of VoIP service and line status. OLT-ID: OLT ID
show onu voip line [*ONU-IDs*]	GPON-OLT	Shows the information of VoIP service and line status. ONU-ID: 1-64 or ONU serial number

11.6.5 Sample Configuration

For the sample configuration, see “Configuration Example 1” in 11.13 Sample Configuration.

11.7 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.

11.7.1 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*	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

11.7.2 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)

11.7.3 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

11.7.4 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.

11.7.5 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.

11.7.6 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

11.7.7 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.

11.7.7.1 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)

11.7.7.2 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

11.7.7.3 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.

11.7.7.4 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.

11.7.8 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.



For the details of how to create and configure the pseudowire maintenance profile, see 11.8 Pseudowire Maintenance Profile.

11.7.9 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.



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.

11.7.10 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 *ONU-ID*	GPON-OLT	Shows the list of source MAC addresses for TDM pseudowire of the specified ONU.

11.8 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.

11.8.1 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*	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

11.8.2 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.

11.8.3 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.

11.8.4 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.

11.8.5 Alarm-related Policy

V5812G 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 malformed-packet: malformed packet misconnect-packet: misconnect packet 1-100: anomaly rate (unit: integer percentage)
loss-packet-declaration-policy <1-100>		
malformed-packet-declaration-policy <1-100>		
misconnect-packet-declaration-policy <1-100>		
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		

11.8.6 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

11.8.7 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.

11.8.8 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.

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.

11.8.9 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

11.9 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.

11.9.1 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*	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.

11.9.2 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.

11.9.3 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 If you modify a running PM profile, you also need to use the **apply** command to apply the changes to ONUs (ONTs). If you do not, it will not be applied.

11.9.4 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

11.9.5 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*]	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 [*ONU-ID*]		Shows the information of GEM port counters collected via PM profile. (15 Min, Prev_15 Min, total)
show onu statistics current [*ONU-ID*]		Shows the information of current ONU counters collected via PM profile. (current counter, total + current counter)
show onu statistics avg-pkt [*ONU-ID*]		Shows the information of ONU counter (average packets) collected via PM profile.
show onu statistics {**pre_15** | **hour** | **day** | **total**} *ONU-ID* {**eth** *PORT* {**us** | **ds**} | **pots** *PORT* | **tdm** *PORT* | **pw** *NUMBER* | **gem** *PORT* | **ani** *PORT* }		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

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.

11.9.6 Sample Configuration

For the sample configuration, see “Configuration Example 2” in 11.13 Sample Configuration.

11.10 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

11.10.1 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*	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

11.10.2 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 <1-3600>		Specifies a general query interval. 1-3600: query interval (default: 125 seconds)
igmp querier max-response-time <1-25>		Specifies a maximum query response time. 1-25: 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*]		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*]		
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 upstream rate-limit <1-65535>		Configures the rate limit of upstream IGMP traffic 1-65535: IGMP message count (message/second)

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 upstream rate-limit		

11.10.3 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.

11.10.4 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.

11.10.5 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 ONU Service Profile

V5812G 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 V5812G 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	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*		

To display the service ONU profile from all ONUs(ONTs), use the following command.

Command	Mode	Description
show olt service-profile	GPON	Shows the configured service ONU profiles.

11.12 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** }	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
no debug gpon {**all** | **func** | **db** | **comm** | **ugrd** | **profile** | **queue** | **statistics** }		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 debug gpon	GPON	Shows the debugging status of GPON.

11.13 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 V5812G 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 V5812G 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! For more information, see Section 4.1.8.1.

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 : V5812G.4.80.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     4.80
 OS2                       16777216      13661428       3115788     3.04
 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                 *
*                       Dasan Networks                     *
*                                                          *
************************************************************
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         = 00:d0:cb: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 V5812G 4.80.x
TFTP from server 10.27.41.82; our IP address is 10.27.41.83
Filename 'V5812G.4.80.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        *             *         4.80
os2       13661412                                3.04

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 V5812G 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 V5812G 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 V5812G. 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! For more information, see Section 4.1.8.1.

The following is an example of upgrading the system software of the V5812G 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 V5812G.4.80.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. For more information, see Section 6.1.11.

12.4 ONU Upgrade

The V5812G 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.

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 <1-64> *FILENAME*	GPON-OLT	Upgrades an ONU with a specified firmware. FILENAME: firmware file name

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: 1-64

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 V5812G 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 V5812G 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.

13 Abbreviations

ACL	Access Control List
AES	Advanced Encryption Standard
ARP	Address Resolution Protocol
ASM	Any Source Multicast
BGP	Border Gateway Protocol
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
OAM	Operation, Administration and Maintenance
OIF	Outgoing Interface
OLT	Optical Line Termination
ONT	Optical Network Terminal
OS	Operating System
OSPF	Open Shortest Path First
PC	Personal Computer
PDU	Protocol Data Unit
PIM-DM	Protocol Independent - Multicast Dense Mode
PIM-SM	Protocol Independent - Multicast Sparse Mode
PIM-SSM	Protocol Independent - Multicast Source-Specific Multicast
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
RIP	Routing Information Protocol
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

Artisan Technology Group is an independent supplier of quality pre-owned equipment

Gold-standard solutions

Extend the life of your critical industrial, commercial, and military systems with our superior service and support.

We buy equipment

Planning to upgrade your current equipment? Have surplus equipment taking up shelf space? We'll give it a new home.

Learn more!

Visit us at **artisantg.com** for more info on price quotes, drivers, technical specifications, manuals, and documentation.

Artisan Scientific Corporation dba Artisan Technology Group is not an affiliate, representative, or authorized distributor for any manufacturer listed herein.

We're here to make your life easier. How can we help you today?

(217) 352-9330 | sales@artisantg.com | artisantg.com

ARTISAN® TECHNOLOGY GROUP