Yamaha L3 Switch

Standard L3 SWX3220 Series

Command Reference

Rev.4.02.22 / Rev.4.03.06 / Rev.4.04.06

Contents

Preface: Introduction 21

Chapter 1: How to read the command reference 22
1.1 Applicable firmware revision 22
1.2 How to read the command reference 22
1.3 Interface names 22
1.4 Input syntax for commands starting with the word "no" 23

Chapter 2: How to use the commands 24
2.1 Operation via console 24
2.1.1 Access from a console terminal 24
2.1.2 Access from a TELNET client 24
2.1.3 Access from an SSH client 25
2.1.4 Console terminal/VTY settings 25
2.2 Operation via configuration (config) files 26
2.2.1 Access from a TFTP client 26
2.2.2 Reading/writing a configuration file 26
2.3 Login 27
2.4 Command input mode 28
2.4.1 Command input mode basics 28
2.4.2 individual configuration mode 29
2.4.3 Command prompt prefix 30
2.4.4 Executing commands of a different input mode 30
2.5 Keyboard operations when using the console 30
2.5.1 Basic operations for console input 30
2.5.2 Command help 31
2.5.3 Input command completion and keyword candidate list display 31
2.5.4 Entering command abbreviations 31
2.5.5 Command history 31
2.6 Commands that start with the word "show" 32
2.6.1 Modifiers 32

Chapter 3: Configuration 33
3.1 Manage setting values 33
3.2 Default value 33
3.3 Preset 36

Chapter 4: Maintenance and operation functions 38
4.1 Passwords 38
4.1.1 Set privileged password 38
4.1.2 Encrypt password 38
4.2 User account maintenance 39
4.2.1 Set user 39
4.2.2 Changing User Permissions 40
4.2.3 Show login user information 41
4.2.4 Set banner 42
4.3 Configuration management 43
4.3.1 Save running configuration 43
4.3.2 Save running configuration 43
4.3.3 Show the running configuration 44
4.3.4 Show startup configuration 45
4.3.5 Erase startup configuration 46
4.3.6 Copy startup configuration 46
4.3.7 Select startup config 47

4.3.8 Set description for startup config.... 47
4.4 Manage boot information.... 48
4.4.1 Show boot information.... 48
4.4.2 Clear boot information.... 48
4.4.3 Set SD card boot.... 49
4.4.4 Configuring the SD card boot auto-apply function.... 49
4.4.5 Show the SD card boot setting information.... 50
4.5 Show unit information.... 50
4.5.1 Show inventory information.... 50
4.5.2 Show operating information.... 50
4.5.3 Disk usage status.... 52
4.5.4 Show currently-executing processes.... 52
4.5.5 Display memory usage.... 52
4.5.6 Show technical support information.... 53
4.5.7 Save technical support information.... 56
4.5.8 Show fan operating history.... 57
4.5.9 Show power supply unit information.... 57
4.6 System self-diagnostics.... 58
4.6.1 Showing system self-diagnostics results.... 58
4.6.2 Executing on-demand diagnostics.... 59
4.6.3 Clearing the on-demand diagnostics results.... 59
4.7 Cable diagnostics.... 60
4.7.1 Execute cable diagnostics.... 60
4.7.2 Clear cable diagnostic results.... 60
4.7.3 Display cable diagnostic results.... 60
4.8 Time management.... 61
4.8.1 Set clock manually.... 61
4.8.2 Set time zone.... 61
4.8.3 Configuring daylight saving time (recurring).... 63
4.8.4 Configuring daylight saving time (by date).... 63
4.8.5 Show current time.... 64
4.8.6 Set NTP server.... 65
4.8.7 Synchronize time from NTP server (one-shot update).... 66
4.8.8 Synchronize time from NTP server (update interval).... 66
4.8.9 Show NTP server time synchronization settings.... 66
4.9 Time synchronization.... 67
4.9.1 PTP function settings (system).... 67
4.9.2 Set PTP function (interface).... 67
4.9.3 PTP operation mode settings.... 68
4.9.4 Forwarding protocol settings for PTP messages.... 69
4.9.5 Set PTP clock domain number.... 70
4.9.6 Set PTP clock priority 1.... 70
4.9.7 Set PTP clock priority 2.... 71
4.9.8 Set PTP message transmission interval.... 71
4.9.9 Set receive timeout for PTP announce messages.... 72
4.9.10 Set PTP sync message transmission interval.... 72
4.9.11 Set PTP delay-request message transmission interval.... 73
4.9.12 Specify VLAN for transmitting/receiving PTP messages.... 74
4.9.13 Show PTP setting status.... 75
4.9.14 Show PTP setting information for the interface.... 75
4.9.15 Show PTP clock information.... 76
4.9.16 Show clock information for the PTP interface.... 77
4.9.17 Show PTP statistical information.... 78
4.9.18 Set Sync-E input port.... 79
4.10 Terminal settings.... 79
4.10.1 Move to line mode (console terminal).... 79
4.10.2 Set VTY port and move to line mode (VTY port).... 80
4.10.3 Set terminal login timeout.... 80
4.10.4 Change the number of lines displayed per page for the terminal in use.... 81
4.10.5 Set the number of lines displayed per page on the terminal.... 81
4.10.6 Changing the serial baud rate.... 82
4.11 Management.... 82
4.11.1 Set management VLAN.... 82
4.12 SYSLOG.... 83
4.12.1 Set log notification destination (SYSLOG server).... 83

4.12.2 Setting the notification format of the log.... 83
4.12.3 Setting the log facility value.... 84
4.12.4 Set log output level (debug).... 84
4.12.5 Set log output level (informational).... 85
4.12.6 Set log output level (error).... 85
4.12.7 Set log console output.... 85
4.12.8 Set log output in event units.... 86
4.12.9 Back up log.... 86
4.12.10 Set log backup to SD card.... 87
4.12.11 Clear log.... 87
4.12.12 Show log.... 87
4.13 SNMP.... 88
4.13.1 Set host that receives SNMP notifications.... 88
4.13.2 Setting the time to wait before sending a notification message at system boot.... 89
4.13.3 Set notification type to transmit.... 90
4.13.4 Set system contact.... 91
4.13.5 Set system location.... 91
4.13.6 Set SNMP community.... 92
4.13.7 Set SNMP view.... 92
4.13.8 Set SNMP group.... 93
4.13.9 Set SNMP user.... 94
4.13.10 IP address restrictions for clients that can access the SNMP server.... 95
4.13.11 Show SNMP community information.... 96
4.13.12 Show SNMP view settings.... 96
4.13.13 Show SNMP group settings.... 97
4.13.14 Show SNMP user settings.... 97
4.14 RMON.... 98
4.14.1 Set RMON function.... 98
4.14.2 Set RMON Ethernet statistical information group.... 98
4.14.3 Set RMON history group.... 99
4.14.4 Set RMON event group.... 100
4.14.5 Set RMON alarm group.... 101
4.14.6 Show RMON function status.... 103
4.14.7 Show RMON Ethernet statistical information group status.... 103
4.14.8 Show RMON history group status.... 104
4.14.9 Show RMON event group status.... 104
4.14.10 Show RMON alarm group status.... 105
4.14.11 Clear counters of the RMON Ethernet statistical information group.... 105
4.15 sFlow.... 106
4.15.1 Set sFlow function.... 106
4.15.2 Set sFlow agent.... 106
4.15.3 Set sFlow collector.... 107
4.15.4 Set maximum size of sFlow datagram.... 107
4.15.5 Set sampling rate of packet flow sampling.... 108
4.15.6 Set maximum Ethernet frame header size for packet flow sampling.... 108
4.15.7 Set polling interval for counter sampling.... 108
4.15.8 Show sFlow status.... 109
4.15.9 Show sFlow sampling information.... 109
4.16 Telnet server.... 110
4.16.1 Start Telnet server and change listening port number.... 110
4.16.2 Show Telnet server settings.... 111
4.16.3 Set host that can access the Telnet server.... 111
4.16.4 Restrict access to the TELNET server according to the IP address of the client.... 112
4.17 Telnet client.... 112
4.17.1 Start Telnet client.... 112
4.17.2 Enable Telnet client.... 113
4.18 TFTP server.... 113
4.18.1 Start TFTP server and change listening port number.... 113
4.18.2 Show TFTP server settings.... 114
4.18.3 Set hosts that can access the TFTP server.... 114
4.19 HTTP server.... 115
4.19.1 Start HTTP server and change listening port number.... 115
4.19.2 Start secure HTTP server and change listening port number.... 115
4.19.3 Show HTTP server settings.... 116
4.19.4 Set hosts that can access the HTTP server.... 116

4.19.5 Restrict access to the HTTP server according to the IP address of the client.... 117
4.19.6 Web GUI display language.... 118
4.19.7 Set log-in timeout time for HTTP server.... 118
4.20 HTTP Proxy.... 119
4.20.1 Enable HTTP Proxy function.... 119
4.20.2 Set HTTP Proxy function timeout.... 119
4.20.3 Show HTTP Proxy function settings.... 119
4.21 SSH server.... 120
4.21.1 Start SSH server and change listening port number.... 120
4.21.2 Show SSH server settings.... 120
4.21.3 Set host that can access the SSH server.... 121
4.21.4 Set client that can access the SSH server.... 121
4.21.5 Generate SSH server host key.... 122
4.21.6 Clear SSH server host key.... 123
4.21.7 Show SSH server public key.... 123
4.21.8 Set SSH client alive checking.... 124
4.22 SSH client.... 125
4.22.1 Start SSH client.... 125
4.22.2 Enable SSH client.... 125
4.22.3 Clear SSH host information.... 126
4.23 E-mail notification.... 126
4.23.1 SMTP e-mail server settings.... 126
4.23.2 SMTP e-mail server name settings.... 127
4.23.3 E-mail notification trigger settings.... 128
4.23.4 E-mail transmission template settings mode.... 129
4.23.5 E-mail transmission server ID settings.... 129
4.23.6 E-mail transmission source address setting.... 129
4.23.7 Destination e-mail address setting for e-mail transmission.... 130
4.23.8 Setting for subject used when sending e-mails.... 130
4.23.9 Wait time settings for e-mail transmission.... 131
4.23.10 E-mail settings when sending certificates.... 131
4.23.11 E-mail settings for certificate notification.... 132
4.23.12 Notification timing settings for expired certificates.... 132
4.23.13 Show e-mail transmission information.... 133
4.24 LLDP.... 133
4.24.1 Enable LLDP function.... 133
4.24.2 Set system description.... 134
4.24.3 Set system name.... 134
4.24.4 Create LLDP agent.... 135
4.24.5 Set automatic setting function by LLDP.... 135
4.24.6 Set LLDP transmission/reception mode.... 136
4.24.7 Set type of management address.... 136
4.24.8 Set basic management TLVs.... 137
4.24.9 Set IEEE-802.1 TLV.... 137
4.24.10 Set IEEE-802.3 TLV.... 138
4.24.11 Set LLDP-MED TLV.... 138
4.24.12 Set LLDP frame transmission interval.... 139
4.24.13 Set LLDP frame transmission interval for high speed transmission period.... 139
4.24.14 Set time from LLDP frame transmission stop until re-initialization.... 140
4.24.15 Set multiplier for calculating time to live (TTL) of device information.... 140
4.24.16 Set number of LLDP frames transmitted during the high speed transmission period.... 141
4.24.17 Set maximum number of connected devices manageable by a port.... 141
4.24.18 Global interface setting for LLDP function.... 142
4.24.19 Show interface status.... 142
4.24.20 Show information for connected devices of all interfaces.... 145
4.24.21 Clear LLDP frame counters.... 146
4.25 L2MS (Layer 2 management service) settings.... 147
4.25.1 Move to L2MS mode.... 147
4.25.2 Set L2MS function.... 147
4.25.3 Set role of L2MS function.... 147
4.25.4 Set L2MS agent watch interval.... 148
4.25.5 Set number of times that is interpreted as L2MS agent down.... 149
4.25.6 Set terminal management function.... 149
4.25.7 Set the device information acquisition time interval.... 150
4.25.8 Set L2MS control frame transmit/receive.... 150

4.25.9 Reset agent management....151
4.25.10 Show L2MS information....151
4.25.11 Show L2MS agent config information....153
4.25.12 Set the device information acquisition time interval for downstream of a wireless AP....155
4.25.13 Set event monitoring function....155
4.25.14 Set event information acquisition time interval....156
4.25.15 Set whether to use the L2MS agent's zero config function....156
4.26 Snapshot....157
4.26.1 Set snapshot function....157
4.26.2 Set whether to include terminals in the snapshot comparison....157
4.26.3 Create snapshot....158
4.26.4 Delete snapshot....158
4.27 Firmware update....158
4.27.1 Set firmware update site....158
4.27.2 Configure the HTTP proxy server used for firmware updates....159
4.27.3 Execute firmware update....160
4.27.4 Set firmware download timeout duration....160
4.27.5 Allow revision-down....161
4.27.6 Show firmware update function settings....161
4.27.7 Update firmware from SD card....162
4.27.8 Set firmware update reload time....162
4.27.9 Set reload method for firmware update of stack configuration....163
4.28 Stack....163
4.28.1 Set stack function....163
4.28.2 Changing the stack ID....164
4.28.3 Show stack information....165
4.28.4 Set range of IP addresses used by the stack port....166
4.28.5 Remote login to a member switch....166
4.29 Schedule....167
4.29.1 Schedule settings....167
4.29.2 Schedule template description text settings....169
4.29.3 Settings to enable/disable schedule template....169
4.29.4 Schedule template settings....169
4.29.5 Schedule template command execution settings....170
4.29.6 Schedule template script execution settings....171
4.30 Buzzer....171
4.30.1 Buzzer system settings....171
4.30.2 Buzzer trigger settings....172
4.30.3 Executing the buzzer check command....173
4.30.4 Mute....173
4.30.5 Unmute....174
4.30.6 Display buzzer information....174
4.31 Yamaha Network Organizer (YNO)....174
4.31.1 Set YNO agent function....174
4.31.2 Set keepalive time interval with YNO server....175
4.31.3 Set HTTPS proxy server for YNO....176
4.31.4 Unregister YNO....176
4.31.5 Show the operating status of the YNO agent....176
4.32 Yamaha Unified Network Operation Service (Y-UNOS)....177
4.32.1 Set Y-UNOS function....177
4.32.2 Show Y-UNOS information....178
4.33 General maintenance and operation functions....179
4.33.1 Set host name....179
4.33.2 Reload system....179
4.33.3 Initialize settings....180
4.33.4 Mount SD card....180
4.33.5 Unmount SD card....180
4.33.6 Set default LED mode....181
4.33.7 Show LED mode....181
4.33.8 Show port error LED status....181
4.33.9 Show DIP switches status....182
4.33.10 Starting the "Find this switch" function....182
4.33.11 Stop the “Find this switch” function....183
4.33.12 Backup system information....183
4.33.13 Restore system information....184

4.33.14 Set ProAV profile type..... 184

Chapter 5: Interface control..... 186

5.1 Interface basic settings..... 186
5.1.1 Set description..... 186
5.1.2 Shutdown..... 186
5.1.3 Set communication speed and communication mode..... 186
5.1.4 Auto negotiation type settings..... 188
5.1.5 Changing forward error correction (FEC)..... 188
5.1.6 Auto negotiation information display..... 189
5.1.7 Set MRU..... 190
5.1.8 Set cross/straight automatic detection..... 191
5.1.9 Set EEE..... 191
5.1.10 Show EEE capabilities..... 192
5.1.11 Show EEE status..... 192
5.1.12 Set port mirroring..... 193
5.1.13 Show port mirroring status..... 194
5.1.14 Show interface status..... 194
5.1.15 Show brief interface status..... 197
5.1.16 Resetting an interface..... 198
5.1.17 Show frame counter..... 199
5.1.18 Clear frame counters..... 200
5.1.19 Show SFP module status..... 201
5.1.20 Set SFP module optical reception level monitoring..... 202
5.1.21 Configuring transmission queue usage rate monitoring (system)..... 202
5.1.22 Configuring transmission queue usage rate monitoring (interface)..... 203
5.1.23 Display configuration for transmission queue usage rate monitoring..... 203
5.2 Link aggregation..... 204
5.2.1 Set static logical interface..... 204
5.2.2 Show static logical interface status..... 204
5.2.3 Set LACP logical interface..... 205
5.2.4 Show LACP logical interface status..... 206
5.2.5 Set LACP system priority order..... 208
5.2.6 Show LACP system priority..... 208
5.2.7 LACP different-speed link aggregation settings..... 209
5.2.8 Set LACP timeout..... 209
5.2.9 Clear LACP frame counters..... 210
5.2.10 Show LACP frame counter..... 210
5.2.11 Set load balance function rules..... 211
5.2.12 Show protocol status of LACP logical interface..... 212
5.2.13 Set LACP port priority order..... 214
5.3 Port authentication..... 214
5.3.1 Configuring the IEEE 802.1X authentication function for the entire system..... 214
5.3.2 Configuring the MAC authentication function for the entire system..... 215
5.3.3 Configuring the Web authentication function for the entire system..... 215
5.3.4 Set operation mode for the IEEE 802.1X authentication function..... 215
5.3.5 Set for forwarding control on an unauthenticated port for IEEE 802.1X authentication..... 216
5.3.6 Set the EAPOL packet transmission count..... 217
5.3.7 Set the MAC authentication function..... 217
5.3.8 Set MAC address format during MAC authentication..... 218
5.3.9 Configuring static registration for MAC authentication..... 218
5.3.10 Set the Web authentication function..... 219
5.3.11 Set host mode..... 220
5.3.12 Configuring the authentication order..... 220
5.3.13 Set re-authentication..... 221
5.3.14 Set dynamic VLAN..... 221
5.3.15 Set the guest VLAN..... 222
5.3.16 Suppression period settings following failed authentication..... 222
5.3.17 Set reauthentication interval..... 223
5.3.18 Set the reply wait time for the RADIUS server overall..... 223
5.3.19 Set supplicant reply wait time..... 224
5.3.20 Set RADIUS server host..... 225
5.3.21 Set the reply wait time for each RADIUS server..... 226
5.3.22 Set number of times to resend requests to RADIUS server..... 226

5.3.23 Set RADIUS server shared password....227
5.3.24 Set time of RADIUS server usage prevention....227
5.3.25 Set NAS-Identifier attribute sent to RADIUS server....227
5.3.26 Set RADIUS server authentication when no response....228
5.3.27 Show port authentication information....228
5.3.28 Show supplicant information....230
5.3.29 Show statistical information....230
5.3.30 Clear statistical information....231
5.3.31 Show RADIUS server setting information....231
5.3.32 Settings for redirect destination URL following successful Web authentication....231
5.3.33 Clear the authentication state....232
5.3.34 Setting the time for clearing the authentication state (system)....232
5.3.35 Setting the time for clearing the authentication state (interface)....233
5.3.36 Locate the file for customizing the Web authentication screen....233
5.3.37 Delete the file for customizing the Web authentication screen....234
5.3.38 Set EAP pass through....235
5.4 Port security....235
5.4.1 Set port security function....235
5.4.2 Register permitted MAC addresses....236
5.4.3 Set operations used for security violations....236
5.4.4 Show port security information....236
5.5 Error detection function....237
5.5.1 Set automatic recovery from errdisable state....237
5.5.2 Show error detection function information....238

Chapter 6: Layer 2 functions....239
6.1 FDB (Forwarding Data Base)....239
6.1.1 Set MAC address acquisition function....239
6.1.2 Set dynamic entry ageing time....239
6.1.3 Clear dynamic entry....240
6.1.4 Set static entry....240
6.1.5 Show MAC address table....241
6.1.6 Show number of MAC addresses....242
6.2 VLAN....242
6.2.1 Move to VLAN mode....242
6.2.2 Set VLAN interface....243
6.2.3 Set private VLAN....243
6.2.4 Set secondary VLAN for primary VLAN....244
6.2.5 Set access port (untagged port)....245
6.2.6 Set associated VLAN of an access port (untagged port)....246
6.2.7 Set trunk port (tagged port)....246
6.2.8 Set associated VLAN for trunk port (tagged port)....247
6.2.9 Set native VLAN for trunk port (tagged port)....248
6.2.10 Set private VLAN port type....249
6.2.11 Set private VLAN host port....249
6.2.12 Set promiscuous port for private VLAN....250
6.2.13 Set voice VLAN....251
6.2.14 Set CoS value for voice VLAN....252
6.2.15 Set DSCP value for voice VLAN....252
6.2.16 Set multiple VALN group....252
6.2.17 Set name of multiple VLAN group....253
6.2.18 Configuring the YMPI frame transmission when multiple VLANs are configured....254
6.2.19 Show VLAN information....254
6.2.20 Show private VLAN information....255
6.2.21 Show multiple VLAN group setting information....255
6.3 STP (Spanning Tree Protocol)....256
6.3.1 Set spanning tree for the system....256
6.3.2 Set forward delay time....256
6.3.3 Set maximum aging time....257
6.3.4 Set bridge priority....257
6.3.5 Set spanning tree for an interface....258
6.3.6 Set spanning tree link type....258
6.3.7 Set interface BPDU filtering....259
6.3.8 Set interface BPDU guard....259

6.3.9 Set interface path cost....260
6.3.10 Set interface priority....261
6.3.11 Set edge port for interface....261
6.3.12 Show spanning tree status....262
6.3.13 Show spanning tree BPDU statistics....264
6.3.14 Clear protocol compatibility mode....265
6.3.15 Move to MST mode....265
6.3.16 Generate MST instance....266
6.3.17 Set VLAN for MST instance....266
6.3.18 Set priority of MST instance....267
6.3.19 Set MST region name....267
6.3.20 Set revision number of MST region....268
6.3.21 Set MST instance for interface....268
6.3.22 Set interface priority for MST instance....269
6.3.23 Set interface path cost for MST instance....269
6.3.24 Show MST region information....270
6.3.25 Show MSTP information....270
6.3.26 Show MST instance information....271
6.4 Loop detection....272
6.4.1 Set loop detection function (system)....272
6.4.2 Set loop detection function (interface)....273
6.4.3 Set port blocking for loop detection....274
6.4.4 Detects Port Blocking loop clearing at regular intervals....275
6.4.5 Reset loop detection status....275
6.4.6 Show loop detection function status....275
6.5 DHCP snooping....276
6.5.1 Enable/disable setting for DHCP snooping (system)....276
6.5.2 Enable/disable DHCP snooping (VLAN) setting....277
6.5.3 DHCP snooping port type setting....278
6.5.4 Enable/disable setting for MAC address verification....278
6.5.5 Enable/disable Option 82 setting....279
6.5.6 Settings for permitting receipt of packets on an untrusted port, including Option 82 information....280
6.5.7 Option 82 Remote-ID settings....280
6.5.8 Option 82 Circuit-ID settings....280
6.5.9 Option 82 Subscriber-ID settings....281
6.5.10 DHCP packet reception rate limitation setting....282
6.5.11 Setting to enable/disable SYSLOG output when DHCP packets are discarded....282
6.5.12 Show DHCP snooping system setting information....283
6.5.13 Show interface setting information for DHCP snooping....283
6.5.14 View the binding database....284
6.5.15 Show DHCP snooping statistics....284
6.5.16 Clear the binding database....284
6.5.17 Clear the DHCP snooping statistics....285

Chapter 7: Layer 3 functions....286
7.1 IPv4 address management....286
7.1.1 Set IPv4 address....286
7.1.2 Show IPv4 address....287
7.1.3 Automatically set IPv4 address by DHCP client....287
7.1.4 Show DHCP client status....288
7.1.5 Set auto IP function....289
7.2 IPv4 route control....289
7.2.1 Set static IPv4 route....289
7.2.2 Set number of equal-cost multi-path registrations....290
7.2.3 Show IPv4 Forwarding Information Base....290
7.2.4 Show IPv4 Routing Information Base....291
7.2.5 Show summary of the route entries registered in the IPv4 Routing Information Base....291
7.2.6 Clear IPv4 route....292
7.3 ARP....292
7.3.1 Show ARP table....292
7.3.2 Clear ARP table....293
7.3.3 Set static ARP entry....293
7.3.4 Set ARP timeout....293
7.3.5 ARP request transmission method settings during ARP timeout....294

7.4 IPv4 forwarding control.... 294
7.4.1 IPv4 forwarding settings (system).... 294
7.4.2 IPv4 forwarding settings (interface).... 295
7.4.3 Show IPv4 forwarding settings.... 295
7.4.4 IPv4 directed broadcast forwarding settings.... 295
7.4.5 MTU setting.... 296
7.5 IPv4 ping.... 297
7.5.1 IPv4 ping.... 297
7.5.2 Check IPv4 route.... 298
7.6 IPv6 address management.... 298
7.6.1 Set IPv6.... 298
7.6.2 Set IPv6 address.... 299
7.6.3 Set RA for IPv6 address.... 299
7.6.4 Set dynamic IPv6 addresses with a DHCPv6 client.... 300
7.6.5 Set an IPv6 address using DHCPv6-PD.... 301
7.6.6 Set DHCPv6-PD client.... 302
7.6.7 Set automatic registration of default gateway using RA.... 303
7.6.8 Show IPv6 address.... 304
7.6.9 Show DHCPv6 client status.... 304
7.6.10 Reset DHCPv6 client.... 305
7.6.11 Set ND prefix received when configuring a DHCPv6 client.... 306
7.7 IPv6 route control.... 306
7.7.1 Set IPv6 static route.... 306
7.7.2 Show IPv6 Forwarding Information Base.... 307
7.7.3 Show IPv6 Routing Information Base.... 308
7.7.4 Show summary of the route entries registered in the IPv6 Routing Information Base.... 308
7.7.5 Clear IPv6 route.... 309
7.8 Neighbor cache.... 309
7.8.1 Set static neighbor cache entry.... 309
7.8.2 Show neighbor cache table.... 310
7.8.3 Clear neighbor cache table.... 310
7.9 IPv6 RA.... 310
7.9.1 Set IPv6 RA transmission.... 310
7.9.2 Set prefix information advertised by RA.... 311
7.9.3 Set maximum RA periodic transmission interval.... 312
7.9.4 Set minimum RA periodic transmission interval.... 312
7.9.5 Set the Cur Hop Limit field for RA.... 313
7.9.6 Set the RA M flag.... 313
7.9.7 Set the RA O flag.... 314
7.9.8 Set RA Router Lifetime.... 314
7.9.9 Set RA Reachable Time.... 315
7.9.10 Set RA Retrans Timer.... 315
7.9.11 Set MTU option for RA.... 316
7.9.12 Show RA information.... 316
7.10 IPv6 forwarding control.... 317
7.10.1 IPv6 forwarding settings.... 317
7.10.2 Show IPv6 forwarding settings.... 317
7.11 IPv6 ping.... 317
7.11.1 IPv6 ping.... 317
7.11.2 Check IPv6 route.... 318
7.12 DNS client.... 319
7.12.1 Set DNS lookup function.... 319
7.12.2 Set DNS server list.... 319
7.12.3 Set default domain name.... 320
7.12.4 Set search domain list.... 320
7.12.5 Show DNS client information.... 321
7.13 BGP.... 322
7.13.1 Set function enable and AS number.... 322
7.13.2 Switch to BGP IPv6 address family mode.... 322
7.13.3 Leave BGP IPv6 address family mode.... 322
7.13.4 Set router ID.... 323
7.13.5 Set IPv4 unicast route exchange operations.... 323
7.13.6 Setting for session reset behavior when an interface goes down.... 324
7.13.7 Setting for output of logs related to state changes.... 324
7.13.8 Check interval setting for routes registered in the BGP routing table.... 325

7.13.9 Set administrative distance (BGP IPv4)....325
7.13.10 Set administrative distance (BGP IPv6)....326
7.13.11 Set the AS_PATH access list....326
7.13.12 Set community list....327
7.13.13 Set IPv4 prefix list....328
7.13.14 Set IPv6 prefix list....328
7.13.15 Keepalive-related timer settings....329
7.13.16 Enable route exchange with BGP peers (BGP IPv4)....330
7.13.17 Enable route exchange with BGP peers (BGP IPv6)....330
7.13.18 Set minimum transmission interval for UPDATE messages....331
7.13.19 Setting for accepting routes even when the AS_PATH attribute of the received route contains the local AS number (BGP IPv4)....331
7.13.20 Setting for accepting routes even when the AS_PATH attribute of the received route contains the local AS number (BGP IPv6)....332
7.13.21 Set minimum transmission interval for UPDATE messages, including local AS....332
7.13.22 Advertise routes without rewriting attributes (BGP IPv4)....333
7.13.23 Advertise routes without rewriting attributes (BGP IPv6)....334
7.13.24 Advertise outbound route filtering capability (BGP IPv4)....334
7.13.25 Advertise outbound route filtering capability (BGP IPv6)....335
7.13.26 Enable route refresh capability....335
7.13.27 Advertise default route to BGP peers (BGP IPv4)....336
7.13.28 Advertise default route to BGP peers (BGP IPv6)....336
7.13.29 BGP peer description....337
7.13.30 Permit/deny peers advertising Hold Time of 0....337
7.13.31 Restricting routes when transmitting/receiving an UPDATE message (BGP IPv4)....338
7.13.32 Restricting routes when transmitting/receiving an UPDATE message (BGP IPv6)....338
7.13.33 Enable/disable capability advertisement....339
7.13.34 Establish BGP peer even if network is not the same....340
7.13.35 Set filter to restrict AS_PATH attributes advertised to BGP peers (BGP IPv4)....340
7.13.36 Set filter to restrict AS_PATH attributes advertised to BGP peers (BGP IPv6)....341
7.13.37 Set interface for communicating with a BGP peer....341
7.13.38 Set number of routes that can be received from a BGP peer (BGP IPv4)....342
7.13.39 Set number of routes that can be received from a BGP peer (BGP IPv6)....342
7.13.40 Set whether to forcibly rewrite the NEXT_HOP attribute to this device’s IP (BGP IPv4)....343
7.13.41 Set whether to forcibly rewrite the NEXT_HOP attribute to this device's IP (BGP IPv6)....343
7.13.42 Set whether to follow advertised capability of BGP peer....344
7.13.43 Do not autonomously start sessions with BGP peers....345
7.13.44 Enable MD5 authentication between BGP peers....345
7.13.45 Create BGP peer group....345
7.13.46 Add a peer to a BGP peer group (BGP IPv4)....346
7.13.47 Add a peer to a BGP peer group (BGP IPv6)....346
7.13.48 Apply prefix list of routes received from a BGP peer (BGP IPv4)....347
7.13.49 Apply prefix list of routes received from a BGP peer (BGP IPv6)....347
7.13.50 Set AS number for BGP peer....348
7.13.51 Remove private AS numbers from the AS_PATH attribute when advertising routes (BGP IPv4)....348
7.13.52 Remove private AS numbers from the AS_PATH attribute when advertising routes (BGP IPv6)....349
7.13.53 Setting to apply route maps when advertisting routes to a BGP peer (BGP IPv4)....349
7.13.54 Apply route maps when advertisting routes to a BGP peer (BGP IPv6)....350
7.13.55 Specify BGP peer as route reflector client (BGP IPv4)....351
7.13.56 Specify BGP peer as route reflector client (BGP IPv6)....351
7.13.57 Permit/deny advertisement of community attributes for a BGP peer (BGP IPv4)....352
7.13.58 Permit/deny advertisement of community attributes for a BGP peer (BGP IPv6)....352
7.13.59 Disconnect session with BGP peer....353
7.13.60 Retain/discard original route information (BGP IPv4)....353
7.13.61 Retain/discard original route information (BGP IPv6)....354
7.13.62 Various timer settings related to communications with BGP peers....354
7.13.63 Set weight of routes received from a BGP peer (BGP IPv4)....355
7.13.64 Set weight of routes received from a BGP peer (BGP IPv6)....356
7.13.65 Set LOCAL_PREF attribute value....356
7.13.66 Settings to retain/disregard messages when the expected AS is not at the start of the AS_PATH attribute....356
7.13.67 Setting to use/disregard MED when selecting routes advertised by eBGPs with different AS associations....357
7.13.68 Set whether to use/disregard AS_PATH attribute in route selection....357
7.13.69 Setting to enable/disable use of AS_PATH length for AS confederations during route selection....358

7.13.70 Set enable/disable router ID conditions for route selection.... 358
7.13.71 Set enable/disable ORIGIN attribute conditions during multiple route selection....358
7.13.72 Set parameter for MED attribute by route selection....359
7.13.73 Delete MED attribute from received route information....359
7.13.74 Delete MED attribute from transmitted route information.... 359
7.13.75 Set processing order for route selection if there are multiple routes with the same destination....360
7.13.76 Aggregate the advertised routes and register in the BGP routing table (BGP IPv4).... 360
7.13.77 Aggregate the advertised route and register in the BGP routing table (BGP IPv6)....361
7.13.78 Setting to enable or disable advertising aggregated routes using classful addresses to peers....361
7.13.79 Prefix settings loaded into the BGP routing table (BGP IPv4)....362
7.13.80 Prefix settings loaded into the BGP routing table (BGP IPv6)....362
7.13.81 Advertise routes to BGP peers only if present in the IP routing table (BGP IPv4).... 363
7.13.82 Advertise routes to BGP peers only if present in the IP routing table (BGP IPv6).... 363
7.13.83 Use BGP to readvertise routes with the specified protocol (BGP IPv4)....363
7.13.84 Use BGP to readvertise routes with the specified protocol (BGP IPv6)....364
7.13.85 Set whether to use route synchronization with the IGP (RIP, OSPF) or not (BGP IPv4)....364
7.13.86 Set whether to use route synchronization with the IGP (RIP, OSPF) or not (BGP IPv6)....365
7.13.87 Only aggregate routes with same NEXT_HOP attribute.... 365
7.13.88 Enable/disable BGP next hop trigger.... 365
7.13.89 Set delay interval for BGP next hop tracking....366
7.13.90 Enable route reflector (BGP IPv4).... 366
7.13.91 Enable route reflector (BGP IPv6).... 366
7.13.92 Cluster ID settings....367
7.13.93 Specify AS number of confederation to join....367
7.13.94 Specify AS number of other confederation....368
7.13.95 Set parameter for AS_PATH attribute.... 368
7.13.96 Set COMMUNITIES attribute parameter.... 368
7.13.97 Set destination address condition (BGP IPv4).... 369
7.13.98 Set condition for IPv4 next hop....369
7.13.99 Set destination address condition (BGP IPv6).... 370
7.13.100 Set condition for IPv6 next hop....370
7.13.101 Set metric value conditions.... 371
7.13.102 Set parameter for ORIGIN attribute....371
7.13.103 Adding AGGREGATOR attributes.... 372
7.13.104 Adding to the start of the AS_PATH attribute....372
7.13.105 Adding ATOMIC_AGGREGATE attributes....373
7.13.106 Delete COMMUNITIES attribute from a community.... 373
7.13.107 Rewriting and adding COMMUNITIES attributes.... 373
7.13.108 Rewrite settings for IPv4 next hop....374
7.13.109 Rewrite settings for IPv6 next hop....375
7.13.110 Rewrite LOCAL_PREF attribute value....375
7.13.111 Rewrite settings for MULTI_EXIT_DISC(MED) attributes....375
7.13.112 Adding ORIGIN attributes.... 376
7.13.113 Adding ORIGINATOR_ID attributes....376
7.13.114 Set route weight....377
7.13.115 Show the status of BGP next hop tracking....377
7.13.116 Display the status of the BGP next hop tree....377
7.13.117 Show AS_PATH access list.... 378
7.13.118 Show IPv4 prefix list....378
7.13.119 Show IPv6 prefix list....378
7.13.120 Show IPv4 BGP routes....379
7.13.121 Show IPv6 BGP routes....379
7.13.122 Show IPv4 BGP routes permitted by a specific community name.... 380
7.13.123 Show IPv6 BGP routes permitted by a specific community name.... 380
7.13.124 Show IPv4 BGP routes permitted by a specified community list.... 381
7.13.125 Show IPv6 BGP routes permitted by a specified community list.... 381
7.13.126 Show IPv4 BGP routes permitted by a specific list.... 381
7.13.127 Show IPv6 BGP routes permitted by a specific list.... 382
7.13.128 Show IPv4 routes to the same destination with different AS_PATH origins....382
7.13.129 Show IPv6 routes to the same destination with different AS_PATH origins....382
7.13.130 Show IPv4 BGP peers....383
7.13.131 Show IPv6 BGP peers....383
7.13.132 Show routes advertised to IPv4 BGP peers....384
7.13.133 Show routes advertised to IPv6 BGP peers....385
7.13.134 Show Hold time for BGP peers....385

7.13.135 Show number of inbound/outbound keepalive messages for a BGP peer.... 386
7.13.136 Keepalive transmission interval for BGP peers.... 386
7.13.137 Show number of inbound/outbound notification messages for a BGP peer.... 386
7.13.138 Show number of open messages sent/received from a BGP peer.... 387
7.13.139 Show number of messages received from a BGP peer.... 387
7.13.140 Show prefix filter information received from a BGP peer.... 387
7.13.141 Show all routes received from IPv4 BGP peers.... 388
7.13.142 Show all routes received from IPv6 BGP peers.... 388
7.13.143 Show all routes received from IPv4 BGP peers and filtered.... 389
7.13.144 Show all routes received from IPv6 BGP peers and filtered.... 389
7.13.145 Show number of messages transmitted to a BGP peer.... 390
7.13.146 Show number of UPDATE messages sent/received from a BGP peer.... 390
7.13.147 Show BGP scan status.... 390
7.13.148 Show IPv4 BGP peer summary.... 391
7.13.149 Show IPv6 BGP peer summary.... 391
7.13.150 Update the session targeting the IPv4 BGP peer.... 392
7.13.151 Update the session targeting the IPv6 BGP peer.... 392
7.13.152 Clear IPv4 prefix list statistical information.... 393
7.13.153 Clear IPv6 prefix list statistical information.... 394
7.13.154 Output the BGP log.... 394
7.14 OSPF.... 395
7.14.1 Move to OSPFv2 mode (IPv4).... 395
7.14.2 Move to OSPFv3 mode (IPv6).... 395
7.14.3 Set authentication for an OSPF area.... 396
7.14.4 Set metric value for default route (OSPFv2).... 397
7.14.5 Set filtering for route information advertised between areas.... 397
7.14.6 Set area as NSSA (OSPFv2).... 398
7.14.7 Summarize route information of a specified network address region, and advertise to other areas (OSPFv2).... 399
7.14.8 Set area as stub area (OSPFv2).... 400
7.14.9 Specify virtual link on area (OSPFv2).... 401
7.14.10 Set bandwidth of interface (OSPFv2).... 402
7.14.11 Set Opaque-LSA.... 403
7.14.12 Set method for calculating the summary route metric.... 403
7.14.13 Set LSDB summary list optimization (OSPFv2).... 403
7.14.14 Set default external route (OSPFv2).... 404
7.14.15 Set metric value when advertising to OSPF routing domain (OSPFv2).... 404
7.14.16 Set priority of route taken from OSPF into FIB (OSPFv2).... 405
7.14.17 Set filtering for route information between RIB and OSPF routing table (OSPFv2).... 405
7.14.18 Set stub host route (OSPFv2).... 406
7.14.19 Set number of concurrent DD exchange processes (OSPFv2).... 407
7.14.20 Associate areas with interface running OSPF.... 407
7.14.21 Set OSPF router ID.... 408
7.14.22 Set upper limit of link status advertisements handled by OSPF process.... 408
7.14.23 Set upper limit of receivable AS external LSA.... 409
7.14.24 Set OSPF passive interface (OSPFv2).... 409
7.14.25 Advertise the specified external route information to the OSPF area as an AS external LSA (OSPFv2).... 410
7.14.26 Set summary destination network address when advertising to OSPF area (OSPFv2).... 410
7.14.27 Set minimum wait time until LSA is received.... 411
7.14.28 Set delay time for changes related to the shortest path calculation.... 411
7.14.29 Set transmission wait time for link state advertisements.... 412
7.14.30 Set metric value for default route (OSPFv3).... 412
7.14.31 Set area as NSSA (OSPFv3).... 413
7.14.32 Summarize route information of a specified network address region, and advertise to other areas (OSPFv3).... 414
7.14.33 Set area as stub area (OSPFv3).... 415
7.14.34 Specify virtual link on area (OSPFv3).... 416
7.14.35 Set bandwidth of interface (OSPFv3).... 416
7.14.36 Set LSDB summary list optimization (OSPFv3).... 417
7.14.37 Set default external route (OSPFv3).... 417
7.14.38 Set metric value when advertising to OSPF routing domain (OSPFv3).... 418
7.14.39 Set priority of route taken from OSPF into FIB (OSPFv3).... 418
7.14.40 Set filtering for route information between RIB and OSPF routing table (OSPFv3).... 419
7.14.41 Set stub host route (OSPFv3).... 419

7.14.42 Set number of concurrent DD exchange processes (OSPFv3)....420
7.14.43 Set OSPF passive interface (OSPFv3)....420
7.14.44 Advertise the specified external route information to the OSPF area as an AS external LSA (OSPFv3)....420
7.14.45 Set OSPF router ID (OSPFv3)....421
7.14.46 Set summary destination network address when advertising to OSPF area (OSPFv3)....422
7.14.47 Set area authentication for each interface....422
7.14.48 Set authentication key used for area authentication....423
7.14.49 Set fixed cost for an interface....423
7.14.50 Reduce LSA flooding for an interface....423
7.14.51 Set time until neighboring router is considered down....424
7.14.52 Disable OSPF....424
7.14.53 Set transmission interval of Hello packets....424
7.14.54 Set MD5 digest authentication key used for OSPF authentication....425
7.14.55 Configuring the OSPF network type (OSPFv2)....425
7.14.56 Set priority for selecting designated router (DR)....426
7.14.57 Set packet retransmission interval....426
7.14.58 Set increment value when transmitting age field of Link State Update packets....426
7.14.59 Set fixed cost for an interface (IPv6)....427
7.14.60 Set time until neighboring router is considered down (IPv6)....427
7.14.61 Set transmission interval of Hello packets (IPv6)....427
7.14.62 Configuring the OSPF network type (OSPFv3)....428
7.14.63 Set priority for selecting designated router (DR) (IPv6)....428
7.14.64 Set packet retransmission interval (IPv6)....429
7.14.65 Specify area in the interface (IPv6)....429
7.14.66 Set increment value when transmitting age field of Link State Update packets (IPv6)....430
7.14.67 Restart OSPF process (IPv4)....430
7.14.68 Show OSPF process information (IPv4)....430
7.14.69 Show ABR and ASBR route information (IPv4)....431
7.14.70 Show LSA information in the link state database matching the specified conditions (IPv4)....431
7.14.71 Show ASBR summary LSA information in the link state database....431
7.14.72 Show AS external LSA information in the link state database (IPv4)....432
7.14.73 Show network LSA information in the link state database (IPv4)....432
7.14.74 Show NSSA AS external LSA information in the link state database....433
7.14.75 Show router LSA information in the link state database (IPv4)....433
7.14.76 Show network summary LSA information in the link state database....433
7.14.77 Show OSPF interface information (IPv4)....434
7.14.78 Show OSPF neighbor information for the specified neighbor (IPv4)....434
7.14.79 Show OSPF routing table (IPv4)....435
7.14.80 Show OSPF virtual link information (IPv4)....435
7.14.81 Show OSPF settings and status (IPv4)....435
7.14.82 Restart OSPF process (IPv6)....435
7.14.83 Show OSPF process information (IPv6)....436
7.14.84 Show ABR and ASBR route information (IPv6)....436
7.14.85 Show LSA information in the link state database matching the specified conditions (IPv6)....436
7.14.86 Show AS external LSA information in the link state database matching the specified conditions (IPv6)....437
7.14.87 Show Inter-Area-Prefix LSA information in the link state database (IPv6)....437
7.14.88 Show Inter-Area-Router LSA information in the link state database (IPv6)....438
7.14.89 Show Intra-Area-Prefix LSA information in the link state database (IPv6)....438
7.14.90 Show Link LSA information in the link state database (IPv6)....439
7.14.91 Show network LSA information in the link state database (IPv6)....439
7.14.92 Show router LSA information in the link state database (IPv6)....440
7.14.93 Show OSPF interface information (IPv6)....440
7.14.94 Show OSPF neighbor information (IPv6)....441
7.14.95 Show OSPF routing table (IPv6)....441
7.14.96 Show OSPF virtual link information (IPv6)....441
7.14.97 Show OSPF settings and status (IPv6)....442
7.15 RIP....442
7.15.1 Move to RIP mode....442
7.15.2 Move to RIPng mode....442
7.15.3 Set default external route....442
7.15.4 Set default metric value when redistributing external route in RIP....443
7.15.5 Set priority of route taken from RIP into RIB....443
7.15.6 Set filtering for RIB and RIP routing table....443

7.15.7 Set neighbor RIP router....444
7.15.8 Set network advertised by RIP....444
7.15.9 Offset metric value for route information matching the access list....445
7.15.10 Set VLAN interface for RIP packet reception only....445
7.15.11 Redistribute external route information to RIP network....446
7.15.12 Set RIP-related timers....446
7.15.13 Set RIP version....447
7.15.14 Set key chain used for RIPv2 authentication....447
7.15.15 Set authentication method used for RIPv2....447
7.15.16 Set password used for RIPv2 authentication....448
7.15.17 Set operation when a route whose metric is 0 is received....448
7.15.18 Set RIP packet reception....448
7.15.19 Set RIP version that can be received....449
7.15.20 Set RIP packet transmission....449
7.15.21 Set RIP version that can be transmitted....449
7.15.22 Set split horizon (IPv4)....450
7.15.23 Set poison reverse (IPv4)....450
7.15.24 Set metric for offsetting route information of the transmitted and received RIPng packets....451
7.15.25 Set split horizon (IPv6)....451
7.15.26 Set poison reveerse (IPv6)....451
7.15.27 Set RIPng....452
7.15.28 Generate key chain used for RIPv2 authentication....452
7.15.29 Generate key for registration in key chain....452
7.15.30 Set password used for RIPv2 authentication....453
7.15.31 Set the term in which key received for use in RIPv2 authentication is accepted as valid....453
7.15.32 Set the term in which key for use in RIPv2 authentication is valid for transmission....454
7.15.33 Delete route information from the RIP routing table (IPv4)....455
7.15.34 Clear RIP statistical information....456
7.15.35 Delete route information from the RIPng routing table (IPv6)....456
7.15.36 Show RIP settings and status (IPv4)....456
7.15.37 Show RIPng settings and status (IPv6)....456
7.15.38 Show RIP routing table (IPv4)....457
7.15.39 Show RIPng routing table (IPv6)....457
7.15.40 Show RIP status for each interface (IPv4)....457
7.15.41 Show RIPng status for each interface (IPv6)....457
7.15.42 Show RIP statistical information....458
7.16 VRRP....458
7.16.1 Move to VRRP mode....458
7.16.2 Move to VRRP mode(IPv6)....458
7.16.3 Set advertisement packet transmission interval....459
7.16.4 Set circuit failover....460
7.16.5 Enable/disable virtual router....460
7.16.6 Set preempt mode....461
7.16.7 Set virtual router's priority....461
7.16.8 Set virtual IP address....462
7.16.9 Set virtual IP address(IPv6)....462
7.16.10 Show VRRP information....463
7.16.11 Show VRRP information(IPv6)....464
7.16.12 Show VRRP statistical information....464
7.16.13 Show VRRP statistical information(IPv6)....465
7.17 PBR....466
7.17.1 Generating a route map....466
7.17.2 Set description to the route map....466
7.17.3 Parameter settings for application to route map entries....467
7.17.4 Processing content (IPv4 forwarding destination) settings for route map entries....468
7.17.5 Processing content (IPv6 forwarding destination) settings for route map entries....468
7.17.6 Processing content (packet discard) settings for route map entries....469
7.17.7 Applying a route map to the interface (for IPv4)....470
7.17.8 Applying a route map to the interface (for IPv6)....470
7.17.9 Enable/disable PBR function....471
7.17.10 Show route map information....472
7.17.11 Show IPv4 PBR information....472
7.17.12 Show IPv6 PBR information....473

Chapter 8: IP multicast control....474

8.1 IP multicast basic settings....474
8.1.1 Set IP multicast routing....474
8.1.2 Set IP multicast routing (physical port)....474
8.1.3 Set RFP check unicast routing information....475
8.1.4 Set maximum number of entries for IP multicast routing....475
8.1.5 Show IP multicast routing information base....476
8.1.6 Show information for virtual interfaces used for IP multicasts....477
8.1.7 Show RPF information....478
8.1.8 Delete entries from the IP multicast routing information base....478
8.1.9 Set processing method for unknown multicast frames....479
8.1.10 Setting the processing method for unknown multicast frames (interface)....479
8.1.11 Forwarding setting for link local multicast frames....480
8.1.12 Forwarding setting for multicast frames....481
8.1.13 Enable/disable function to transmit IGMP/MLD query when topology changes....481
8.2 IGMP snooping....482
8.2.1 Set enable/disable IGMP snooping....482
8.2.2 Set IGMP snooping fast-leave....482
8.2.3 Set multicast router connection destination....483
8.2.4 Set query transmission function....484
8.2.5 Set IGMP query transmission interval....484
8.2.6 Set TTL value verification function for IGMP packets....485
8.2.7 Set RA verification function for IGMP packets....485
8.2.8 Set ToS verification function for IGMP packets....486
8.2.9 Set IGMP version....486
8.2.10 Settings for IGMP Report Suppression....487
8.2.11 Set the IGMP report forwarding function....488
8.2.12 Settings for Suppression of Data Transmission to Multicast Router Ports....489
8.2.13 Show multicast router connection port information....489
8.2.14 Show IGMP group membership information....490
8.2.15 Show an interface's IGMP-related information....490
8.2.16 Clear IGMP group membership entries....491
8.3 MLD snooping....491
8.3.1 Enable/disable MLD snooping....491
8.3.2 Set MLD snooping fast-leave....492
8.3.3 Set multicast router connection destination....493
8.3.4 Set query transmission function....493
8.3.5 Set MLD query transmission interval....494
8.3.6 Set MLD version....494
8.3.7 Settings for MLD Report Suppression....495
8.3.8 Show multicast router connection port information....495
8.3.9 Show MLD group membership information....496
8.3.10 Show an interface's MLD-related information....496
8.3.11 Clear MLD group membership entries....497
8.4 PIM....498
8.4.1 Set PIM operation mode....498
8.4.2 Set Hello message interval....498
8.4.3 Set Hello message timeout....499
8.4.4 Set PIM neighbor filter....499
8.4.5 Set Generation ID....500
8.4.6 Set DR priority order....500
8.4.7 Set static RP....501
8.4.8 Set RP candidate....501
8.4.9 Set Candidate-RP-Advertisement message....502
8.4.10 Set BSR candidate....503
8.4.11 Set BSR message transmit/receive....503
8.4.12 Set RP priority usage....503
8.4.13 Set source IP address for Register messages....504
8.4.14 Set register message filtering....504
8.4.15 Set upper limit value of the Register message transmission rate....505
8.4.16 Set calculation method for Register message checksums....505
8.4.17 Set Register message transmission standby time....506
8.4.18 Set Join/Prune message transmission interval....506

8.4.19 Set RP Keepalive Timer....507
8.4.20 Set SPT move operation....507
8.4.21 Set PIM-SSM....508
8.4.22 Set State Refresh message transmission interval....508
8.4.23 Set Graft message maximum resend count....509
8.4.24 Set forward delay time for PIM messages....509
8.4.25 Set unicast BSM send/receive....510
8.4.26 Set confirmation for RP-reachability messages....510
8.4.27 Show PIM interface information....510
8.4.28 Show IP multicast routing information base....512
8.4.29 Show PIM neighbor information....514
8.4.30 Show necthop information....514
8.4.31 Show RP information....515
8.4.32 Show RP selection candidate....516
8.4.33 Show BSR information....516
8.4.34 Clear RP information....517
8.5 IGMP....517
8.5.1 Set IGMP....517
8.5.2 Set IGMP version....517
8.5.3 Set Query Interval....518
8.5.4 Set General Membership Query maximum reply time....518
8.5.5 Set Last Member Query Interval....519
8.5.6 Set Last Member Query Count....519
8.5.7 Set Other Querier Present Interval....520
8.5.8 Set Robustness Variable....520
8.5.9 Set IGMP immediate-leave....521
8.5.10 Set source address check for IGMP packets....521
8.5.11 Set limit multicast group membership....522
8.5.12 Set maximum number of registerable groups for IGMP group membership....522
8.5.13 Set IGMP group membership static entry....523
8.5.14 Set SSM mapping function....523
8.5.15 Set SSM mapping static entry....524
8.5.16 Set downstream interface for the IGMP proxy....525
8.5.17 Set IGMP proxy upstream interface....525
8.5.18 Show multicast group information....526
8.5.19 Show IGMP interface information....526
8.5.20 Show IGMP SSM map information....527
8.5.21 Show IGMP proxy interface information....527
8.5.22 Clear IGMP group membership....528

Chapter 9: Traffic control....529
9.1 ACL....529
9.1.1 Generate IPv4 access list....529
9.1.2 Adding a description for IPv4 access list....531
9.1.3 Apply IPv4 access list....531
9.1.4 Generate IPv6 access list....532
9.1.5 Adding a description for IPv6 access list....533
9.1.6 Apply IPv6 access list....533
9.1.7 Generate MAC access list....534
9.1.8 Adding a description for MAC access lists....535
9.1.9 Apply MAC access list....536
9.1.10 Show generated access list....537
9.1.11 Clear counters....537
9.1.12 Show access list applied to interface....537
9.1.13 Set VLAN access map and move to VLAN access map mode....538
9.1.14 Set access list for VLAN access map....538
9.1.15 Set VLAN access map filter....539
9.1.16 Show VLAN access map....540
9.1.17 Show VLAN access map filter....540
9.2 QoS (Quality of Service)....540
9.2.1 Enable/disable QoS....540
9.2.2 Set default CoS....541
9.2.3 Set trust mode....541
9.2.4 Show status of QoS function setting....543

9.2.5 Show QoS information for interface.... 543
9.2.6 Show egress queue usage ratio.... 544
9.2.7 Set CoS - egress queue ID conversion table.... 545
9.2.8 Set DSCP - egress queue ID conversion tabl.... 546
9.2.9 Set port priority order.... 546
9.2.10 Specify egress queue of frames transmitted from the switch itself.... 547
9.2.11 Generate class map (traffic category conditions).... 547
9.2.12 Associate class map.... 548
9.2.13 Set traffic classification conditions (access-list).... 549
9.2.14 Set traffic classification conditions (CoS).... 549
9.2.15 Set traffic classification conditions (TOS precedence).... 550
9.2.16 Set traffic classification conditions (DSCP).... 550
9.2.17 Set traffic classification conditions (Ethernet Type).... 551
9.2.18 13.2.22 Set traffic classification conditions (VLAN ID).... 551
9.2.19 Set traffic classification conditions (VLAN ID range).... 552
9.2.20 Show class map information.... 552
9.2.21 Generate policy map for received frames.... 553
9.2.22 Apply policy map for received frames.... 554
9.2.23 Set pre-marking (CoS).... 555
9.2.24 Set pre-marking (TOS precedence).... 555
9.2.25 Set pre-marking (DSCP).... 556
9.2.26 Set individual policers (single rate).... 557
9.2.27 Set individual policers (twin rate).... 558
9.2.28 Set remarking of individual policers.... 559
9.2.29 Generate aggregate policer.... 561
9.2.30 Set aggregate policer (single rate).... 561
9.2.31 Set aggregate policer (twin rate).... 562
9.2.32 Set remarking of aggregate policers.... 563
9.2.33 Show aggregate policers.... 565
9.2.34 Apply aggregate policer.... 565
9.2.35 Show metering counters.... 566
9.2.36 Clear metering counters.... 566
9.2.37 Set egress queue (CoS-Queue).... 567
9.2.38 Set egress queue (DSCP-Queue).... 568
9.2.39 Show policy map information.... 568
9.2.40 Show map status.... 570
9.2.41 Set egress queue scheduling.... 571
9.2.42 Set traffic shaping (individual port).... 572
9.2.43 Sets traffic shaping (per queue).... 572
9.3 Flow control.... 573
9.3.1 Set flow control (IEEE 802.3x PAUSE send/receive) (system).... 573
9.3.2 Set flow control (IEEE 802.3x PAUSE send/receive) (interface).... 574
9.3.3 Show flow control operating status.... 575
9.4 Storm control.... 575
9.4.1 Set storm control.... 575
9.4.2 Show storm control reception upper limit.... 576

Chapter 10: Application.... 577
10.1 DHCP server.... 577
10.1.1 Set the DHCP server function (system).... 577
10.1.2 Set the DHCP server function (interface).... 577
10.1.3 DHCP server operation type settings.... 578
10.1.4 Set DHCP pool.... 578
10.1.5 Set network interface.... 579
10.1.6 Set range of IP addresses to be assigned(DHCP).... 580
10.1.7 Setting the IP address to assign to a specific client.... 580
10.1.8 Set lease time(DHCP).... 581
10.1.9 Settings for duplication checks of leased IP addresses.... 582
10.1.10 Timeout duration settings for duplication checks of leased IP addresses.... 582
10.1.11 Default gateway address notification setting(DHCP).... 583
10.1.12 DNS server settings for notification(DHCP).... 583
10.1.13 Domain name settings for notification(DHCP).... 584
10.1.14 Set boot file name.... 584
10.1.15 Settings for the server on which the boot file is located.... 585

10.1.16 Set user-defined DHCP pptions(DHCP)..... 585
10.1.17 DHCP class settings..... 588
10.1.18 Remote-id settings..... 588
10.1.19 circuit-id settings..... 589
10.1.20 subscriber-id settings..... 589
10.1.21 DHCP pool class settings..... 590
10.1.22 Range of IP addresses to assign (DHCP pool class)..... 590
10.1.23 Lease time settings (DHCP pool class)..... 591
10.1.24 Default gateway address notification setting (DHCP pool class)..... 592
10.1.25 DNS server settings for notification (DHCP pool class)..... 593
10.1.26 Domain name settings for notification (DHCP pool class)..... 593
10.1.27 Show information of DHCP pool..... 594
10.1.28 Show IP address assignment information for DHCP clientsDHCP..... 595
10.1.29 Show DHCP server status..... 595
10.1.30 Delete lease information on DHCP server..... 596
10.2 DHCPv6 server..... 596
10.2.1 DHCPv6 server function settings (system)..... 596
10.2.2 Set DHCPv6 server function (interface)..... 597
10.2.3 DHCPv6 pool settings..... 597
10.2.4 Set the range of IPv6 addresses assigned dynamically (DHCPv6)..... 598
10.2.5 Set a prefix to dynamically assign to a PD client..... 600
10.2.6 DNS server settings for notification (DHCPv6)..... 601
10.2.7 Setting the domain name for resolving names to be notified (DHCPv6)..... 602
10.2.8 Set user-defined DHCPv6 option (DHCPv6)..... 603
10.2.9 Set subnet prefix for identifying the link address field..... 604
10.2.10 Show DHCPv6 pool information..... 605
10.2.11 Displaying IPv6 address assignment information for DHCPv6 clients..... 606
10.2.12 Show DHCPv6 server status..... 607
10.2.13 Delete DHCPv6 server lease information..... 607
10.3 DHCP relay..... 607
10.3.1 Set the DHCP relay agent function..... 607
10.3.2 Configuring the forwarding address for the DHCP relay agent function..... 608
10.3.3 Configuring the broadcast forward for the DHCP relay agent function..... 609
10.3.4 Show status of DHCP relay agent..... 609
10.4 DNS relay..... 610
10.4.1 Set DNS relay function (system)..... 610
10.4.2 Set DNS relay function (interface)..... 610
10.4.3 Set DNS relay function forwarding address..... 611
10.4.4 Set maximum TTL for DNS relay function cache entries..... 612
10.4.5 Clear DNS relay function cache entries..... 612
10.4.6 Set DNS relay function static record..... 612
10.4.7 Show status of DNS relay..... 613
10.4.8 Show cache of DNS relay..... 613
10.5 Local RADIUS server..... 614
10.5.1 Local RADIUS server function settings..... 614
10.5.2 Set access interface..... 614
10.5.3 Generate a route certificate authority..... 615
10.5.4 RADIUS configuration mode..... 615
10.5.5 Authentication method settings..... 616
10.5.6 RADIUS client (NAS) settings..... 616
10.5.7 Authenticated user settings..... 617
10.5.8 Reauthentication interval setting..... 619
10.5.9 Apply setting data to local RADIUS server..... 619
10.5.10 Issuing a client certificate..... 620
10.5.11 Aborting the issue of a client certificate..... 621
10.5.12 Revoking client certificates..... 621
10.5.13 Exporting client certificates (copying to SD card)..... 621
10.5.14 Exporting of client certificates (sending via e-mail)..... 622
10.5.15 Copying RADIUS data..... 623
10.5.16 Show RADIUS client (NAS) status..... 624
10.5.17 Show authenticated user information..... 624
10.5.18 Client certificate issuance status display..... 625
10.5.19 Client certificate list display..... 625
10.5.20 Revoked client certificate list display..... 626

Index **627**

Preface

Introduction

- Unauthorized reproduction of this document in part or in whole is prohibited.
- The contents of this document are subject to change without notice.
- Yamaha disclaims all responsibility for any damages caused by loss of data or other problems resulting from the use of this product.
  The warranty is limited to this physical product itself. Please be aware of these points.
- The information contained in this document has been carefully checked and is believed to be reliable. However, if you find some of the contents to be missing or have questions regarding the contents, please contact us.
- All the company and product names used in this manual are registered trademarks or trademarks of the companies concerned.

Chapter 1

How to read the command reference

1.1 Applicable firmware revision

This command reference applies to firmware Yamaha Standard L3 Switch SWX3220 of Rev.4.02.22 / Rev.4.03.06 / Rev.4.04.06.
For the latest firmware released after printing of this command reference, manuals, and items that differ, access the following URL and see the information in the WWW server.
http://www.rtpro.yamaha.co.jp

1.2 How to read the command reference

This command reference describes the commands that you enter from the console of the Yamaha Standard L3 Switch SWX3220.

Each command is described by a combination of the following items.

[Syntax]	Explains the command input syntax. Key input can use either uppercase or lowercase characters.
	Command names are shown in bold (**Bold face**).
	The parameter portion is shown in italic (*Italic face*).
	Keywords are shown in normal characters.
	Parameters that can be omitted are enclosed in square brackets ([ ]).
[Keyword]	Explains the type and significance of keywords that can be specified for the command.
[Parameter]	Explains the type and significance of parameters that can be specified for the command.
[Initial value]	Displays the default setting value for the command.
[Input mode]	Indicates the modes in which the command can be executed.
[Description]	Explains the command.
[Note]	Explains points that you should be aware of when using the command.
[Example]	Provides specific examples of the command.
[Models]	Shows the names of models for which the command applies. Only commands for which the applicability differs depending on the model are listed. Commands that are not listed apply in common to the entire series.

1.3 Interface names

In the command input syntax, interface names are used to specify each interface of the switch.
The following interface names are handled by the SWX3220.

Interface type	Prefix	Description	Examples
LAN/SFP port	port	Used to specify a physical port. Specify "stack ID" + "." + "port number" after the port number.	When specifying LAN port #1 on LAN port stack #1 : port1.1

Interface type	Prefix	Description	Examples
VLAN interface	vlan	Used to specify a VLAN. Specify vlan followed by the "VLAN ID".	To specify VLAN #1: vlan1
static logical interface	sa	Used to specify link aggregation that combines multiple LAN/SFP port. Specify sa or po followed by "logical interface ID".	To specify static logical interface #1: sa1
LACP logical interface	po		To specify LACP logical interface #2: po2

1.4 Input syntax for commands starting with the word "no"

Many commands also have a form in which the command input syntax starts with the word **no**. If you use a syntax that with begins with the word **no**, the settings of that command are deleted and returned to the default value, unless explained otherwise.

Chapter 2

How to use the commands

The SWX3220 lets you perform command operations in the following two ways.

Type of operation	Method of operation	Description
Operation via console	• Access from a console terminal • Access from a TELNET client • Access from a SSH client	Issue commands one by one to interactively make settings or perform operations.
Operation via a config file	• File transfer via TFTP • File transfer via GUI operation • File copy via SD card	A file containing a set of necessary commands (called a configuration or "config" file) is used to specify multiple settings, or to obtain multiple settings from the SWX3220, in a single operation.

This chapter explains how to use each method.

2.1 Operation via console

2.1.1 Access from a console terminal

Use a USB cable or RJ-45/DB-9 console cable when making settings from a terminal that is connected to the CONSOLE port of SWX3220.

For the USB cable connected to the mini-USB CONSOLE port, use a USB cable that supports data communication between a USB Type A connector and a mini-USB Type B (5-pin) connector. Cables for recharging only cannot be used.

If you are using a computer as a console terminal (serial terminal), you'll need a terminal program to control the computer's serial (COM) port. Set the communication settings of the console terminal as follows.

Setting item	Value
Baud rate	9600bps
Data	8-bit
Parity	none
Stop bit	1-bit
Flow control	Xon/Xoff

For settings related to the console terminal, use the **line con** command to move to line mode.

2.1.2 Access from a TELNET client

You can use a TELNET client on a computer to connect to the TELNET server of the SWX3220 and control it. In order to make settings using TELNET, you must first set up a connection environment (IP network) and then make TELNET server settings.

The IP address settings of the SWX3220 are as follows.

- The default IPv4 address setting is 192.168.100.240/24 for VLAN #1.
- To change the IPv4 address, use the **ip address** command.

The TELNET server settings of the SWX3220 are as follows.

- With the default settings of the TELNET server function, it runs on the default port (TCP port 23) and allows access only from VLAN #1 (vlan0.1).
- To change the reception port number, use the **telnet-server** command.
- Access to the TELNET server can be controlled in VLAN units, and can be specified by the **telnet-server interface** command.

A virtual communication port by which a TELNET client connects is called a "virtual terminal (VTY: Virtual TYpewriter) port." The maximum number of simultaneous TELNET client connections depends on the number of VTY ports of the SWX3220. The VTY ports of the SWX3220 are as follows.

- With the default VTY port settings, eight VTY ports (ID: 0--7) can be used.
- To check the number of VTY ports, use the **show running-config | include line vty** command.

- To change the number of VTY ports, use the **line vty** command. (maximum 8 (ID: 0--7))

To make VTY port settings, use the **line vty** command to specify the target VTY port, and then move to line mode. ID management for virtual terminal ports is handled within the SWX3220, but since login session and ID assignments depend on the connection timing, you should normally make the same settings for all VTY ports.

2.1.3 Access from an SSH client

You can use an SSH client on a computer to connect to the SSH server of the SWX3220 and control it. In order to make settings using SSH, you must first set up a connection environment (IP network) and then make SSH server settings.

The IP address settings of the SWX3220 are as follows.

- The default IPv4 address setting is 192.168.100.240/24 for VLAN #1.
- To change the IPv4 address, use the **ip address** command.

The following settings on the SWX3220 must be made beforehand when accessing from an SSH client.

- Generate a host key on the SSH server using the **ssh-server host key generate** command.
- Enable the SSH server functions using the **ssh-server** command.
- Register the user name and password using the **username** command.

The SSH server settings of the SWX3220 are as follows.

- Access to an SSH server can be controlled for each VLAN, and is set using the **ssh-server interface** command.
- Note that the following functions are not supported.
- SSH protocol version 1
- User authentication aside from password authentication (host response authentication, public key authentication, challenge-response authentication, GSSAPI authentication)
- Port forwarding (X11/TCP forwarding)
- Gateway Ports (Port relay)
- Permitting blank passwords

A virtual communication port by which an SSH client connects is called a "virtual terminal (VTY: Virtual TYpewriter) port." The maximum number of simultaneous SSH client connections depends on the number of VTY ports of the SWX3220. The VTY ports of the SWX3220 are as follows.

- With the default VTY port settings, eight VTY ports (ID: 0--7) can be used.
- To check the number of VTY ports, use the **show running-config | include line vty** command.
- To change the number of VTY ports, use the **line vty** command. (maximum 8 (ID: 0--7))

To make VTY port settings, use the **line vty** command to specify the target VTY port, and then move to line mode. ID management for virtual terminal ports is handled within the SWX3220, but since login session and ID assignments depend on the connection timing, you should normally make the same settings for all VTY ports.

2.1.4 Console terminal/VTY settings

The SWX3220 lets you make the following settings for console terminals and VTY.

1. Timeout duration interpreted as no operation
2. Number of lines shown in one page of the terminal screen

Setting item	Content of setting
Timeout duration interpreted as no operation	Specifies the time after which the login session is forcibly ended when there has been no key input from the terminal. With the default setting, the session is forcibly disconnected after ten minutes. To make this setting, use the **exec-timeout** command of the line mode; this takes effect from the next session.

Setting item	Content of setting
Number of lines shown in one page of the terminal screen	Specifies the number of lines shown on one page of the terminal screen. This can be set as 0--512 lines/page, and the default setting is 24 lines/page. When displaying in this state, 23 lines are displayed, then "---More---" is displayed and the system waits for key input. There are two types of this setting, and they are applied to the system starting with the upper type. 1) unprivileged EXEC mode **terminal length** command 2) global configuration mode **service terminal-length** command Setting 1) is a function that temporarily applies to the user who is using the terminal, and is applied as soon as the command is executed. Setting 2) applies starting with the next session.

2.2 Operation via configuration (config) files

A file containing a set of needed commands is called a configuration (config) file.

The settings that have been made on the SWX3220 can be read as a configuration file by a host on the LAN via TFTP. A configuration file on the host can also be loaded into the SWX3220 to specify its settings.

A configuration file contains all the settings for the entire unit; it is not possible to partially read or write only the settings for a specific area. The configuration file is a text file consisting of ASCII + line-return (CRLF or LF).

The commands and parameters in a configuration file must be in the correct syntax. If the syntax or content are incorrect, that content is ignored and is not applied to operation.

2.2.1 Access from a TFTP client

In order to transfer a configuration file via TFTP, you must first set up a connection environment (IP network) and then make TFTP server settings.

The IP address settings of the SWX3220 are as follows.

- The default IPv4 address setting is 192.168.100.240/24 for VLAN #1.
- To change the IPv4 address, use the **ip address** command.

The TFTP server settings of the SWX3220 are as follows.

- With the default settings of the TFTP server function, it is running on the default port (UDP port 69) and does not allow access from anywhere.
- To change the reception port number, use the **tftp-server** command.
- Access to the TFTP server can be controlled in VLAN units, and can be specified by the **tftp-server interface** command. Specify the VLAN ID for which access is allowed.

2.2.2 Reading/writing a configuration file

Reading/writing a configuration file is performed by executing a TFTP command from the host on the LAN.

The following configuration files are read or written.

- configuration file

Applicable configuration	Applicable file	Description
running-config	CONFIG file (.txt)	Setting values for current operation (Basic settings)
startup-config #0, #1, #SD	CONFIG file (.txt)	Saved setting values (Basic settings)
	All settings (.zip)	Saved setting values (All settings)

Specify the following as the remote path of the configuration file read (GET) or write (PUT) destination.

- Remote path for applicable files (No automatic restart)

Applicable configuration	Applicable file	Remote path	Load (GET)	Save (PUT)	Automatic restart
running-config	CONFIG file (.txt)	config	✓	✓	-
startup-config #0	CONFIG file (.txt)	config0	✓	✓	-
	All settings (.zip)	config0-all	✓	✓	-
startup-config #1	CONFIG file (.txt)	config1	✓	✓	-
	All settings (.zip)	config1-all	✓	✓	-
startup-config #SD	CONFIG file (.txt)	configsd	✓	✓	-
	All settings (.zip)	configsd-all	✓	✓	-

If you want to restart the system automatically after applying the CONFIG file, specify the following remote path. The currently running configuration is applicable.

- Remote path for applicable files (with automatic restart)

Applicable configuration	Applicable file	Remote path	Load (GET)	Save (PUT)	Automatic restart
Currently running startup-config	CONFIG file (.txt)	reconfig	-	✓	✓
	All settings (.zip)	reconfig-all	-	✓	✓

When applying (PUT) a CONFIG file, confirm that the target CONFIG and the type of the target file are correct.

If an incorrect file is specified, it cannot be reflected correctly.

The command syntax used depends on the OS of that host (TFTP client). Keep the following points in mind when executing commands.

- IP address of the SWX3220
- Use "binary mode" as the transmission mode.
- You must specify the privileged password after the remote path in the format "/PASSWORD".
  When the privileged password is in the default state, you cannot read/write configuration files. The privileged password must be changed first.
- If you PUT (write) with "config" specified as the remote path, the changes are added or overwritten to the current operating settings.
  Settings that you do not add or change will remain as the current operating settings.
  Since the setting values are not saved, you must use the **write** command etc. if you want to save them.
- The encrypted password (**password 8** or **enable password 8** command format) is not applied to the settings even if it is PUT to running-config via TFTP.
  And, users are not actually registered when making settings for users that include encrypted passwords (**username** command).

2.3 Login

When the SWX3220 has finished starting up, a login screen is displayed.

You can log in by entering the configured user name and password.

By default, a default administrator is configured, and you can log in with the user name:**admin**and password:**admin**.

- Login screen

```
Username:admin
Password:
```

- Console screen following login

```
SWX3220 Rev.4.02.02 (Mon Dec 14 12:07:35 2020)
  Copyright (c) 2021 Yamaha Corporation. All Rights Reserved.

SWX3220>
```

When logging in as the default administrator for the first time, the password change screen is displayed. Change the password.

- Password change screen

```
Username:admin
Password:
```

```
SWX3220 Rev.4.02.02 (Mon Dec 14 12:07:35 2020)
  Copyright (c) 2021 Yamaha Corporation. All Rights Reserved.

Please change the default password for admin.
New Password:
New Password(Confirm):
Saving ...
Succeeded to write configuration
```

If the incorrect password is entered three times in a row, you will be restricted from logging in for one minute. After one minute has passed, please enter the correct password.

- Login restriction screen

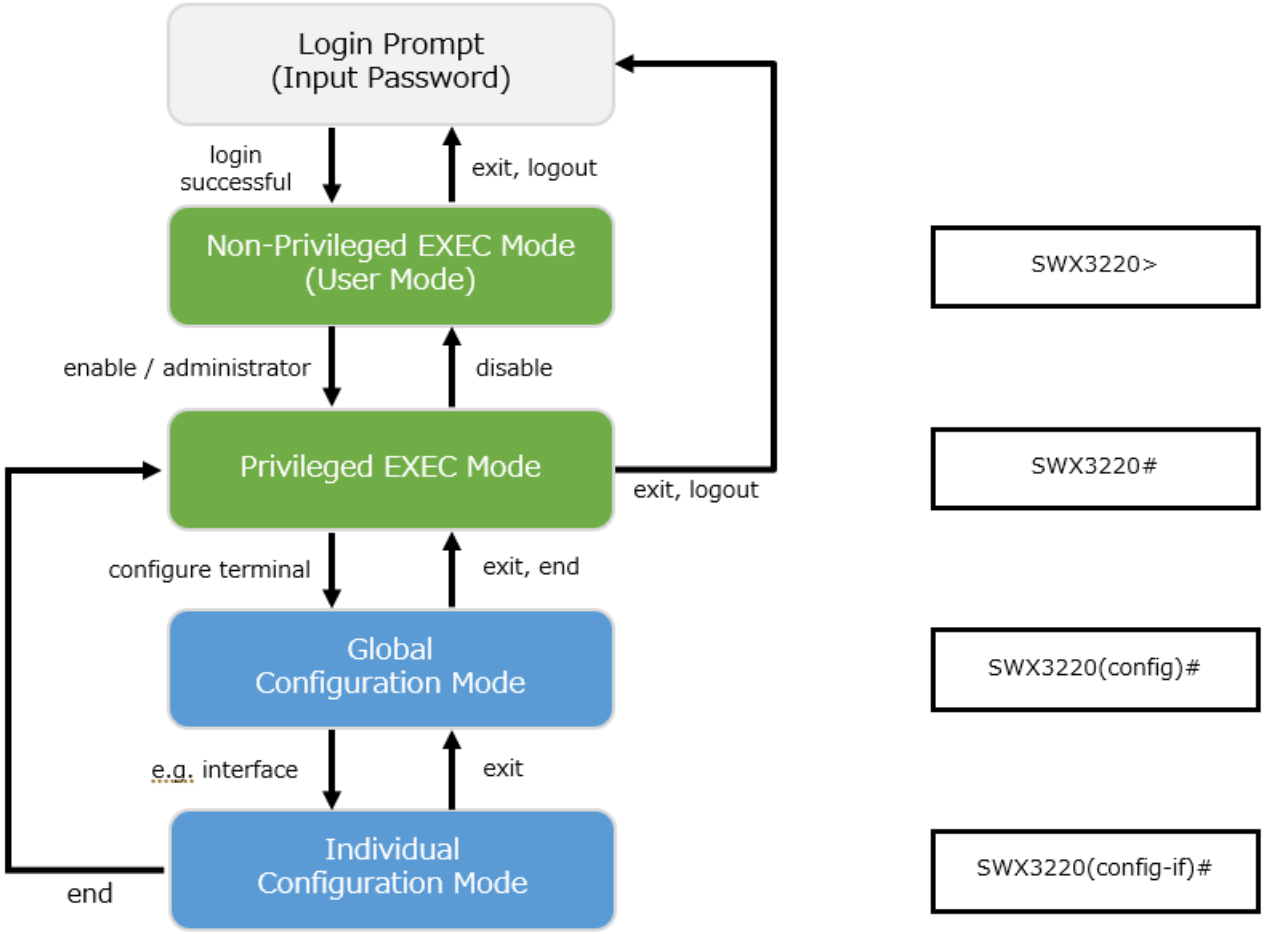
```
Username: user
Password:
% Incorrect username or password, or login as user is restricted.
Password:
% Incorrect username or password, or login as user is restricted.
Password:
% Incorrect username or password, or blocked upon 3 failed login attempts for user.
% Please try again later.
```

- If a restricted user enters the wrong password again, the time limit will be refreshed.
- After the restriction time limit expires, you can log in by entering the correct password.

2.4 Command input mode

2.4.1 Command input mode basics

In order to change the settings of the SWX3220 or to reference the status, you must move to the appropriate command input mode and then execute the command. Command input mode is divided into hierarchical levels as shown below, and the commands that can be entered in each mode are different. By noting the prompt, the user can see which mode they are currently in.



The basic commands related to moving between command input modes are described below. For commands that move from global configuration mode mode to individual configuration mode, refer to "individual configuration mode."

- **exit** command
- **logout** command
- **enable** command / **administrator** command
- **disable** command
- **configure terminal** command
- **end** command

2.4.2 individual configuration mode

individual configuration mode is the overall name for the mode in which you can make detailed settings for specific items such as LAN/SFP port, VLAN interface, and QoS. To enter individual configuration mode, issue the command for transitioning to the respective mode from global configuration mode.

The following items individual configuration mode are available for SWX3220. Some of the modes within individual configuration mode have a hierarchy. For example, policy map mode → policy map class mode.

individual configuration mode	Transition command	Prompt
interface mode	**interface** command	SWX3220(config-if)#
line mode	**line con** command **line vty** command	SWX3220(config-line)#
VLAN mode	**vlan database** command	SWX3220(config-vlan)#
VLAN access map mode	**vlan access-map** command	SWX3220(config-vlan-access-map)#
MST mode	**spanning-tree mst configuration** command	SWX3220(config-mst)#
class map mode	**class-map** command	SWX3220(config-cmap)#
policy map mode	**policy-map** command	SWX3220(config-pmap)#
policy map class mode	**class** command	SWX3220(config-pmap-c)#
aggregate policer mode	**aggregate-police** command	SWX3220(config-agg-policer)#
L2MS mode	**l2ms configuration** command	SWX3220(config-l2ms)#
LLDP agent mode	**lldp-agent** command	SWX3220(lldp-agent)#
OSPFv2 mode	**router ospf** command	SWX3220(config-router)#
OSPFv3 mode	**router ipv6 ospf** command	SWX3220(config-router)#
RIP mode	**router rip** command	SWX3220(config-router)#
RIPng mode	**router ipv6 rip** command	SWX3220(config-router)#
key chain mode	**key chain** command	SWX3220(config-keychain)#
key chain key mode	**key** command	SWX3220(config-keychain-key)#
VRRP mode	**router vrrp** command	SWX3220(config-router)#
VRRP mode(IPv6)	**router ipv6 vrrp** command	SWX3220(config-router)#
Route map mode	**route-map** command	SWX3220(config-route-map)#
DHCP mode	**dhcp pool** command	SWX3220(config-dhcp)#
DHCP class mode	**dhcp class** command	SWX3220(config-dhcp-class)#
DHCP pool class mode	**dhcp pool class** command	SWX3220(config-dhcp-pool-class)#
DHCPv6 mode	**dhcpv6 pool** command	SWX3220(config-dhcp6)#
E-mail template mode	**mail template** command	SWX3220(config-mail)#
Schedule template mode	**schedule template** command	SWX3220(config-schedule)#
RADIUS configuration mode	**radius-server local-profile** command	SWX3220(config-radius)#
BGP mode	**bgp** command	SWX3220(config-router)#

individual configuration mode	Transition command	Prompt
BGP IPv6 address-family mode	**address-family** command	SWX3220(config-radius-af)#

2.4.3 Command prompt prefix

he command prompt prefix indicates the host name. In the default state, the host name is the model name "SWX3220". This indication can be changed by using the **hostname** command to specify the host name. In cases where multiple SWX3220 units are used, management will be easier if separate names are assigned to each switch.

Changing the host name

```
SWX3220(config)# hostname Switch-012
Switch-012(config)#
```

2.4.4 Executing commands of a different input mode

Because the commands that can be used on the SWX3220 differ depending on the mode, you must transition to the mode in which a command can be executed before you execute that command. The **do** command is provided as a way to avoid this requirement.

By using the **do** command you can execute privileged EXEC mode commands from any configuration mode. This allows you to reference the current configuration or save settings from any configuration mode without having to transition to privileged EXEC mode.

However, since the completion function cannot be used with **do**, you must enter the command that follows either in its full spelling or in its abbreviated form.

- Entry in full spelling

  ```
  SWX3220(config)#do show running-config
  ```
- Entry in abbreviated form

  ```
  SWX3220(config)#do sh ru
  ```

2.5 Keyboard operations when using the console

2.5.1 Basic operations for console input

The SWX3220 allows the following operations in the command line.

- Moving the cursor

Keyboard operation	Description and notes
→	Move right one character
←	Move left one character
Press Esc, then F	Move right one word (move to the character following the end of the word at the cursor location)
Press Esc, then B	Move left one word (move to the first character of the word at the cursor location)
Ctrl + A	Move to the beginning of the line
Ctrl + E	Move to the end of the line

- Deleting an input character

Keyboard operation	Description and notes
Backspace	Delete the character at the left of the cursor
Ctrl + H	
Ctrl + D	Delete the character at the cursor. If this operation is performed when the command line is empty, the result is the same as the **exit** command.
Press Esc, then D	Delete from the cursor position until immediately before the first space
Ctrl + K	Delete from the cursor position until the end of the line

Keyboard operation	Description and notes
Ctrl + U	Delete all characters that are being entered

- Other

Keyboard operation	Description and notes
Ctrl + T	Exchange the character at the cursor position with the preceding character. If the cursor is at the end of the line, exchange the preceding character with the character that precedes it.
Ctrl + C	In unprivileged EXEC mode and privileged EXEC mode, discard the command being entered and move to the next line. In individual configuration mode, discard the command line being entered and move to privileged EXEC mode. Command processing that is currently being executed will be stopped. (ex: **ping** command)
Ctrl + Z	Move from individual configuration mode to privileged EXEC mode. This is the same operation as the **end** command.

2.5.2 Command help

By entering '?' in the command line you can search for the available commands or parameters.

```
SWX3220#show vlan ?
  <1-4094>      VLAN id
  access-map    Show VLAN Access Map
  brief         VLAN information for all bridges (static and dynamic)
  filter        Show VLAN Access Map Filter
  private-vlan  private-vlan information

SWX3220#show vlan
```

2.5.3 Input command completion and keyword candidate list display

If you press the "Tab" key while entering a command in the console, the command name is completed. If you press the "Tab" key after entering a keyword, a list of keyword candidates that can be entered next is shown. The same operation can also be performed by pressing the "Ctrl + I" key.

- Command name completion

```
SWX3220#con "press the <Tab>key"
      ↓
SWX3220#configure
```

- Keyword candidate list display

```
SWX3220(config)#vlan "press the <Tab> key"
access-map  database    filter
SWX3220(config)#vlan
```

2.5.4 Entering command abbreviations

When you enter commands or parameters in abbreviated form, and the characters you entered can be recognized unambiguously as a command or parameter, that command is executed.

Example of entering a command abbreviation (show running-config)

```
SWX3220# sh run
```

2.5.5 Command history

By using the command history function, you can easily re-execute a command that you previously input, or partially modify a previously input command and re-execute it. Command history is shown as a history that is common to all modes.

Operation is shown below.

Keyboard operation	Description and notes
↑	Move backward through command history
Ctrl + P	
↓	Move forward through command history
Ctrl + N	

2.6 Commands that start with the word "show"

2.6.1 Modifiers

Modifiers send the information produced by the **show** command through a filter, restricting the content that is shown in the screen and making it easier for you to see the desired information.

The SWX3220 provides the following three modifiers for the **show** command.

Modifiers	Description
include	Output only the lines that include the specified character string
grep	
exclude	Output only the lines that do not include the specified character string

Modifiers can be used only one at a time. You cannot specify more than one modifier.

- (Example) Using **show running-config** to view information that includes VLAN #1 (vlan1).

```
SWX3220#show running-config | grep vlan1
interface vlan1
http-server interface vlan1
telnet-server interface vlan1
```

- (Example) Using **show spanning-tree** to view information that includes Role.

```
SWX3220# show spanning-tree | include Role
%   po1: Port Number 505 - Ifindex 4601 - Port Id 0x81f9 - Role Disabled - State
Discarding
%   port1.1: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - Role Disabled -
State Forwarding
%   port1.2: Port Number 906 - Ifindex 5002 - Port Id 0x838a - Role Disabled -
State Forwarding
%   port1.3: Port Number 907 - Ifindex 5003 - Port Id 0x838b - Role Disabled -
State Forwarding
%   port1.4: Port Number 908 - Ifindex 5004 - Port Id 0x838c - Role Disabled -
State Forwarding
%   port1.6: Port Number 910 - Ifindex 5006 - Port Id 0x838e - Role Disabled -
State Forwarding
%   port1.7: Port Number 911 - Ifindex 5007 - Port Id 0x838f - Role Disabled -
State Forwarding
%   port1.8: Port Number 912 - Ifindex 5008 - Port Id 0x8390 - Role Disabled -
State Forwarding
%   port1.9: Port Number 913 - Ifindex 5009 - Port Id 0x8391 - Role Disabled -
State Forwarding
%   port1.10: Port Number 914 - Ifindex 5010 - Port Id 0x8392 - Role Disabled -
State Forwarding
```

Chapter 3

Configuration

3.1 Manage setting values

The SWX3220 uses the following configurations to manage its settings.

Types of configuration	Description	User operations that can be performed
Running configuration (running-config)	Setting values currently used for operation. Managed in RAM.	Note / Save to startup configuration
Startup configuration (startup-config)	These are the saved setting values. This manages 2 configurations in Flash ROM and 1 configuration on an SD card. The data in Flash ROM to be used is determined using the **startup-config select** command. The configuration on the SD card is managed in the following folder. - SWX3220-16MT or SWX3220-16TMs : "/swx3220/startup-config" - SWX3220-30MC : "/swx3220-30mc/startup-config" - SWX3220-30TCs : "/swx3220-30tcs/startup-config"	Note / Delete / Copy
Default configuration (default-config)	Default setting values. Managed in Flash ROM.	No operations possible

The start-up flow for the SWX3220 system is as follows.

1. The setting value of the **startup-config select** command is referenced to determine the startup config that will be used.
   If "sd" is specified by the **startup-config select** command, and an SD card on which a startup config is saved is not inserted, startup config #0 is selected.
2. If the startup configuration that was selected exists, the data in question is deployed to RAM as a running configuration.
   If the startup configuration file that was selected according to the setting values in the **startup-config select** command does not exist in Flash ROM, the default configuration is deployed to RAM.

If commands etc. are used to modify the settings while the SWX3220 is running, the modified settings are immediately reflected in the running configuration. After modifying the running configuration, executing the **write** or **copy** command will update the startup configuration. If you restart without saving the content that was specified or modified, the settings or modifications are lost. Please be aware of this.

3.2 Default value

The default setting values for the SWX3220 are shown in the table below.

Note that the default values listed in this documentation are not applied for the factory settings, but the default settings listed below for each command are used instead.

- Default setting values for the entire system

Category	Setting item	Default value
CONFIG	CONFIG used at startup	Startup config in SD card
Terminal settings	Console timeout	600 sec
	Number of VTYs	8
	Number of lines displayed	24

Category	Setting item	Default value
Password	Login password of no user	none
	Privileged password	admin
	Password encryption	not encrypted
Time management	Time zone	JST (UTC + 9.0H)
	NTP server	none
	NTP update cycle	once per hour
RMON	Behavior	enabled
sFlow	Behavior	disabled
Firmware update	Download URL	• SWX3220-16MT、SWX3220-16TMs firmware-update url http://www.rtpro.yamaha.co.jp/firmware/revision-up/swx3220.bin • SWX3220-30MC firmware-update url http://www.rtpro.yamaha.co.jp/firmware/revision-up/swx3220-30mc.bin • SWX3220-30TCs firmware-update url http://www.rtpro.yamaha.co.jp/firmware/revision-up/swx3220-30tcs.bin
	Allow revision-down	don't allow
	Timeout	300 sec
LLDP	Behavior	enabled
	Automatically set	enabled
L2MS	Behavior	enabled
	Role	agent
SYSLOG	Debug level log output	OFF
	Information level log output	ON
	Error level log output	ON
	SYSLOG server	none
Access control	Telnet server status	run
	Telnet server access	allow only VLAN #1
	SSH server status	do not run
	TFTP server status	do not run
	HTTP server status	run
	HTTP server access	allow only VLAN #1
	Secure HTTP server status	do not run
Maintenance VLAN	VLAN interface	VLAN #1

Category	Setting item	Default value
L2 switching	Automatic MAC address learning	enabled
	Automatic MAC address learning aging time	300 sec
	Spanning tree	enabled
	Proprietary loop detection	disabled
	Multiple VLANs	None
	Transparent YMPI frames for multiple VLANs	None
DNS cliant	Behavior	enabled
Interface control	PoE power supply	-
Traffic control	QoS	disabled
	Flow control (IEEE 802.3x)	disabled
Web GUI	Language setting	Japanese (selectable)
Stack	Operation	Disabled
	Stack ID	1
	Range of IP addresses used by the stack port	192.168.250.0/24
Buzzer	Enabled	Disabled
	Buzzer triger	All disabled

- Default settings per LAN/SFP port

Category	Setting item	Default value
Common setting	Speed/duplex mode setting	auto
	Cross/straight automatic detection	enabled
	MRU	1,522 Byte
	Port description	none
	EEE	disabled
	Port Mode	Access
	Associated VLAN ID	1 (default VLAN)
L2MS	L2MS filter	disabled
L2 switching	Spanning tree	enabled
	Proprietary loop detection	enabled
Traffic control	QoS trust mode	CoS
	Flow control (IEEE 802.3x)	disabled
	Storm control	disabled
PoE power supply	Power supply operation	-
	Power supply priority	-
LLDP agent	Transmit/Receive mode	transmit and receive
	Basic management TLV	enabled

- Settings for the default VLAN (vlan1)

Category	Setting item	Default value
Layer3 function	IPv4 address	192.168.100.240/24

Category	Setting item		Default value
IP multicast	Multicast frame forwarding		239.192.128.250 (for Y-UNOS)
	IGMP Snooping	Behavior	disabled
		Querier	disabled
		Fast-Leave	disabled
		Check TTL	enabled
		Check RA	disabled
		Check ToS	disabled
		Report-Suppression	enabled
		Report-Foward	disabled
		Mrouter-Port Data-Suppression	disabled
	MLD Snooping	Behavior	disabled
		Querier	disabled
		Fast-Leave	disabled
		Report-Suppression	enabled

3.3 Preset

For SWX3220-30MC and SWX3220-30TCs, you can use DIP switch to easily make the settings that are optional for AVoIP networks that transmit audio and video traffic such as Dante or NDI.

Simple presets for each network environment are provided, so that you can make settings and perform switching without logging into this product.

The presets are applied without saved settings (factory default settings), such as those saved by the **write** command. To apply the presets, you must revert the SWX3220 back to its factory default state.

The configurable preset types are as follows.

- DIP switch #1–#4 settings

  Sets the preset type. If specialized settings for an AVoIP network are unnecessary, set this to "Normal", the basic switch setting.

DIP switch				Preset type	Content
#1	#2	#3	#4		
OFF	OFF	OFF	OFF	Normal	Basic switch settings
ON	OFF	OFF	OFF	Dante type A	Optimal Dante settings (basic settings)
OFF	ON	OFF	OFF	Dante type B	Optimal Dante settings (basic settings + trunk port)
ON	ON	OFF	OFF	Dante type C	Optinal Dante settings (basic settings + L2MS/BPDU filter)
OFF	OFF	ON	OFF	ADECIA	Settings for ADECIA link
ON	OFF	ON	OFF	NDI	Optimal NDI settings

DIP switch				Preset type	Content
#1	#2	#3	#4		
OFF	ON	ON	OFF	SDVoE	Optimal SDVoE settings
ON	ON	ON	OFF	IPMX	Optimal IPMX settings
OFF	OFF	OFF	ON	SMPTE ST 2110 with PTP TC	Optimal SMPTE ST 2110 (PTP TC) settings
ON	OFF	OFF	ON	Extron NAV	Optional Extron NAV settings

- DIP switch #7 settings

  Enables/disables L2MS functionality. This setting is applied when a preset aside from Normal is applied.

DIP switch #7	Function
ON	L2MS function enabled
OFF	L2MS function disabled

- DIP switch #8 settings

  Sets whether the LED is lit/unlit. This setting is applied when a preset aside from Normal is applied.

DIP switch #8	Function
ON	LED lights up
OFF	LED goes dark

To check the current DIP switch state, you can use the **show dipsw** command.

Chapter 4

Maintenance and operation functions

4.1 Passwords

4.1.1 Set privileged password

[Syntax]

enable password *password*

[Parameter]

password : Privileged password

Single-type alphanumeric characters and " and ' and | and > and ? and single-byte symbols other than space characters (Within 8–32 characters)

The first character must be a single-byte alphanumeric character

[Initial value]

enable password admin

[Input mode]

global configuration mode

[Description]

Specifies the password needed to enter privileged EXEC mode.

You cannot change it to the default password, "admin".

[Note]

If the password was encrypted by the **password-encryption** command, it is shown in the configuration in the form "**enable password** 8 *password*."

The user cannot enter the password in this form when making configuration settings from the command line. As "8" is a reserved character, you cannot set a password of "8" alone.

Automatically set the default password (admin) if no privileged password is set at boot.

[Example]

Specify admin1234 as the privileged password.

```
SWX3220(config)#enable password admin1234
```

4.1.2 Encrypt password

[Syntax]

password-encryption *switch*
no password-encryption

[Parameter]

switch : Set password encryption

Setting value	Description
enable	Encrypt
disable	Don't encrypt

[Initial value]

password-encryption disable

[Input mode]

global configuration mode

[Description]

Enables password encryption.

If this is enabled, the password entered by the **password** command, the **enable password** command, and the **username** command are saved in the configuration in an encrypted form.

If this command is executed with the "no" syntax, password encryption is disabled, and the password entered by the **password** command, the **enable password** command, and the **username** command are saved in the configuration as plaintext.

[Note]

If password encryption is changed from disabled to enabled, previously-entered passwords are converted from plaintext to an encrypted form; however if it is changed from enabled to disabled, previously-encrypted passwords in a configuration file do not return to plaintext.

[Example]

Enables password encryption.

```
SWX3220(config)#password-encryption enable
```

Disabled password encryption.

```
SWX3220(config)#no password-encryption
```

4.2 User account maintenance

4.2.1 Set user

[Syntax]

username *username* [privilege *privilege*] password *password*
no username *username*

[Keyword]

privilege	:	Specifies the user's privileges
password	:	Specifies the user's password

[Parameter]

username : User name

Single-byte alphanumeric characters (32 characters or less)

privilege : Whether to grant privilege

Setting value	Description
on	Password input is not requested when moving to privileged EXEC mode Access to Web GUI is allowed with administrator privileges
off	Password input is requested when moving to privileged EXEC mode Access to Web GUI is allowed with guest

password : User's login password

Single-type alphanumeric characters and " and ' and | and > and ? and single-byte symbols other than space characters (Within 8–32 characters)

The first character must be a single-byte alphanumeric character

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Sets user information.

A maximum of 33 items of user information can be registered. However, while there can be up to 32 privilege off users, 1 privilege on user is required.

The following words cannot be registered as user names.

lp, adm, bin, ftp, gdm, man, rpc, sys, xfs, halt, mail, news, nscd, sync, uucp, root, sshd, games, daemon, gopher, nobody, ftpuser, mtsuser, rpcuser, mailnull, operator, shutdown

The default password of "admin" cannot be used as a password.

[Note]

If the password was encrypted by the **password-encryption** command, it is shown in the configuration in the form "**username** *username* password 8 *password*."

The user cannot enter the password in this form when making configuration settings from the command line. As "8" is a reserved character, you cannot set a password of "8" alone.

At boot, if no privilege on user has been set, a default administrator (admin/admin) is added.

At boot, users who do not have a password set will have their password set to the same string as the user name.

[Example]

Set the user "**user1234**".

```
SWX3220(config)#username user1234 password user_pass
```

Set the privilege on user **user1234** .

```
SWX3220(config)#username user1234 privilege on password user_pass
```

4.2.2 Changing User Permissions

[Syntax]

username *username* privilege *privilege*

[Keyword]

privilege : Specifies user permissions

[Parameter]

username : User name

Up to 32 half-width alphanumeric characters

privilege : Whether or not privileges are granted

Setting value	Description
on	Users will not be prompted to enter a password when switching to privileged EXEC mode Web GUI can be accessed with Administrator permissions
off	Users will be prompted to enter a password when switching to privileged EXEC mode Web GUI can be accessed with Guest permissions

[Initial value]

None

[Input mode]

global configuration mode

[Description]

Permissions of a registered users can be changed.

[Note]

Cannot be configured for unregistered users.

[Example]

Grants privileges to **user1234** registered users.

```
SWX3220(config)#username user1234 privilege on
```

4.2.3 Show login user information

[Input mode]

unprivileged EXEC mode, privileged EXEC mode, global configuration mode

[Description]

Shows information on the current logged-in users.

The following items are shown.

Item	Description
Line	Shows the login method. **con 0** is the serial console port **vty N** is the VTY port **stk N** is the remote login port **http N** is the Web GUI
Own	An * is shown for the line of one's own connection port.
User	Shows the currently logged-in user names.
Status	Shows the login status. If the user is in use, this indicates **Login**.
Login time	Shows the login time.
IP address	Shows the IP address of the connected user.

[Example]

Show login information for the users when the stack function is disabled.

```
SWX3220>show users

  Line    Own  User                                Status  Login time  IP address
-------------------------------------------------------------------------------------
---------
  con  0       user1234                            Login   02:15:23
  vty  0  *    operators1                          Login   00:12:59    192.168.100.1
  vty  1       abcdefghijklmnopqrstuvwxyzabcdef    Login   00:00:50    192.168.100.24
  vty  2       -                                   Login   00:00:21    192.168.100.10
  vty  3       -                                   -       -
  vty  4       -                                   -       -
  vty  5       -                                   -       -
  vty  6       -                                   -       -
  vty  7       -                                   -       -
  http 0       user1234                            Login   01:12:25    192.168.100.4
  http 1       (noname)                            Login   00:18:04    192.168.100.102
  http 2       -                                   -       -
  http 3       -                                   -       -
```

Show login information for the users when the stack function is enabled.

```
SWX3220>show users

  Line    Own  User                                Status  Login time  IP address
-------------------------------------------------------------------------------------
---------
  con  0       user1234                            Login   02:15:23
  vty  0  *    operators1                          Login   00:12:59    192.168.100.1
  vty  1       abcdefghijklmnopqrstuvwxyzabcdef    Login   00:00:50    192.168.100.24
```

```
  vty  2       -                                Login   00:00:21    192.168.100.10
  vty  3       -                                -       -
  vty  4       -                                -       -
  vty  5       -                                -       -
  vty  6       -                                -       -
  vty  7       -                                -       -
  stk  0       -                                Login   00:33:11
  stk  1       -                                -       -
  stk  2       -                                -       -
  stk  3       -                                -       -
  http 0       user1234                         Login   01:12:25    192.168.100.4
  http 1       (noname)                         Login   00:18:04    192.168.100.102
  http 2       -                                -       -
  http 3       -                                -       -
```

4.2.4 Set banner

[Syntax]

banner motd *word*
no banner motd

[Parameter]

word	:	Single-byte alphanumeric characters and single-byte symbols (256 characters or less)

[Initial value]

no banner motd

[Input mode]

global configuration mode

[Description]

Sets the banner that is displayed when logging in to the console.

[Example]

Set the banner display to "Hello World!".

```
Username:
Password:

SWX3220 Rev.4.02.02 (Mon Dec 14 12:07:35 2020)
  Copyright (c) 2021 Yamaha Corporation. All Rights Reserved.

SWX3220>enable
SWX3220#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWX3220(config)#banner motd Hello World!
SWX3220(config)#exit
SWX3220#exit

Username:
Password:

Hello World!

SWX3220>enable
SWX3220#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWX3220(config)#no banner motd
SWX3220(config)#exit
SWX3220#exit

Username:
Password:

SWX3220 Rev.4.02.02 (Mon Dec 14 12:07:35 2020)
  Copyright (c) 2021 Yamaha Corporation. All Rights Reserved.

SWX3220>
```

4.3 Configuration management

4.3.1 Save running configuration

[Syntax]

copy running-config startup-config [*config_num*]

[Parameter]

config_num : Configuration number

Setting value	Description
<0-1>	Startup configuration #0-#1
sd	Startup config in SD card

[Input mode]

privileged EXEC mode

[Description]

Saves the current operating settings (running configuration) as the settings for startup (startup configuration).

If *config_num* is omitted, it is saved in the startup config that was used for the current startup.

[Note]

The running configuration can also be saved by executing the **write** command and **save** command.

In a state in which the SD card is not mounted, executing this command on a config that is in the SD card produces an error.

When stack is enabled, this can be executed only on the main switch (Active status).

[Example]

Save the running configuration.

```
SWX3220#copy running-config startup-config
Succeeded to write configuration
SWX3220#
```

4.3.2 Save running configuration

[Syntax]

write [*config_num*]
save [*config_num*]

[Parameter]

config_num : Configuration number

Setting value	Description
<0-1>	Startup configuration #0-#1
sd	Startup config in SD card

[Input mode]

privileged EXEC mode, individual configuration mode

[Description]

Saves the current operating settings (running configuration) as the settings for startup (startup configuration).

If *config_num* is omitted, it is saved in the startup config that was used for the current startup.

[Note]

The running configuration can also be saved by executing the **copy running-config startup-config** command.

In a state in which the SD card is not mounted, executing this command on a config that is in the SD card produces an error.

When stack is enabled, this can be executed only on the main switch (Active status).

[Example]

Save the running configuration.

```
SWX3220#write
Succeeded to write configuration.
SWX3220#
```

4.3.3 Show the running configuration

[Syntax]

show running-config [*section*]
show config

[Parameter]

section : Section to be shown

Setting value	Description
access-list	Access list related
dhcp	DHCP server related
dhcp-relay	DHCP relay related
dhcpv6	DHCPv6 server-related
dns-forwarding	DNS relay-related
http-server	HTTP server related
interface	Interface related
ip	IP related
ipv6	IPv6 related
key	Authentication key related
l2ms	L2MS related
lldp	LLDP related
mail	E-mail notification-related
multicast	Multicast related
pim	PIM related
radius-server	RADIUS server related
router	Router setting related
router-id	Router ID related
schedule	Schedule related
sflow	sFlow-related
snmp	SNMP related
spanning-tree	STP related
ssh-server	SSH server related
telnet-sever	TELNET server related

[Input mode]

privileged EXEC mode, individual configuration mode

[Description]

Shows the currently-operating settings (running configuration).

If *section* is not specified, all settings are shown.

[Example]

Show the running configuration.

```
SWX3220#show running-config
!
interface port1.1
 switchport
...
!
line con 0
line vty 0 7
!
end

SWX3220#
```

4.3.4 Show startup configuration

[Syntax]

show startup-config [*config_num*]
show config [*config_num*]

[Parameter]

config_num : Configuration number

Setting value	Description
<0-1>	Startup configuration #0-#1
sd	Startup config in SD card

[Input mode]

privileged EXEC mode

[Description]

Shows the startup settings (startup configuration).

If *config_num* is omitted, the following are displayed.

- show startup-config: Displays the startup configuration for the currently operating configuration number.

- show config: Shows the currently operating running configuration.

[Note]

In a state in which the SD card is not mounted, executing this command on a config that is in the SD card produces an error.

[Example]

Show the startup configuration on the next startup.

```
SWX3220#show startup-config
!
!  Last Modified: 00:00:00 JST Mon Jan 01 2018
!
interface port1.1
 switchport
 switchport mode access
 no shutdown
!

...

!
interface vlan1
 no switchport
 ip address 192.168.100.240/24
 no shutdown
!
clock timezone JST
!
http-server enable
http-proxy enable
!
telnet-server enable
!
```

```
line con 0
line vty 0 7
!
end

SWX3220#
```

4.3.5 Erase startup configuration

[Syntax]

erase startup-config [*config_num*]

[Parameter]

config_num : Configuration number

Setting value	Description
<0-1>	Startup configuration #0-#1
sd	Startup config in SD card

[Input mode]

privileged EXEC mode

[Description]

Erase the settings used at startup (startup config) and the information associated with them.

If *config_num* is omitted, the startup config that was used for the current startup is erased.

[Note]

In a state in which the SD card is not mounted, executing this command on a config that is in the SD card produces an error.

[Example]

Erase the startup configuration.

```
SWX3220#erase startup-config
Succeeded to erase configuration.
SWX3220#
```

4.3.6 Copy startup configuration

[Syntax]

copy startup-config *src_config_num dst_config_num*

[Parameter]

src_config_num : Copy source configuration number

Setting value	Description
<0-1>	Startup configuration #0-#1
sd	Startup config in SD card

dst_config_num : Copy destination configuration number

Setting value	Description
<0-1>	Startup configuration #0-#1
sd	Startup config in SD card

[Input mode]

privileged EXEC mode

[Description]

Copy the startup settings (startup config) and the information associated with them.

[Note]

In a state in which the SD card is not mounted, executing this command on a config that is in the SD card produces an error.

[Example]

Copy startup config #0 to startup config #1.

```
SWX3220#copy startup-config 0 1
Succeeded to copy configuration
SWX3220#
```

4.3.7 Select startup config

[Syntax]

startup-config select *config_num*
no startup-config select

[Parameter]

config_num : Configuration number

Setting	Description
<0-1>	Startup config #0-#1
sd	Startup config on the SD card

[Initial value]

startup-config select sd

[Input mode]

privileged EXEC mode

[Description]

Select the settings to use at startup (startup config), and restart.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

At startup, if "sd" is specified as *config_num* and an SD card on which a startup config is saved is not inserted, startup config #0 is selected.

This command cannot be used if the stack function is enabled.

[Example]

Select startup config #1 and restart.

```
SWX3220#startup-config select 1
reboot system? (y/n): y
```

4.3.8 Set description for startup config

[Syntax]

startup-config description *config_num line*
no startup-config description *config_num*

[Parameter]

config_num : <0-1>

Configuration number

line : Single-byte alphanumeric characters and single-byte symbols (63 characters or less)

Description for applicable startup config

[Input mode]

privileged EXEC mode

[Description]

Specify a description for the applicable startup config.

If this command is executed with the "no" syntax, the description is deleted.

The description is shown at the beginning of the execution result of the **show startup-config** command.

[Example]

Specify a description for startup config #1.

```
SWX3220#startup-config description 1 TEST_CONFIG_1
```

4.4 Manage boot information

4.4.1 Show boot information

[Syntax]

show boot *num*
show boot all
show boot list

[Keyword]

all	:	Shows up to five entries of the boot information history
list	:	Shows a simplified version of up to five entries of the boot information history

[Parameter]

num	:	<0-4> Shows the boot history entry of the specified number

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Show the boot information.

[Note]

This history is cleared when you execute the **cold start** command or the **clear boot list** command.

[Example]

Show the current boot information.

```
SWX3220>show boot
 Running EXEC: SWX3220 Rev.4.02.02 (Mon Dec 14 12:07:35 2020)
Previous EXEC: SWX3220 Rev.4.02.02 (Mon Dec 14 12:07:35 2020)
Restart by reload command
```

Shows a list of the boot history.

```
SWX3220>show boot list
No. Date       Time     Info
--- ---------- -------- --------------------------------------------------
  0 2018/03/15 09:50:29 Restart by reload command
  1 2018/03/14 20:24:40 Power-on boot
--- ---------- -------- --------------------------------------------------
```

4.4.2 Clear boot information

[Syntax]

clear boot list

[Input mode]

privileged EXEC mode

[Description]

Clears the boot information history.

[Example]

Clear the boot information.

```
SWX3220#clear boot list
```

4.4.3 Set SD card boot

[Syntax]

boot prioritize sd *switch*
no boot prioritize sd

[Parameter]

switch : Enable or disable SD card boot

Setting	Description
enable	Enable SD card boot
disable	Disable SD card boot

[Initial value]

boot prioritize sd enable

[Input mode]

privileged EXEC mode

[Description]

Enable or disable the SD card boot function of the firmware.

After this command is executed, the system will restart.

Since this setting is common to the system, it cannot be specified individually for each startup configuration (startup-config #0 ~ strtup-config #1).

By default, SD card boot is enabled.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

The SD card boot function enabled/disabled status can be viewed by using the **show boot prioritize sd** command.

[Example]

Enable the SD card boot function of the firmware.

```
SWX3220#boot prioritize sd enable
reboot system? (y/n): y
```

4.4.4 Configuring the SD card boot auto-apply function

[Syntax]

boot auto-apply *switch*

[Parameter]

switch : Enable or disable the SD card boot auto-apply function

Setting value	Description
enable	Enable or disable the SD card boot auto-apply function
disable	Disables the SD card boot auto-apply function.

[Initial value]

boot auto-apply enable

[Input mode]

privileged EXEC mode

[Description]

Enables or disables the SD card boot auto-apply function.

The state of this function can be checked with the **show environment** command.

[Example]

Disables the SD card boot auto-apply function.

```
SWX3220#boot auto-apply disable
```

4.4.5 Show the SD card boot setting information

[Syntax]

show boot prioritize sd

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the setting of the SD card boot function.

[Example]

Show the setting of the SD card boot function.

```
SWX3220#show boot prioritize sd
SD boot configuration:
  firmware  :  enable
```

4.5 Show unit information

4.5.1 Show inventory information

[Syntax]

show inventory

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows inventory information for this unit and the SFP modules.

The following items are shown.

Item	Description
NAME	Name
DESCR	Description
Vendor	Vendor name
PID	Product ID
VID	Version ID, 0 if invalid
SN	Serial number

[Example]

Show inventory information.

```
SWX3220>show inventory
NAME: L3 switch
DESCR: SWX3220-16MT
Vendor: Yamaha
PID: SWX3220-16MT
VID: 0000
SN: S00000000

SWX3220>
```

4.5.2 Show operating information

[Syntax]

show environment

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows information about the system's operating environment.

The following items are shown.

- Model name
- Boot version
- Firmware revision
- Board version
- Destination
- Serial number
- Device ID
- MAC address
- CPLD version
- PHY version
- PSU version (only for models that support the power redundancy function)
- CPU usage ratio
- Memory usage ratio
- SD card mount status
- Fan status
- Fan speed
- Temperature status
- Temperature
- Status of power supply unit (only for models that support the power redundancy function)
- Firmware file
- Startup configuration file
- Configuring the SD card boot auto-apply function
- Serial baud rate
- Boot time
- Current time
- Elapsed time from boot

[Example]

Show operating information.

```
SWX3220>show environment
[Device]
  Model              : SWX3220-16MT
  BootROM version    : 1.00
  Firmware version   : Rev.4.02.20 (Mon Sep  1 00:00:00 2025)
  Board version      : 00
  Destination        : 00 (-)
  Serial             : S00000000
  Device ID          : 0000000-0000000-0000000-00000
  MAC-Address        : ac44.f200.0000
  CPLD version       : 00
  PHY version        : 10.5.0.0

[Status]
  CPU                : 1%(5sec)  1%(1min)  1%(5min)
  Memory             : 8% used
  SD card            : Unmounted
  Fan status         : Normal
      speed          : FAN1:5882rpm  FAN2:6047rpm  FAN3:5825rpm
  Temperature status : Normal
              value  : 31 degree C

[Configuration]
  Startup firmware           : exec0
  Startup Configuration file : config0
               selected file : config(SD)
  Boot auto-apply            : Enable
  Serial Baudrate            : 9600
```

```
[Time]
  Boot time                  : 2025/09/01 11:13:00 +09:00
  Current time               : 2025/09/02 16:18:00 +09:00
  Elapsed time from boot     : 1days 05:05:00
```

4.5.3 Disk usage status

[Syntax]

show disk-usage

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the usage status of the disk used by the system.

- System : Area used by the system
- Config : Settings information area
- Temporary : Temporary area

[Example]

Shows the usage status of the disk used by the system.

```
SWX3220#show disk-usage
  Category    Total    Used     Free     Used (%)
  ----------- -------- -------- -------- --------
  System        46.1M     2.2M    41.5M       5%
  Config       103.4M     2.5M    96.2M       2%
  Temporary     80.0M   152.0K    79.9M       0%
```

4.5.4 Show currently-executing processes

[Syntax]

show process

[Input mode]

privileged EXEC mode

[Description]

Shows all currently-executing processes.

[Example]

Show currently-executing processes.

```
SWX3220#show process
```

4.5.5 Display memory usage

[Syntax]

show memory

[Input mode]

privileged EXEC mode

[Description]

Shows how much memory is used by each process.

The following items are shown.

Item	Explanation
PID	Process ID
NAME	Process name
%MEM	Percentage of physical memory used
SIZE	Amount of physical memory used (current value)

Item	Explanation
PEAK	Amount of physical memory used (maximum value until now)
DATA	Size of dynamic virtual memory area
STK	Stack size

[Example]

This shows how much memory is used by each process.

```
SWX3220#show memory
```

4.5.6 Show technical support information

[Syntax]

show tech-support

[Input mode]

privileged EXEC mode

[Description]

Show technical support information. The technical support information includes a list of the results of executing the following commands.

If stack functions are enabled, technical support information for all devices configured for the stack is shown.

Note that the commands executed using a main switch or member switch are different. Refer to the command list below for details.

Command	Stack disabled	Stack enabled	
		Main switch	Member switch
show environment	✓	✓	✓
show running-config	✓	✓	✓
show startup-config	✓	✓	✓
show stack	✓	✓	✓
show system-diagnostics	✓	✓	✓
show clock detail	✓	✓	-
show disk-usage	✓	✓	✓
show dipsw	✓ (*1)	✓ (*1)	✓ (*1)
show inventory	✓	✓	✓
show power-supply	✓ (*2)	✓ (*2)	-
show boot all	✓	✓	✓
show boot prioritize sd	✓	✓	✓
show fan history	✓	✓	✓
show logging	✓	✓	✓
show process	✓	✓	✓
show users	✓	✓	✓
show interface	✓	✓	-
show frame-counter	✓	✓	-
show vlan brief	✓	✓	-
show spanning-tree mst detail	✓	✓	-

Command	Stack disabled	Stack enabled	
		Main switch	Member switch
show etherchannel status detail	✓	✓	-
show loop-detect	✓	✓	-
show mac-address-table	✓	✓	-
show l2ms detail	✓	✓	-
show qos queue-counters	✓	✓	-
show ddm status	✓	✓	✓
show errdisable	✓	✓	-
show auth status	✓	✓	-
show auth supplicant	✓	✓	-
show error port-led	✓	✓	-
show ip interface brief	✓	✓	-
show ip forwarding	✓	✓	-
show ipv6 interface brief	✓	✓	-
show ipv6 dhcp interface	✓	✓	-
show ipv6 forwarding	✓	✓	-
show ip route	✓	✓	-
show ip route database	✓	✓	-
show ip route pbr	✓	✓	-
show ipv6 route	✓	✓	-
show ipv6 route database	✓	✓	-
show ipv6 route pbr	✓	✓	-
show arp	✓	✓	-
show ipv6 neighbors	✓	✓	-
show ip rip	✓	✓	-
show ip rip interface	✓	✓	-
show ipv6 rip	✓	✓	-
show ipv6 rip interface	✓	✓	-
show ip ospf	✓	✓	-
show ip ospf database	✓	✓	-
show ip ospf interface	✓	✓	-
show ip ospf neighbor	✓	✓	-
show ip ospf route	✓	✓	-
show ipv6 ospf	✓	✓	-
show ipv6 ospf database	✓	✓	-
show ipv6 ospf interface	✓	✓	-
show ipv6 ospf neighbor	✓	✓	-
show ipv6 ospf route	✓	✓	-
show ip bgp	✓	✓	-
show ip bgp neighbors	✓	✓	-

Command	Stack disabled	Stack enabled	
		Main switch	Member switch
show ipv6 bgp	✓	✓	-
show ipv6 bgp neighbors	✓	✓	-
show ip mroute	✓	✓	-
show ip mroute summary	✓	✓	-
show ip mroute count	✓	✓	-
show ip igmp groups	✓	✓	-
show ip igmp interface	✓	✓	-
show ip igmp ssm-map	✓	✓	-
show ip pim bsr-router	✓	✓	-
show ip pim interface detail	✓	✓	-
show ip pim mroute detail	✓	✓	-
show ip pim neighbor detail	✓	✓	-
show ip pim nexthop	✓	✓	-
show ip pim rp mapping	✓	✓	-
show ip igmp snooping groups	✓	✓	-
show ip igmp snooping interface	✓	✓	-
show ipv6 mld snooping groups	✓	✓	-
show ipv6 mld snooping interface	✓	✓	-
show vrrp	✓	✓	-
show dhcp server	✓	✓	-
show dhcp binding	✓	✓	-
show dhcp relay	✓	✓	-
show dhcpv6 server	✓	✓	-
show dhcpv6 binding	✓	✓	-
show dns-forwarding	✓	✓	-
show dns-forwarding cache	✓	✓	-
show radius-server local certificate status	✓	✓	-
show radius-server local nas	✓	✓	-
show radius-server local user	✓	✓	-
show radius-server local certificate list	✓	✓	-
show radius-server local certificate revoke	✓	✓	-
show sflow	✓	✓	-
show sflow sampling	✓	✓	-
show ptp	✓ (*3)	✓ (*3)	-
show ptp interface	✓ (*3)	✓ (*3)	-
show ptp data default	✓ (*3)	✓ (*3)	-
show ptp data current	✓ (*3)	✓ (*3)	-
show ptp data parent	✓ (*3)	✓ (*3)	-
show ptp port-data	✓ (*3)	✓ (*3)	-

Command	Stack disabled	Stack enabled	
		Main switch	Member switch
show yno	✓	✓	-

*1: Included only with models that include a DIP switch.

*2: Included only with models that support the power redundancy function.

*3: Included only with models that support PTP boundary clock mode.

[Example]

Show technical support information.

```
SWX3220#show tech-support
#
# Information for Yamaha Technical Support
#

*** show running-config ***
!
!  - Running Configuration -
!  Current Time:  Fri Jan 1 00:00:00 JST 2021
!
dns-client enable
!
vlan database
 vlan 2 name VLAN0002
 vlan 3 name VLAN0003
!
interface port1.1
 switchport
 switchport mode access
...

*** show startup-config ***
...

*** show stack ***
...

*** show environment ***
...

*** show disk-usage ***
...
...
...

#
# End of Information for Yamaha Technical Support
#

SWX3220#
```

4.5.7 Save technical support information

[Syntax]

copy tech-support sd

[Input mode]

privileged EXEC mode

[Description]

Saves technical support information to the SD card.

This is saved on the SD card with the following file name.

- SWX3220-16MT、SWX3220-16TMs

  ```
  /swx3220/tech-support/YYYYMMDDHHMMSS_techsupport.txt
  ```

- SWX3220-30MC

```
/swx3220-30mc/tech-support/YYYYMMDDHHMMSS_techsupport.txt
```

- SWX3220-30TCs

```
/swx3220-30tcs/tech-support/YYYYMMDDHHMMSS_techsupport.txt
```

YYYYMMDDHHMMSS ... Year month day hour minute second that the command was executed

[Note]

The SD card must be inserted in advance.

[Example]

Save technical support information to the SD card.

```
SWX3220#copy tech-support sd
```

4.5.8 Show fan operating history

[Syntax]

show fan history

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

Shows the fan operating history.

[Example]

Shows the fan operating history.

```
SWX3220>show fan history
2020/10/22 15:45:54: FAN1 status:Low perform:80%
```

4.5.9 Show power supply unit information

[Syntax]

show power-supply

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

Shows the power supply unit information and status.

The following content is displayed.

Item	Description
Slot	Power supply unit slot ID (stack ID + slot ID)
Model	Power supply unit model name
Serial	Serial number of power supply unit
Status	Status of power supply unit
Volt	Input voltage value
Watt	Input power consumption value
Max	Maximum power consumption value
FanSpeed	Fan speed value of power supply unit

One of the following items are shown in the status.

Status	Description
None	Power supply unit is not plugged in
Powered	Power is being supplied normally

Status	Description
No AC-cable	Power cable is not plugged in
Wrong module	Unsupported power supply unit is plugged in
Warned(In)	Warning has occurred for current/voltage/power consumption on the input side
Warned(Out)	Warning has occurred for current/voltage/power consumption on the output side
Warned(Temp)	Temperature warning has occurred on the power supply unit
Warned(FAN)	Warning has occurred for the power supply unit fan
Failed(In)	Current/voltage/power consumption abnormality occurred on the input side
Failed(Out)	Current/voltage/power consumption abnormality occurred on the output side
Failed(Temp)	Abnormality has occurred with the temperature on the power supply unit
Failed(FAN)	Abnormality has occurred with the fan on the power supply unit

[Example]

Shows the power supply unit information and status.

The following example uses the chassis for stack ID1.

```
SWX3220>show power-supply
Slot Model        Serial     Status                   Volt Watt  Max FanSpeed
-------------------------------------------------------------------------------
 1.1 YPSU-550W-AC Z8X00000DZ Powered                  104V  54W 750W  3472rpm
 1.2 YPSU-550W-AC Z8X00001DZ No AC-cable                0V   0W 750W     0rpm
```

[Models]

SWX3220-30MC, SWX3220-30TCs

4.6 System self-diagnostics

4.6.1 Showing system self-diagnostics results

[Syntax]

show system-diagnostics

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

Shows all system self-diagnostics results (bootup diagnostics, on-demand diagnostics, and health-monitoring diagnostics).

[Example]

Shows system self-diagnostics results.

```
SWX3220#show system-diagnostics
Test results:
  P = Pass, F = Fail, U = Untested
  N = Normal, W = Warning

- Bootup
  Loading Test: Pass

  RTC Test: Pass

   . . .

- On-demand
  Last on-demand diagnostics information:
```

```
    Date      : 2025/01/01 09:00:00 +09:00
    BootROM   : Ver.1.00
    • • •

  PHY Test:
    Port   1   2   3   4   5   6   7   8   9  10  11  12
    ----------------------------------------------------
           P   P   P   P   P   P   P   P   P   P   P   P

  • • •

- Health monitoring
  • • •

  SFP Test:
    Port  13  14  15  16
    --------------------
           N   N   N   N
```

4.6.2 Executing on-demand diagnostics

[Syntax]

system-diagnostics on-demand execute [no-confirm]

[Keyword]

no-confirm	:	Execute on-demand diagnostics immediately without an execution check (y or n)

[Input mode]

privileged EXEC mode

[Description]

Executes on-demand diagnostics.

Shut down all LAN/SFP port during the diagnostics. At the end of the diagnostics, simple diagnostic results are shown and the system is automatically rebooted.

If no parameters are specified, confirmation is requested as to whether to execute on-demand diagnostics.

You must enter "y” to execute diagnostics or "n" to not execute diagnostics.

[Note]

Detailed on-demand diagnostics results can be checked after reboot by using the **show system-diagnostics** command.

[Example]

Executes on-demand diagnostics.

```
SWX3220#system-diagnostics on-demand execute
The system will be rebooted after diagnostics. Continue ? (y/n) y
on-demand diagnostics completed (pass). reboot immediately...
```

4.6.3 Clearing the on-demand diagnostics results

[Syntax]

clear system-diagnostics on-demand

[Input mode]

privileged EXEC mode

[Description]

Clears the on-demand diagnostics results.

[Example]

Clears the on-demand diagnostics results.

```
SWX3220#clear system-diagnostics on-demand
```

4.7 Cable diagnostics

4.7.1 Execute cable diagnostics

[Syntax]

cable-diagnostics tdr execute interface *ifname*
test cable-diagnostics tdr interface *ifname*

[Parameter]

ifname	:	LAN port interface name Target interface

[Input mode]

privileged EXEC mode

[Description]

Execute cable diagnostics. The previous diagnostic result can be viewed with the show cable-diagnostics tdr command.

[Note]

Only the prior diagnostic result is stored, and the result is overwritten when executing the cable diagnostics again.

[Example]

Execute diagnostics on the LAN cable connected to port1.1.

```
SWX3220#cable-diagnostics tdr execute interface port1.1
The port will be temporarily down during test. Continue? (y/n): y
% To check result, enter "show cable-diagnostics tdr"
```

4.7.2 Clear cable diagnostic results

[Syntax]

clear cable-diagnostics tdr
clear test cable-diagnostics tdr

[Input mode]

privileged EXEC mode

[Description]

Clears the results of the prior cable-diagnostics tdr execute interface command execution.

[Example]

Clear the results of the prior cable diagnostic execution.

```
SWX3220#clear cable-diagnostics tdr
SWX3220#
```

4.7.3 Display cable diagnostic results

[Syntax]

show cable-diagnostics tdr
show test cable-diagnostics tdr

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

Displays the result of the prior cable-diagnostics tdr execute interface command execution.

[Example]

Display the result of the last cable diagnostic execution.

```
SWX3220#show cable-diagnostics tdr
Last run on Tue May 31 14:29:35 2022
Port      Pair  Status  Fault distance
-----------------------------------------
port1.8   1     OK      -
          2     OK      -
```

```
          3     Open    15   m
          4     Open    15   m
```

4.8 Time management

4.8.1 Set clock manually

[Syntax]

clock set *time month day year*

[Parameter]

time : hh:mm:ss

Time

month : <1-12> or Jan, Feb, Mar, ... , Dec

Month or name of month

day : <1-31>

Day

year : Year (four digits)

[Input mode]

privileged EXEC mode

[Description]

Set the system time.

[Example]

Set the time to 0 hours 0 minutes 0 seconds on January 1, 2015.

```
SWX3220#clock set 00:00:00 Jan 1 2015
```

4.8.2 Set time zone

[Syntax]

clock timezone *zone*
clock timezone *offset*
no clock timezone

[Parameter]

zone : Name of the time zone

Setting value	Description
UTC	Coordinated Universal Time
JST	Japan Standard Time

offset : Set the difference from UTC

Setting value	Description
-12:00	GMT-12:00
-11:00	GMT-11:00
-10:00	GMT-10:00
-9:00	GMT-9:00
-8:00	GMT-8:00
-7:00	GMT-7:00
-6:00	GMT-6:00
-5:00	GMT-5:00
-4:30	GMT-4:30
-4:00	GMT-4:00
-3:30	GMT-3:30
-3:00	GMT-3:00
-2:00	GMT-2:00
-1:00	GMT-1:00
+0:00	GMT+0:00
+1:00	GMT+1:00
+2:00	GMT+2:00
+3:00	GMT+3:00
+3:30	GMT+3:30
+4:00	GMT+4:00
+4:30	GMT+4:30
+5:00	GMT+5:00
+5:30	GMT+5:30
+5:45	GMT+5:45
+6:00	GMT+6:00
+6:30	GMT+6:30
+7:00	GMT+7:00
+8:00	GMT+8:00
+9:00	GMT+9:00
+9:30	GMT+9:30
+10:00	GMT+10:00
+11:00	GMT+11:00
+12:00	GMT+12:00
+13:00	GMT+13:00

[Initial value]

clock timezone UTC

[Input mode]

global configuration mode

[Description]

Sets the time zone.

If this command is executed with the "no" syntax, UTC is specified.

[Example]

Set the time zone to JST.

```
SWX3220(config)#clock timezone JST
```

Set the time zone to UTC+9 hours.

```
SWX3220(config)#clock timezone +9:00
```

4.8.3 Configuring daylight saving time (recurring)

[Syntax]

clock summer-time *name* **recurring** *week wday month time week wday month time* [*offset*]
no clock summer-time

[Parameter]

name	:	Time zone name to be displayed when daylight saving time is in effect Alphanumeric characters (up to 7 characters)
week	:	<1-4> or first, last Specifies the week of the month
wday	:	Sun, Mon, Tue, ... , Sat Day of the week
month	:	<1-12> or Jan, Feb, Mar, ... , Dec Month or month name
time	:	hh:mm Time
offset	:	<1-1440> Time to add during daylight saving time. Specify in minutes. The default value is 60.

[Initial value]

None

[Input mode]

global configuration mode

[Description]

Configure daylight saving time.

Configure daylight saving time to start and end on a specified week and day of the week every year.

The first part specifies the daylight saving time start period and the second part specifies the end period.

If this command is executed with the "no" syntax, the setting is cleared.

[Note]

Daylight saving times cannot overlap.

[Example]

Set daylight saving time to start at 2 AM on the second Sunday of March and end at 2 AM on the first Sunday of November every year.

```
SWX3220(config)#clock summer-time JDT recurring 2 Sun Mar 2:00 1 Sun Nov 2:00
```

4.8.4 Configuring daylight saving time (by date)

[Syntax]

clock summer-time *name* **date** *month day year time month day year time* [*offset*]
no clock summer-time

[Parameter]

name	:	Time zone name to be displayed when daylight saving time is in effect

		Alphanumeric characters (up to 7 characters)
month	:	<1-12> or Jan, Feb, Mar, ... , Dec
		Month or month name
day	:	<1-31>
		Day
year	:	Year (4 digits)
time	:	hh:mm
		Time
offset	:	<1-1440>
		Time to add during daylight saving time. Specify in minutes. The default value is 60.

[Initial value]

None

[Input mode]

global configuration mode

[Description]

Configure daylight saving time.

Configure daylight saving time to start and end on specified dates.

The first part specifies the daylight saving time start date and the second part specifies the end date.

If this command is executed with the "no" syntax, the setting is cleared.

[Note]

Daylight saving times cannot overlap.

[Example]

Set daylight saving time to start on March 14, 2021 at 2 AM and end on November 7, 2021 at 2 AM.

```
SWX3220(config)#clock summer-time JDT date Mar 14 2021 2:00 Nov 7 2021 2:00
```

4.8.5 Show current time

[Syntax]

show clock [detail]

[Keyword]

detail	:	Also display detailed information

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the current time, year, month, and date.

When detail is specified, detailed information (current time and daylight saving time) is displayed.

If daylight saving time is recurring, it displays the actual date of the next (or currently in effect) daylight saving time period.

[Example]

Show current time.

```
SWX3220>show clock
Thu Jan 1 00:00:00 JST 2015
```

Display detailed information about the current time. (If daylight saving time is configured)

```
SWX3220>show clock detail
Thu Jan 1 00:00:00 JST 2021

Summer Time
  Type   : Recurring
```

```
  Offset : 60 (min)
  From   : Sun Mar 14 02:00:00 JST 2021
  To     : Sun Nov 7 02:00:00 JDT 2021
```

Display detailed information about the current time. (If daylight saving time is not configured)

```
SWX3220>show clock detail
SWX3220>show clock detail
Thu Jan 1 00:00:00 JST 2021

Summer Time Disabled
```

4.8.6 Set NTP server

[Syntax]

ntpdate server ipv4 *ipv4_addr*
ntpdate server ipv6 *ipv6_addr*
ntpdate server name *fqdn*
no ntpdate server

[Keyword]

ipv4	:	Specify the NTP server by IPv4 address
ipv6	:	Specify the NTP server by IPv6 address
name	:	Specify the NTP server by host name

[Parameter]

ipv4_addr	:	IPv4 address of the NTP server
ipv6_addr	:	IPv6 address of the NTP server If you specify an IPv6 link local address, you must also specify the output interface (fe80::X%vlanN format)
fqdn	:	Host name of the NTP server As character types, alphabetical characters (uppercase/lowercase), numerals, . (period), and - (hyphen) can be used

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Registers the address or host name of the NTP server.

Up to two instances of this command can be set.

If this command is executed with the "no" syntax, the NTP server setting is deleted.

If time synchronization is performed with two NTP servers specified, they are queried in the order of NTP server 1 and NTP server 2 as shown by the **show ntpdate** command.

The query to NTP server 2 is performed only if synchronization with NTP server 1 fails.

[Example]

Specify 192.168.1.1 as the NTP server.

```
SWX3220(config)#ntpdate server ipv4 192.168.1.1
```

Specify fe80::2a0:deff:fe11:2233%vlan1 as the NTP server.

```
SWX3220(config)#ntpdate server ipv6 fe80::2a0:deff:fe11:2233%vlan1
```

Specify ntp.example.com as the NTP server.

```
SWX3220(config)#ntpdate server name ntp.example.com
```

4.8.7 Synchronize time from NTP server (one-shot update)

[Syntax]

ntpdate oneshot

[Input mode]

privileged EXEC mode

[Description]

Attempts to obtain time information from the registered NTP server.

This is performed only once when this command is executed.

[Example]

Obtain time information from the NTP server.

```
SWX3220#ntpdate oneshot
```

4.8.8 Synchronize time from NTP server (update interval)

[Syntax]

ntpdate interval *interval-time*
no ntpdate interval

[Parameter]

interval-time	:	<0-24> Interval (hours) for time synchronization. If this is set to 0 hours, periodic synchronization will not occur.

[Initial value]

ntpdate interval 1

[Input mode]

global configuration mode

[Description]

Specifies the interval (in one-hour units) at which time information is periodically obtained from the registered NTP server.

If this command is executed with the "no" syntax, the setting returns to the default.

When this command is executed, the time is updated immediately, and is subsequently updated at the specified interval.

[Example]

Request the time every two hours.

```
SWX3220(config)#ntpdate interval 2
```

Disable periodic time synchronization.

```
SWX3220(config)#ntpdate interval 0
```

4.8.9 Show NTP server time synchronization settings

[Syntax]

show ntpdate

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the settings that are related to time synchronization from an NTP server.

[Example]

Show time synchronization settings. *If the synchronization update interval is one hour

```
SWX3220#show ntpdate
NTP Server 1 : ntp.nict.jp
```

```
NTP Server 2 : none
adjust time : Thu Jan 1 09:00:00 2015 + interval 1 hour
sync server : ntp.nict.jp
```

Show time synchronization settings. *If periodic synchronization is not being performed

```
SWX3220#show ntpdate
NTP Server 1 : ntp.nict.jp
NTP Server 2 : none
adjust time : Thu Jan 1 09:00:00 2015
sync server : ntp.nict.jp
```

4.9 Time synchronization

4.9.1 PTP function settings (system)

[Syntax]

ptp *type*
no ptp

[Parameter]

type : System-wide operations for the PTP function

Setting value	Description
enable	Enables the PTP function for the entire system
disable	Disables the PTP function for the entire system

[Initial value]

ptp disable

[Input mode]

global configuration mode

[Description]

Enables or disables the system-wide PTP function.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

To make the PTP function operate, you must enable the PTP function for the interface as well.

Also This command cannot be used if the stack function is enabled.

This command can be used in transparent clock mode and boundary clock mode.

[Example]

Enable the PTP function for the entire system.

```
SWX3220(config)#ptp enable
```

Disable the PTP function for the entire system.

```
SWX3220(config)#ptp disable
```

4.9.2 Set PTP function (interface)

[Syntax]

ptp *type*
no ptp

[Parameter]

type : Operations for the PTP function of the applicable interface

Setting value	Description
enable	Enable PTP function for the applicable interface
disable	Disable PTP function for the applicable interface

[Initial value]

ptp disable

[Input mode]

interface mode

[Description]

Enables or disables the PTP function for the applicable interface.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be specified only for LAN/SFP port.

If the system-wide PTP function is disabled, this will not operate.

Also This command cannot be used if the stack function is enabled.

This command can be used in transparent clock mode and boundary clock mode.

[Example]

Enables the PTP function for LAN port #1.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#ptp enable
```

Disables the PTP function for LAN port #1.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#ptp disable
```

4.9.3 PTP operation mode settings

[Syntax]

ptp mode *type* delay-mechanism *mechanism* step *step-mode*
no ptp mode

[Keyword]

delay-mechanism : Specifies the delay mechanism type

step : Specifies the step mode type

[Parameter]

type : PTP operation mode

Setting value	Description
boundary	Boundary clock (2 steps)
transparent	Transparent clock (1 step)

mechanism : Delay mechanism

Setting value	Description
e2e	End-to-end mode

step-mode : Step mode

Setting value	Description
one-step	One-step mode

[Initial value]

ptp mode transparent delay-mechanism e2e step one-step

[Input mode]

global configuration mode

[Description]

This sets the PTP operation mode and delay mechanism.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command does not operate if the system-wide PTP function is disabled.

This can only be modified if the system-wide PTP function is disabled.

Only SWX3220-30MC or SWX3220-30TCs can be set in boundary clock mode.

Delay mechanisms only support end-to-end mode.

Step mode only supports two steps for boundary clocks and one step for transparent clocks. Only SWX3220-16MT or SWX3220-16TMs can be specified.

[Example]

This sets the PTP operation mode to transparent clocks and the delay mechanism to end-to-end mode. (SWX3220-16MT, SWX3220-16TMs)

```
SWX3220(config)#ptp mode transparent delay-mechanism e2e step one-step
```

This sets the PTP operation mode to boundary clocks and the delay mechanism to end-to-end mode. (SWX3220-30MC, SWX3220-30TCs)

```
SWX3220(config)#ptp mode boundary delay-mechanism e2e
```

4.9.4 Forwarding protocol settings for PTP messages

[Syntax]

ptp transport protocol *type*
no ptp transport protocol

[Parameter]

type : Protocol used for forwarding PTP messages

Setting value	Description
ipv4-udp	Use IPv4 UDP
ipv6-udp	Use IPv6 UDP
layer2	Use L2 Ethernet frames

[Initial value]

ptp transport protocol ipv4-udp

[Input mode]

global configuration mode

[Description]

Sets the forwarding protocol settings for PTP messages.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command does not operate if the system-wide PTP function is disabled.

This can only be modified if the system-wide PTP function is disabled.

This command can be used in transparent clock mode and boundary clock mode.

[Example]

This uses IPv6 in UDP to forward PTP messages.

```
SWX3220(config)#ptp transport protocol ipv6-udp
```

4.9.5 Set PTP clock domain number

[Syntax]

ptp domain *domain*
no ptp domain

[Parameter]

domain : <0 - 127>
Domain number

[Initial value]

ptp domain 0

[Input mode]

global configuration mode

[Description]

This sets the PTP clock domain number.
If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This can be changed only if the PTP function for the system is disabled.
This command can be used in boundary clock mode.

[Example]

Sets the domain number to 24.

```
SWX3220(config)#ptp domain 24
```

[Models]

SWX3220-30MC, SWX3220-30TCs

4.9.6 Set PTP clock priority 1

[Syntax]

ptp priority1 *priority*
no ptp priority1

[Parameter]

priority : <0 - 255>
Priority value

[Initial value]

ptp priority1 128

[Input mode]

global configuration mode

[Description]

This sets the priority 1 value that is used for selecting the Best Time Transmitter Clock.
Lower numbers have higher priority.
If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This can be changed only if the PTP function for the system is disabled.
This command can be used in boundary clock mode.

[Example]

Sets the priority 1 value to 255.

```
SWX3220(config)#ptp priority1 255
```

[Models]

SWX3220-30MC, SWX3220-30TCs

4.9.7 Set PTP clock priority 2

[Syntax]

ptp priority2 *priority*
no ptp priority2

[Parameter]

priority : <0 - 255>
Priority value

[Initial value]

ptp priority1 128

[Input mode]

global configuration mode

[Description]

This sets the priority 2 value that is used for selecting the Best Time Transmitter Clock.
Lower numbers have higher priority.
If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This can be changed only if the PTP function for the system is disabled.
This command can be used in boundary clock mode.

[Example]

Sets the priority 2 value to 255.

```
SWX3220(config)#ptp priority2 255
```

[Models]

SWX3220-30MC, SWX3220-30TCs

4.9.8 Set PTP message transmission interval

[Syntax]

ptp announce interval *interval*
no ptp announce interval

[Parameter]

interval : <-3 - 4>
Announce message transmission interval (log)

Setting value	Transmission interval
-3	1/8 second
-2	1/4 second
-1	1/2 second
0	1 second
1	2 seconds
2	4 seconds
3	8 seconds
4	16 seconds

[Initial value]

ptp announce interval 1

[Input mode]

interface mode

[Description]

Sets the transmission interval for announce messages from the applicable interface.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be specified only for LAN/SFP port.

This can be changed only if the PTP function for the interface is disabled.

This command can be used in boundary clock mode.

[Example]

This sets the transmission interval of the announce message for LAN port #1 to -3 (1/8 second).

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#ptp announce interval -3
```

[Models]

SWX3220-30MC, SWX3220-30TCs

4.9.9 Set receive timeout for PTP announce messages

[Syntax]

ptp announce timeout-interval *interval*
no ptp announce timeout-interval

[Parameter]

interval	:	Receive timeout for announce messages [2-10]

[Initial value]

ptp announce timeout-interval 3

[Input mode]

interface mode

[Description]

This sets the receive timeout for announce messages from the applicable interface.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be specified only for LAN/SFP port.

This can be changed only if the PTP function for the interface is disabled.

This command can be used in boundary clock mode.

[Example]

Sets the receive timeout for announce messages from LAN port #1 to "5".

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#ptp announce timeout-interval 5
```

[Models]

SWX3220-30MC, SWX3220-30TCs

4.9.10 Set PTP sync message transmission interval

[Syntax]

ptp sync interval *interval*
no ptp sync interval

[Parameter]

interval	:	<-4 - 4>

Sync message transmission interval (log)

Setting value	Transmission interval
-4	1/16 second
-3	1/8 second
-2	1/4 second
-1	1/2 second
0	1 second
1	2 seconds
2	4 seconds
3	8 seconds
4	16 seconds

[Initial value]

ptp sync interval 0

[Input mode]

interface mode

[Description]

Sets the transmission interval for sync messages from the applicable interface.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be specified only for LAN/SFP port.

This can be changed only if the PTP function for the interface is disabled.

This command can be used in boundary clock mode.

[Example]

Sets the transmission interval of the sync message for LAN port #1 to -4 (1/16 second).

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#ptp sync interval -4
```

[Models]

SWX3220-30MC, SWX3220-30TCs

4.9.11 Set PTP delay-request message transmission interval

[Syntax]

ptp delay-req interval *interval*
no ptp delay-req interval

[Parameter]

interval : <-4 - 4>

Delay-request message transmission interval (log)

Setting value	Transmission interval
-4	1/16 second
-3	1/8 second
-2	1/4 second
-1	1/2 second
0	1 second
1	2 seconds
2	4 seconds
3	8 seconds
4	16 seconds

[Initial value]

ptp delay-req interval 0

[Input mode]

interface mode

[Description]

Sets the Delay-Request message transmission interval for the applicable interface.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be specified only for LAN/SFP port.

This can be changed only if the PTP function for the interface is disabled.

This command can be used in boundary clock mode.

[Example]

Sets the delay-request message transmission interval for LAN port #1 to -4 (1/16 seconds).

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#ptp delay-req interval -4
```

[Models]

SWX3220-30MC, SWX3220-30TCs

4.9.12 Specify VLAN for transmitting/receiving PTP messages

[Syntax]

ptp vlan *vlanid*
no ptp vlan

[Parameter]

vlanid : <1 - 4094>
VLAN id

[Initial value]

None

[Input mode]

interface mode

[Description]

This sets the VLAN used for transmitting/receiving PTP messages on the trunk port.

When this command is not set, the native VLAN is used.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be specified only for LAN/SFP port.

This can be changed only if the PTP function for the interface is disabled.

To set a VLAN with this command, you must associate the interface with a trunk port beforehand. If the interface is not associated with a VLAN, the PTP message is discarded.

This command can be used in boundary clock mode.

[Example]

This sets the VLAN used for transmitting/receiving PTP messages on LAN port #1 to VLAN100.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#ptp vlan 100
```

[Models]

SWX3220-30MC, SWX3220-30TCs

4.9.13 Show PTP setting status

[Syntax]

show ptp

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

Shows the PTP setting status.

[Note]

This command can be used in transparent clock mode and boundary clock mode.

[Example]

Shows the PTP setting status in transparent clock mode.

```
SWX3220>show ptp
  PTP State                  : Enabled
  PTP Mode                   : Transparent Clock
  Delay Mechanism            : End to End
  Step Mode                  : One-step
  Transport Protocol         : UDP (IPv4)
```

Shows the PTP setting status in boundary clock mode.

```
SWX3220#show ptp
  PTP State                  : Enabled
  PTP Mode                   : Boundary Clock
  Delay Mechanism            : End to End
  Step Mode                  : Two-step
  Transport Protocol         : Layer2

  Boundary Clock Config
  Priority1                  : 128
  Priority2                  : 128
  Domain                     : 0
```

4.9.14 Show PTP setting information for the interface

[Syntax]

show ptp interface *ifname*

[Keyword]

interface	:	Specifies the interface to show

[Parameter]

ifname	:	LAN/SFP port interface name Interface to show

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

This shows the PTP setting information for the specified interface.

If "ifname" is omitted, information is shown for all interfaces.

[Note]

This command can be used in transparent clock mode and boundary clock mode.

[Example]

This shows PTP information for all ports. (SWX3220-16MT, SWX3220-16TMs)

```
SWX3220>show ptp interface
Interface  PTP
-------------------
port1.1    Disable
port1.2    Disable
port1.3    Enable
port1.4    Enable
port1.5    Enable
port1.6    Enable
port1.7    Enable
port1.8    Enable
```

Shows PTP information for all ports. (SWX3220-30MC, SWX3220-30TCs)

```
SWX3220#show ptp interface
AI: Anounce Interval     AT: Announce Receipt Timeout
SI: Sync Interval        DI: Delay Request Interval

Interface  PTP       AI   AT   SI   DI
----------------------------------------
port1.1    Disable    1    3    0    0
port1.2    Disable    1    3    0    0
port1.3    Enable     1    3    0    0
port1.4    Enable     1    3    0    0
port1.5    Enable     1    3    0    0
port1.6    Enable     1    3    0    0
port1.7    Enable     1    3    0    0
port1.8    Enable     1    3    0    0
```

Shows the PTP information for LAN port #1. (SWX3220-16MT, SWX3220-16TMs)

```
SWX3220>show ptp interface port1.1
Interface  PTP
-------------------
port1.1    Disable
```

4.9.15 Show PTP clock information

[Syntax]

show ptp data *type*

[Parameter]

type :

Setting value	Description
default	Show the clock information for this device
current	Show the current status of the clock
parent	Show the information for the time transmitter clock currently synchronized to this device
transparent	Show the transparent clock information

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

This shows the PTP information for the specified interface.

[Note]

This command can be used in transparent clock mode and boundary clock mode.

[Example]

Show the clock information for this device.

```
SWX3220#show ptp data default
CLOCK(Boundary Clock)
   Two Step Flag           : Yes
   Clock Identity          : 00:00:5e:ff:fe:00:53:01
   Number Of Ports         : 30
   Clock Quality
     Class                 : 248
     Accuracy              : 39
     Offset (log variance) : ffff
   Priority1               : 128
   Priority2               : 128
   Domain Number           : 0
   TimeReceiver Only       : No
```

Show the current status of the clock.

```
SWX3220#show ptp data current
CLOCK(Boundary Clock)
   Steps Removed      : 1
   Offset From timeTransmitter : -2
   Mean Path Delay    : 52
```

Show the information for the master clock currently synchronized to this device.

```
SWX3220#show ptp data parent
CLOCK(Boundary Clock)
   Parent Port Identity
     Clock Identity                        : 00:00:5e:ff:fe:00:53:02
     Port Number                           : 1
   Parent Stats                            : No
   Observed Parent Offset (log variance)   : ffff
   Observed Parent Clock Phase Change Rate : 7fffffff
   Grandmaster
     Clock Identity                        : 00:00:5e:ff:fe:00:53:02
     Clock Quality
       Class                               : 248
       Accuracy                            : 39
       Offset (log variance)               : ffff
     Priority1                             : 128
     Priority2                             : 128
```

Show the transparent clock information

```
SWX3220#show ptp data transparent
CLOCK(TRANSPARENT)
Clock Identity  : 00:00:5e:ff:fe:00:53:01
 Number Of Ports : 1
Delay Mechanism : End to End
Primary Domain  : 0
```

[Models]

SWX3220-30MC, SWX3220-30TCs

4.9.16 Show clock information for the PTP interface

[Syntax]

show ptp port-data *ifname*

[Parameter]

ifname	:	LAN/SFP port interface name Interface to show

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

This shows the clock information for the specified interface.

If "ifname" is omitted, information is shown for all interfaces.

[Note]

This command can be used in boundary clock mode.

[Example]

Show port data set

```
SWX3220#show ptp port-data port1.1
==========================================
Interface port1.1

  Port State [PTP_TIMETRANSMITTER]
  Port Clock Identity                      : 00:00:5e:ff:fe:00:53:01
  Port Number                              : 1
  Mean Path Delay                          : 0
  Announce interval (log base 2)           : 1
  Announce Receipt Timeout                 : 3
  Sync Interval (log base 2)               : 0
  Delay Mechanism                          : End to end
  Delay Request Interval (log base 2)      : 0
  PTP version                              : 2
```

[Models]

SWX3220-30MC, SWX3220-30TCs

4.9.17 Show PTP statistical information

[Syntax]

show ptp statistics *interface ifname*

[Parameter]

ifname	:	LAN/SFP port interface name Interface to show

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

This shows the statistical information for the specified interface.

[Note]

This command can be used in boundary clock mode.

[Example]

Shows the statistical information for port1.1.

```
SWX3220#show ptp statistics interface port1.1
==========================================
Interface port1.1

                RX                       TX
  ------------- ------------------------ ------------------------
   Announce             203 ( 8.00/sec)            0 ( 0.00/sec)
   Sync                 399 (16.00/sec)            0 ( 0.00/sec)
   Follow_Up            399 (16.00/sec)            0 ( 0.00/sec)
   Delay_Req              0 ( 0.00/sec)          403 (16.00/sec)
   Delay_Resp           403 (16.00/sec)            0 ( 0.00/sec)
  ------------- ------------------------ ------------------------
   Signaling              0 ( 0.00/sec)            0 ( 0.00/sec)
   Management             0 ( 0.00/sec)            0 ( 0.00/sec)
  ------------- ------------------------ ------------------------
   Total               1418 (56.00/sec)          403 (16.00/sec)

  Announce Recept Timeout :          0
  Total RX Error          :          0
```

[Models]

SWX3220-30MC, SWX3220-30TCs

4.9.18 Set Sync-E input port

[Syntax]

sync-e input-source *priority interface ifname* [*speed*]
no sync-e input-source *priority*

[Parameter]

priority : Priority (fixed at 1)

ifname : LAN/SFP port interface name

Interface to set to Sync-E input port

speed : Link speed

Setting value	Description	LAN port	SFP+ port	SFP28 port	QSFP28 port
sfp-1g	1 Gbps	-	○	○	-
sfp-10g	10 Gbps	-	○	○	-
sfp-25g	25 Gbps	-	-	○	-

[Initial value]

None

[Input mode]

global configuration mode

[Description]

Sets the Sync-E input port.

Synchronization occurs only when the *speed* parameter setting matches the port's link speed.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This can be changed only if the PTP function for the system is disabled.

This command can be used in boundary clock mode.

[Example]

This sets LAN port #1 to the Sync-E input port.

```
SWX3220(config)#sync-e input-source 1 interface port1.1
```

This sets SFP28 port #25 (25 Gbps) to the Sync-E input port.

```
SWX3220(config)#sync-e input-source 1 interface port1.25 sfp-25g
```

[Models]

SWX3220-30MC, SWX3220-30TCs

4.10 Terminal settings

4.10.1 Move to line mode (console terminal)

[Syntax]

line con *port*

[Parameter]

port : 0

Serial console port number

[Initial value]

line con 0

[Input mode]

global configuration mode

[Description]

Moves to line mode in order to make console terminal settings.

[Note]

To return from line mode to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

[Example]

Move to line mode in order to make console terminal settings.

```
SWX3220(config)#line con 0
SWX3220(config-line)#
```

4.10.2 Set VTY port and move to line mode (VTY port)

[Syntax]

line vty *port1* [*port2*]
no line vty *port1* [*port2*]

[Parameter]

port1 : <0-7>

VTY port number

port2 : <0-7>

Last VTY port number when specifying a range

[Initial value]

no line vty 0 7

[Input mode]

global configuration mode

[Description]

After enabling the specified VTY ports, moves to line mode for making VTY port settings.

If this command is executed with the "no" syntax, the specified VTY ports are disabled.

If you specify *port2*, a range of ports is specified; all VTY ports from *port1* through *port2* are specified. *port2* must be a number greater than *port1*.

[Note]

The maximum number of simultaneous Telnet client connections depends on the number of VTY ports that are enabled.

To return from line mode to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

[Example]

Enable VTY port #0 and then move to line mode.

```
SWX3220(config)#line vty 0
SWX3220(config-line)#
```

4.10.3 Set terminal login timeout

[Syntax]

exec-timeout *min* [*sec*]
no exec-timeout

[Parameter]

min : <0-35791>

Timeout time (minutes)

sec : <0-2147483>

Timeout time (seconds)

[Initial value]

exec-timeout 10

[Input mode]

line mode

[Description]

Sets the time after which automatic logout occurs if there has been no key input from the console terminal or VTY.

If *sec* is omitted, 0 is specified. If *min* and *sec* are both set to 0, automatic logout does not occur.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

After this command is executed, the setting is applied starting at the next login.

[Example]

Set the console timeout time to five minutes.

```
SWX3220(config)#line con 0
SWX3220(config-line)#exec-timeout 5 0
SWX3220(config-line)#
```

4.10.4 Change the number of lines displayed per page for the terminal in use

[Syntax]

terminal length *line*
terminal no length

[Parameter]

line	:	<0-512> Number of lines displayed per page on the terminal

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Changes the number of lines displayed per page for the terminal in use.

If *line* is set to 0, the display is not paused per page.

If the **terminal no length** command is executed, the number of lines is set to 24 in the case of a serial console, or to the window size when connected in the case of VTY.

[Note]

When this command is executed, the change applies immediately.

The result of executing this command takes priority over the setting applied by the **service terminal-length** command.

[Example]

Change the number of lines displayed per page for the terminal in use to 100 lines.

```
SWX3220>terminal length 100
SWX3220>
```

4.10.5 Set the number of lines displayed per page on the terminal

[Syntax]

service terminal-length *line*
no service terminal-length

[Parameter]

line	:	<0-512> Number of lines displayed per page on the terminal

[Initial value]

no service terminal-length

[Input mode]

global configuration mode

[Description]

Sets the number of lines displayed per page on the terminal.

If *line* is set to 0, the display is not paused per page.

If this command is executed with the "no" syntax, the number of lines is set to 24 in the case of a serial console, or to the window size when connected in the case of VTY.

[Note]

After this command is executed, the setting is applied starting at the next login.

If the **terminal length** command is executed, the result of executing the **terminal length** command takes priority.

[Example]

Change the number of lines displayed per page for the terminal in use to 100 lines.

```
SWX3220(config)#service terminal-length 100
SWX3220(config)#
```

4.10.6 Changing the serial baud rate

[Syntax]

baudrate select *baudrate*

[Parameter]

baudrate	:	9600, 19200, 38400, 57600, 115200 Serial baud rate (bps)

[Initial value]

baudrate select 9600

[Input mode]

privileged EXEC mode

[Description]

This sets the serial baud rate.

[Example]

Sets the serial baud rate to 115200.

```
SWX3220#baudrate select 115200
```

4.11 Management

4.11.1 Set management VLAN

[Syntax]

management interface *interface*
no management interface

[Parameter]

interface	:	VLAN interface name

[Initial value]

management interface vlan1

[Input mode]

global configuration mode

[Description]

Set the VLAN that is used for management.

By setting this command, it will be possible to set and acquire the IP address assigned by the L2MS manager to the corresponding VLAN when operating as an L2MS agent.

If this is executed with the "no" syntax, or if the VLAN is deleted, this command also returns to the default settings.

[Example]

Set VLAN #2 as the management VLAN.

```
SWX3220(config)#management interface vlan2
```

4.12 SYSLOG

4.12.1 Set log notification destination (SYSLOG server)

[Syntax]

logging host *host*
no logging host *host*

[Parameter]

host : A.B.C.D

IPv4 address of the SYSLOG server

: X:X::X:X

IPv6 address of the SYSLOG server

If you specify an IPv6 link local address, you must also specify the output interface (fe80::X%vlanN format)

[Initial value]

no logging host

[Input mode]

global configuration mode

[Description]

Specifies the IP address of the SYSLOG server to which log notifications are sent.

Up to 2 entries can be specified.

If this command is executed with the "no" syntax, the setting returns to its default value, and notifications are not sent.

[Example]

Set the SYSLOG server IPv4 address to 192.168.100.1.

```
SWX3220(config)#logging host 192.168.100.1
```

Set the SYSLOG server IPv6 address to fe80::2a0:deff:fe11:2233.

```
SWX3220(config)#logging host fe80::2a0:deff:fe11:2233%vlan1
```

4.12.2 Setting the notification format of the log

[Syntax]

logging format *type*
no logging format

[Parameter]

type : Log format type

Setting value	Description
legacy	Proprietary format that does not include the header section (time stamp, host name)

[Initial value]

no logging format

[Input mode]

global configuration mode

[Description]

Change the format of messages sent to the SYSLOG server.

If this command is executed with the "no" syntax, the header (time stamp, host name) is included in the SYSLOG message.

[Example]

Sets the format of the SYSLOG message to no header.

```
SWX3220(config)#logging format legacy
```

4.12.3 Setting the log facility value

[Syntax]

logging facility *facility*
no logging facility

[Parameter]

facility : Log facility value

Setting value	Description
0..23	facility value
user	1
local0..local7	16..23

[Initial value]

logging facility local0

[Input mode]

global configuration mode

[Description]

Change the facility value of messages sent to the SYSLOG server.

[Note]

The meanings of the facility values are assigned independently on each SYSLOG server.

[Example]

Set the facility value of the SYSLOG message to 10.

```
SWX3220(config)#logging facility 10
```

4.12.4 Set log output level (debug)

[Syntax]

logging trap debug
no logging trap debug

[Initial value]

no logging trap debug

[Input mode]

global configuration mode

[Description]

Output the debug level log to SYSLOG. If this command is executed with the "no" syntax, the log is not output.

Since enabling debug level will output a large volume of log data, you should enable this only if necessary.

If you use the **logging host** command to send notifications to the SYSYLOG server, you should ensure that there is sufficient disk space on the host. With the default setting, this is not output.

[Example]

Output the debug level log to SYSLOG.

```
SWX3220(config)#logging trap debug
```

4.12.5 Set log output level (informational)

[Syntax]

logging trap informational
no logging trap informational

[Initial value]

logging trap informational

[Input mode]

global configuration mode

[Description]

Outputs the informational level log to SYSLOG.

If this command is executed with the "no" syntax, the log is not output.

[Note]

This can be output to the console by executing the **logging stdout info** command.

[Example]

Output the informational level log to SYSLOG.

```
SWX3220(config)#logging trap informational
```

4.12.6 Set log output level (error)

[Syntax]

logging trap error
no logging trap error

[Initial value]

logging trap error

[Input mode]

global configuration mode

[Description]

Outputs the error level log to SYSLOG.

If this command is executed with the "no" syntax, the log is not output.

[Example]

Output the error level log to SYSLOG.

```
SWX3220(config)#logging trap error
```

4.12.7 Set log console output

[Syntax]

logging stdout info
no logging stdout info

[Initial value]

no logging stdout info

[Input mode]

global configuration mode

[Description]

Outputs the informational level SYSLOG to the console.

If this command is executed with the "no" syntax, the log is not output.

[Example]

Output the informational level SYSLOG to the console.

```
SWX3220(config)#logging stdout info
```

4.12.8 Set log output in event units

[Syntax]

logging event *type*
no logging *type*

[Parameter]

type : Type of events specified for log output

Setting value	Description
lan-map	LAN map

[Initial value]

no logging event lan-map

[Input mode]

global configuration mode

[Description]

Enables log output for the specified type of events.

If this command is executed with the "no" syntax, the log is not output.

[Example]

Enable log output for LAN map.

```
SWX3220(config)#logging event lan-map
```

4.12.9 Back up log

[Syntax]

save logging

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Saves all logs accumulated in RAM to Flash ROM.

Logs are accumulated in RAM, and are periodically backed up automatically to Flash ROM, but you can use this command to back up this data manually.

If the **logging backup sd enable** command has been set and an SD card is inserted, the log data is saved to Flash ROM and also simultaneously saved to the SD card with the following file name.

```
/swx3220/log/YYYYMMDD_syslog.txt

 YYYYMMDD … Year month day that the save logging command was executed
```

[Example]

Back up the log.

```
SWX3220#save logging
```

4.12.10 Set log backup to SD card

[Syntax]

logging backup sd enable
logging backup sd disable
no logging backup sd

[Keyword]

enable	:	Enable log backup to SD card
disable	:	Disable log backup to SD card

[Initial value]

logging backup sd disable

[Input mode]

global configuration mode

[Description]

Enables or disables backup of the log to the SD card.

If this is enabled, the log is saved on the SD card when you execute the **save logging** command.

If this command is executed with the "no" syntax, the setting returns to the default.

This is saved on the SD card with the following file name.

```
/swx3220/log/YYYYMMDD_syslog.txt

 YYYYMMDD … Year month day that the save logging command was executed
```

[Example]

Enable log backup to SD card.

```
SWX3220(config)#logging backup sd enable
```

4.12.11 Clear log

[Syntax]

clear logging

[Input mode]

privileged EXEC mode

[Description]

Clears the log.

[Example]

Clear the log.

```
SWX3220#clear logging
```

4.12.12 Show log

[Syntax]

show logging [reverse]

[Keyword]

reverse	:	Shows the log in reverse order

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the log that records the operating status of the unit. Normally the log is shown starting with the oldest events, but the display order is reversed if "reverse" is specified.

The log contains a maximum of 10,000 events. If this maximum number is exceeded, the oldest events are successively deleted. In order to save more than the maximum number of logs, you must use the **logging host** command to forward the log to the SYSLOG server and save it on the host.

The level of log events to be output can be specified by the **logging trap** command.

[Note]

Log events are accumulated in RAM, and are automatically backed up to Flash ROM at regular intervals. When the power is turned off, log entries that are not backed up will not be saved, so you must back them up manually if you want to save the log.

The log is maintained when the **reload** command or a firmware update etc. cause a reboot.

[Example]

Show the log.

```
SWX3220#show logging
```

4.13 SNMP

4.13.1 Set host that receives SNMP notifications

[Syntax]

snmp-server host *host_address type* **version** *version community*
snmp-server host *host_address type* **version** *version seclevel user*
no snmp-server host *host_address*
no snmp-server host *host_address type* **version** *version community*
no snmp-server host *host_address type* **version** *version seclevel user*

[Parameter]

host_address : Destination IPv4 address or IPv6 address for notifications

If you specify an IPv6 link local address, you must also specify the output interface (fe80::X%vlanN format)

type : Notification message

Setting value	Description
traps	Send notifications as traps (without response confirmation)
informs	Send notifications as inform requests (with response confirmation). This can be specified if *version* is '2c' or '3'.

version : SNMP version

Setting value	Description
1	Use SNMPv1
2c	Use SNMPv2c
3	Use SNMPv3

community : Community name (maximum 32 characters)

This can be specified if *version* is '1' or '2c'

When both ends are enclosed in "" or '', the "" and '' at both ends are not included in the number of characters

seclevel : Security level requested for authenticating the notification

This can be specified only if *version* is '3'

Setting value	Description
noauth	No authentication / No encryption (noAuthNoPriv)
auth	Authentication / No encryption (authNoPriv)
priv	Authentication / Encryption (authPriv)

user : User name (maximum 32 characters)

This can be specified only if *version* is '3'

When both ends are enclosed in "" or '', the "" and '' at both ends are not included in the number of characters

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Set the destination of SNMP notifications.

Up to 8 entries can be specified.

If this command is executed with the "no" syntax, the specified destination hosts are deleted.

[Note]

Note that if this is specified as an IPv6 link local address, and you add a setting that specifies a different transmitting interface for the same address, the combination of address and transmitting interface is considered to have changed, and all settings of the old combination are deleted. For example if there are multiple settings that specify "fe80::10%vlan1" and you newly add the setting "fe80::10%vlan2," all settings for "fe80::10%vlan1" are deleted, and only the settings of the added "fe80::10%vlan2" will remain.

[Example]

Using SNMPv1, set 192.168.100.11 as the destination for traps. Set "snmptrapname" as the trap community name.

```
SWX3220(config)#snmp-server host 192.168.100.11 traps version 1 snmptrapname
```

Using SNMPv2c, set 192.168.100.12 as the destination for notifications. Specify the notification type as informs, and the notification screen community name as "snmpinformsname".

```
SWX3220(config)#snmp-server host 192.168.100.12 informs version 2c snmpinformsname
```

Using SNMPv3, set 192.168.10.13 as the destination for notifications. Set the notification type to traps, set the security level for transmission to priv, and set the user name to "admin1".

```
SWX3220(config)#snmp-server host 192.168.10.13 traps version 3 priv admin1
```

4.13.2 Setting the time to wait before sending a notification message at system boot

[Syntax]

snmp-server startup-trap-delay *sec*
no snmp-server startup-trap-delay

[Parameter]

sec : <10-600>

Wait time (seconds)

[Initial value]

snmp-server startup-trap-delay 10

[Input mode]

global configuration mode

[Description]

Sets the time to wait before sending an SNMP notification message (trap) at system startup.

SNMP notification messages generated after system boot and before the wait time has elapsed will be sent after the wait time has elapsed.

If this command is executed with the "no" syntax, the setting is cleared.

[Note]

The wait time measurement starts and ends at the timing at which the following logs are output.

```
[    SNMP]:dbg: SNMP startup trap delay timer start (delay_sec : XX)
[    SNMP]:dbg: SNMP startup trap delay timer end (delay_sec : XX)
```

[Example]

Set the time to wait before sending an SNMP notification message at system startup to 30 seconds.

```
SWX3220(config)#snmp-server startup-trap-delay 30
```

4.13.3 Set notification type to transmit

[Syntax]

snmp-server enable trap *trap_type* [*trap_type*]
no snmp-server enable trap

[Parameter]

trap_type : Type of trap

Setting value	Description
coldstart	During power off/on and firmware update
warmstart	When executing the “reload” command
linkdown	At linkdown
linkup	At linkup
authentication	When authentication fails
temperature	When temperature abnormality is detected or resolved
fan	When fan speed changes / When fan stops
psu	When a change in power supply unit status occurs, or an error is detected/resolved
l2ms	When L2MS agent is detected or lost
errdisable	When ErrorDisable is detected or canceled
rmon	When RMON event is executed
termmonitor	When terminal monitoring is detected
bridge	When spanning tree root is detected / When topology is changed
loopdetect	During loop detection/clearing
vrrp	When VRRP event is executed
all	All trap types. All of the above trap types are specified in the config.

[Initial value]

no snmp-server enable trap

[Input mode]

global configuration mode

[Description]

Specifies the type of trap notification that is sent.

If this command is executed with the "no" syntax, traps are disabled.

[Note]

"psu" can only be specified on SWX3220-30MC and SWX3220-30TCs.

[Example]

Enable coldstart trap.

```
SWX3220(config)#snmp-server enable trap coldstart
```

Disable traps.

```
SWX3220(config)#no snmp-server enable trap
```

4.13.4 Set system contact

[Syntax]

snmp-server contact *contact*
no snmp-server contact

[Parameter]

contact	:	Name (maximum 255 characters) to register as the system contact

[Initial value]

no snmp-server contact

[Input mode]

global configuration mode

[Description]

Sets the MIB variable sysContact.

sysContact is a variable that is typically used to enter the name of the administrator or contact.

If this command is executed with the "no" syntax, the setting is deleted.

[Example]

Set the system contact to "swx_admin@sample.com".

```
SWX3220(config)#snmp-server contact swx_admin@sample.com
```

4.13.5 Set system location

[Syntax]

snmp-server location *location*
no snmp-server location

[Parameter]

location	:	Name to register as the system location (255 characters or less)

[Initial value]

no snmp-server location

[Input mode]

global configuration mode

[Description]

Sets the MIB variable sysLocation.

sysLocation is a variable that is generally used to enter the installed location of the unit.

If this command is executed with the "no" syntax, the setting is deleted.

[Example]

Set the system location as "MainOffice-1F".

```
SWX3220(config)#snmp-server location MainOffice-1F
```

4.13.6 Set SNMP community

[Syntax]

snmp-server community *community ro_rw*
no snmp-server community *community*

[Parameter]

community : Community name (maximum 32 characters)

When both ends are enclosed in "" or '', the "" and '' at both ends are not included in the number of characters

ro_rw : Access restriction

Setting value	Description
ro	Read only
rw	Write allowed

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Sets the SNMP community.

Up to 16 communities can be registered.

If this is executed with the "no" syntax, the specified community is deleted.

[Example]

Set the read-only community name to "public".

```
SWX3220(config)#snmp-server community public ro
```

Delete the "public" community.

```
SWX3220(config)#no snmp-server community public
```

4.13.7 Set SNMP view

[Syntax]

snmp-server view *view oid type*
no snmp-server view *view*

[Parameter]

view : View name (maximum 32 characters)

oid : MIB object ID

type : Type

Setting value	Description
include	Include the specified object ID in management
exclude	Exclude the specified object ID from management

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Sets the SNMP MIB view.

The MIB view is the set of MIB objects to specify when allowing access rights.

Up to 16 MIB views can be registered.

The combination of the *oid* parameter and the *type* parameter indicates whether the MIB sub-tree following the specified object ID is or is not subject to management. Taking the *oid* parameter and the *type* parameter together as one entry, you can specify multiple entries for each MIB view, up to a maximum of 8.

When multiple entries are specified, the *type* parameter for the specified object ID takes priority for entries that are contained at a lower level within the specified object ID.

If this command is executed with the "no" syntax, the MIB view is deleted. It is not possible to delete individual entries.

[Example]

Specify the "most" view which shows the internet node (1.3.6.1) and below.

```
SWX3220(config)#snmp-server view most 1.3.6.1 include
```

Specify the "standard" view which shows the mib-2 node (1.3.6.1.2.1) and below.

```
SWX3220(config)#snmp-server view standard 1.3.6.1.2.1 include
```

4.13.8 Set SNMP group

[Syntax]

snmp-server group *group seclevel* read *read_view* [write *write_view*]
snmp-server group *group seclevel* write *write_view* [read *read_view*]
no snmp-server group *group*

[Keyword]

read : Specify the MIB view that can be read by users belonging to this group

write : Specify the MIB view that can be written by users belonging to this group

[Parameter]

group : Group name (maximum 32 characters)

seclevel : Security level required of users belonging to this group

Setting value	Description
noauth	No authentication / No encryption (noAuthNoPriv)
auth	Authentication / No encryption (authNoPriv)
priv	Authentication / Encryption (authPriv)

read_view : Name of the MIB view (maximum 32 characters) that can be read by users belonging to this group

write_view : Name of the MIB view (maximum 32 characters) that can be written by users belonging to this group

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Sets the user group.

Access to MIB objects not included in the MIB view specified by this command is prohibited.

The MIB view is defined by the **snmp-server view** command.

The maximum number of entries is 16.

If this command is executed with the "no" syntax, the specified group setting is deleted.

[Example]

Create the user group "admins," and grant users belonging to the "admins" group full access rights to the "most" view.

```
SWX3220(config)#snmp-server group admins priv read most write most
```

Create the user group "users," and grant users belonging to the "users" group read access rights to the "standard" view.

```
SWX3220(config)#snmp-server group users auth read standard
```

4.13.9 Set SNMP user

[Syntax]

snmp-server user *user group* [auth *auth auth_pass* [priv *priv priv_pass*]]
no snmp-server user *user*

[Keyword]

auth : Set the authentication algorithm

priv : Set the encryption algorithm

[Parameter]

user : User name (maximum 32 characters)

When both ends are enclosed in "" or ", the "" and " at both ends are not included in the number of characters

group : Group name (maximum 32 characters)

When both ends are enclosed in "" or ", the "" and " at both ends are not included in the number of characters

auth : Authentication algorithm

Setting value	Description
md5	HMAC-MD5-96
sha	HMAC-SHA-96

auth_pass : Authentication password (8 or more characters, maximum 32 characters)

When both ends are enclosed in "" or ", the "" and " at both ends are not included in the number of characters

priv : Encryption algorithm

Setting value	Description
des	DES-CBC
aes	AES128-CFB

priv_pass : Encryption password (8 or more characters, maximum 32 characters)

When both ends are enclosed in "" or ", the "" and " at both ends are not included in the number of characters

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Specifies a user.

The group name of this command specifies the name defined by the snmp-server group command; according to the security level specified by the group setting, it specifies the algorithm and password that are used to authenticate and encrypt the content of communication.

It is not possible to only encrypt without authentication.

The maximum number of entries is 16.

The setting as to whether authentication and encryption are used, the algorithm, and the password, must match the user setting of the SNMP manager that is the other party.

If this command is executed with the "no" syntax, the setting of the specified user is deleted.

[Example]

Create "admin1" as a user. According to the specified group and the security level prescribed for that group, specify the protocol (SHA, AES) and password (passwd1234) used for authentication and encryption.

```
SWX3220(config)#snmp-server user admin1 admins auth sha passwd1234 priv aes
passwd1234
```

Create "user1" as a user. According to the specified group and the security level prescribed for that group, specify the protocol (SHA) and password (passwd5678) used for authentication and encryption.

```
SWX3220(config)#snmp-server user user1 users auth sha passwd5678
```

4.13.10 IP address restrictions for clients that can access the SNMP server

[Syntax]

snmp-server access *action info* [community *community*]
no snmp-server access [*action info* [community *community*]]

[Keyword]

community : Specify a community

[Parameter]

action : Specify behavior for access conditions

Setting value	Description
permit	"Permit" the condition

info : Sets the sending source IPv4/IPv6 address information used as a condition

Setting value	Description
A.B.C.D	Specifies an IPv4 address (A.B.C.D)
A.B.C.D/M	Specifies an IPv4 address (A.B.C.D) with a subnet mask length (Mbit)
X:X::X:X	Specifies an IPv6 address (X:X::X:X)
X:X::X:X/M	Specifies an IPv6 address (X:X::X:X) with a subnet mask length (Mbit)
any	Specifies all IPv4/IPv6 addresses

community : Community name (up to 32 characters)

Community to which the access conditions apply

If the community specification is omitted, the access conditions will apply to all communities

When both ends are enclosed in "" or ", the "" and " at both ends are not included in the number of characters.

[Initial value]

None

[Input mode]

global configuration mode

[Description]

Restrict client terminals that are permitted to access the SNMP server by IPv4/IPv6 address.

Up to 32 items can be set with this command, and those applied first are given priority.

When this command is set, all access that does not meet the registered conditions is denied.

However, if this command is not set, all access is permitted.

If this command is executed with the "no" syntax, the specified setting is cleared.

If community is omitted in the “no” syntax, all settings for the specified info are cleared.

If all parameters are omitted in the “no” syntax, all settings are cleared.

[Note]

The access restrictions of this command apply only to SNMPv1 and SNMPv2c access.

It does not apply to SNMPv3 access.

[Example]

Permit SNMP server access only from the 192.168.100.0/24 segment.

```
SWX3220(config)#snmp-server access permit 192.168.100.0/24
```

Restrict access to only 192.168.100.0/24 hosts with the ‘public’ community name and to only 192.168.100.12 hosts with the 'private’ community name.

```
SWX3220(config)#snmp-server access permit 192.168.100.0/24 community public
SWX3220(config)#snmp-server access permit 192.168.100.12 community private
```

4.13.11 Show SNMP community information

[Syntax]

show snmp community

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows SNMP community information.

Shows the community name, and access mode.

[Example]

Show SNMP community information.

```
SWX3220#show snmp community
SNMP Community information
  Community Name: public
  Access: Read-Only


  Community Name: private
  Access: Read-Write
```

4.13.12 Show SNMP view settings

[Syntax]

show snmp view

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the contents of the SNMP view settings.

Shows the view name, object ID, and type.

[Example]

Show the contents of the SNMP view settings.

```
SWX3220#show snmp view
SNMP View information
  View Name: most
  OID: 1.6.1
  Type: include

  View Name: standard
  OID: 1.3.6.1.2.1
  Type: include
```

4.13.13 Show SNMP group settings

[Syntax]

show snmp group

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the contents of the SNMP group settings.

Shows the group name, security level, reading view, and writing view.

[Example]

Show the contents of the SNMP group settings.

```
SWX3220#show snmp group
SNMP Group information
  Group Name: admins
  Security Level: priv
  Read View: most
  Write View: most

  Group Name: users
  Security Level: auth
  Read View: standard
  Write View: standard
```

4.13.14 Show SNMP user settings

[Syntax]

show snmp user

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the contents of the SNMP user settings.

Shows the engine ID, user name, affiliated group name, authentication method, and encryption method.

[Example]

Show the contents of the SNMP user settings.

```
SWX3220#show snmp user
SNMP User information
  EngineID: 0x8000049e0300a0deaeb90e

  User Name: admin1
  Group Name: admins
  Auth: sha
  Priv: aes

  User Name: user1
  Group Name: users
  Auth: sha
  Priv: none
```

4.14 RMON

4.14.1 Set RMON function

[Syntax]

rmon *switch*
no rmon

[Parameter]

switch : RMON function operation

Setting value	Description
enable	Enable RMON function
disable	Disable RMON function

[Initial value]

rmon enable

[Input mode]

global configuration mode

[Description]

Sets the system-wide operation of the RMON function.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

If this command is used to disable the system-wide RMON function, the following RMON group operations are disabled.

- Ethernet statistical information group
- History group
- Alarm group
- Event group

This command can be set using the private MIB ysrmonSetting (1.3.6.1.4.1.1182.3.7.1).

[Example]

Enable RMON function.

```
SWX3220(config)#rmon enable
```

Disable RMON function.

```
SWX3220(config)#rmon disable
```

4.14.2 Set RMON Ethernet statistical information group

[Syntax]

rmon statistics *index* [owner *owner*]
no rmon statistics *index*

[Parameter]

index : <1 - 65535>

Index of the Ethernet statistical information group (etherStatsIndex)

owner : Name of the Ethernet statistical information group owner (etherStatsOwner)

Maximum 127 characters
(if omitted : RMON_SNMP)

[Initial value]

none

[Input mode]

interface mode

[Description]

Enables the RMON Ethernet statistical information group setting for the applicable interface.

If this command is set, statistical information is collected, and the RMON MIB's etherStatsTable can be acquired.

This command can be specified a maximum number of eight times for the same interface.

If this command is executed with the "no" syntax, selete the setting and the collected statistical information.

[Note]

To enable the Ethernet statistical information group setting of the RMON function, it is necessary to enable the system-wide RMON function in addition to this command.

If this command is overwritten, the previously collected statistical information is deleted, and collection is once again started.

If the system-wide RMON function is disabled, collection of statistical information is interrupted. Subsequently, if the system-wide RMON function is enabled, the previously collected statistical data is deleted, and collection is once again started.

[Example]

Enable the RMON Ethernet statistical information group settings for port1.1.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#rmon statistics 1
```

4.14.3 Set RMON history group

[Syntax]

rmon history *index* [buckets *buckets*] [interval *interval*] [owner *owner*]
no rmon history *index*

[Parameter]

index	:	<1 - 65535> Index of history group (historyControlIndex)
buckets	:	<1 - 65535> Number of history group items to maintain (historyControlBucketsRequested) (if omitted : 50)
interval	:	<1 - 3600> Interval at which to save history group items (seconds) (historyControlInterval) (if omitted : 1800)
owner	:	Name of history group owner (historyControlOwner) Maximum 127 characters (if omitted : RMON_SNMP)

[Initial value]

none

[Input mode]

interface mode

[Description]

Enables RMON history group settings for the applicable interface.

If this command is set, it will be possible to acquire the RMON MIB's historyControlTable. After setting this command, history information is collected at the specified interval, and the RMON MIB's etherHistoryTable can be acquired.

This command can be specified a maximum number of eight times for the same interface.

If this command is executed with the "no" syntax, delete the setting and the collected historical information.

[Note]

To enable the history group setting of the RMON function, it is necessary to enable the system-wide RMON function in addition to this command.

If this command is overwritten, the previously collected historical information is deleted, and collection is once again started.

If the system-wide RMON function is disabled, collection of historical information is interrupted. Subsequently, if the system-wide RMON function is enabled, the previously collected historical data is deleted, and collection is once again started.

[Example]

Enable the RMON historical group settings for port1.1.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#rmon history 1
```

4.14.4 Set RMON event group

[Syntax]

rmon event *index type community* [description *description*] [owner *owner*]
no rmon event *index*

[Parameter]

index : <1 - 65535>

Index of event group (eventIndex)

type : Event type (eventType)

Setting value	Description
log	Record in log
trap	Send SNMP trap
log-trap	Record in log and send SNMP trap

community : Community name (eventCommunity)

Maximum 127 characters

This can be specified if *type* is "trap" or "log-trap".

description : Description of event (eventDescription)

Maximum 127 characters

(if omitted : RMON_SNMP)

owner : Name of event group owner (eventOwner)

Maximum 127 characters

(if omitted : RMON_SNMP)

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Enables the RMON event group settings.

If this command is set, it will be possible to acquire the RMON MIB's eventTable. Use the **rmon alarm** command to set the event group for this command.

If this command is executed with the "no" syntax, the setting value is deleted.

[Note]

To enable the event group setting of the RMON function, it is necessary to enable the system-wide RMON function in addition to this command.

In order for RMON to send an SNMP trap, you must have made SNMP trap transmission settings.

[Example]

After making SNMP trap settings, enable the RMON event group setting. Set the type of event as "log-trap", and the community name of the trap as "public".

```
SWX3220(config)#snmp-server host 192.168.100.3 traps version 2c public
SWX3220(config)#snmp-server enable trap rmon
SWX3220(config)#rmon event 1 log-trap public
```

4.14.5 Set RMON alarm group

[Syntax]

rmon alarm *index variable* interval *interval* [*type*] rising-threshold *rising_threshold* event *rising_event-index* falling-threshold *falling_threshold* event *falling_event_index* [alarmstartup *startup*] [owner *owner*]

rmon alarm *index variable* interval *interval* [*type*] rising-threshold *rising_threshold* event *rising_event-index* [owner *owner*]

rmon alarm *index variable* interval *interval* [*type*] falling-threshold *falling_threshold* event *falling_event_index* [owner *owner*]

no rmon alarm *index*

[Parameter]

index : <1-65535>

Index of alarm group (alarmIndex)

variable : MIB object to be monitored (alarmVariable)

interval : <1-2147483647>

Sampling interval (seconds)(alarmInterval)

type : Sampling type (alarmSampleType)

Setting value	Description
absolute	Compare by absolute value. Directly compare sample value and threshold value
delta	Compare by relative value. Compare the difference between the latest sample value and the previous sample value

(if omitted : absolute)

rising_threshold : <1-2147483647>

Upper threshold value (alarmRisingThreshold)

rising_event_index : <1-65535>

Event index (alarmRisingEventIndex)

falling_threshold : <1-2147483647>

Lower threshold value (alarmFallingThreshold)

falling_event_index : <1-65535>

Event index (alarmFallingEventIndex)

startup : <1-3>

Threshold value used for first alarm decision (alarmStartupAlarm)

Setting value	Description
1	Use only upper threshold value (risingAlarm)
2	Use only lower threshold value (fallingAlarm)
3	Use both upper threshold value and lower threshold value (risingOrFallingAlarm)

(if omitted : 3)

owner : Name of alarm group owner (alarmOwner)

maximum 127 characters
(if omitted : RMON_SNMP)

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Enables the RMON alarm group settings.

Set *variable* as the MIB object that will be the target of monitoring by the RMON alarm group. Of the etherStatsEntry(.1.3.6.1.2.1.16.1.1.1) MIB objects, *variable* can be specified only as a MIB object that has a counter type. This can be specified in the following three formats.

- etherStatsEntry.X.Y
- (OID name under etherStatsEntry).Y
- .1.3.6.1.2.1.16.1.1.1.X.Y

For example, if specifying etherStatsPkts.1(.1.3.6.1.2.1.16.1.1.1.5.1), it can be specified in any of the following formats.

Format	Description
etherStatsEntry.X.Y	etherStatsEntry.5.1
(OID name under etherStatsEntry).Y	etherStatsPkts.1
.1.3.6.1.2.1.16.1.1.1.X.Y	.1.3.6.1.2.1.16.1.1.1.5.1

You can use a format that specifies either *rising_threshold* or *falling_threshold*, not both. In this case, the following values are used for parameters whose setting is omitted.

- Use only *rising_threshold*
  - *falling_threshold* : Same value as *rising_threshold*
  - *falling_event_index* : Same value as *rising_event_index*
  - *startup* : 1 (Use only upper_threshold)
- Use only *falling_threshold*
  - *rising_threshold* : Same value as *falling_threshold*
  - *rising_event_index* : Same value as *falling_event_index*
  - *startup* : 2 (Use only lower_threshold)

If this command is set, it will be possible to acquire the RMON MIB's alarmTable.

If this command is executed with the "no" syntax, the setting value is deleted.

[Note]

To enable the alarm group setting of the RMON function, it is necessary to enable the system-wide RMON function in addition to this command.

The MIB object specified in *variable* is a MIB object of the Ethernet statistical information group. If an Ethernet statistical information group possessing the applicable index has not been created, this command returns an error.

The Ethernet statistical information group can be created by the **rmon statistics** command. If the Ethernet statistical information group being used by this command is deleted, this command is also deleted.

The event index specifies the index that is set by the **rmon event** command. If the event group being used by this command is deleted, this command is also deleted.

The *rising_threshold* value must be a higher value than the *falling_threshold* value.

If this command is overwritten, the previous sampling data is deleted, and sampling is once again started.

If the system-wide RMON function is disabled, sampling is interrupted. Subsequently, if the system-wide RMON function is enabled, the previous sampling data is deleted, and sampling is once again started.

[Example]

Enable the RMON alarm group settings with the following conditions.

- The MIB object to be monitored is etherStatsPkts.1.
- The sampling interval is 180 seconds.
- The sampling type is delta.
- The upper threshold value is 3000, and the event when rising above the upper threshold value is 1.

- The lower threshold value is 2000, and the event when falling below the lower threshold value is 1.

```
SWX3220(config)#rmon alarm 1 etherStatsPkts.1 interval 180 delta rising-threshold
3000 event 1 falling-threshold 2000 event 1
```

4.14.6 Show RMON function status

[Syntax]

show rmon

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the settings and status of the RMON function.

The following items are shown.

- System-wide RMON function settings
- RMON function settings for each group
  - Ethernet statistical information group
  - History group
  - Alarm group
  - Event group

[Example]

```
SWX3220>show rmon
rmon: Enable

statistics:
    rmon collection index 1
    stats->ifindex = 5001
    input packets 7, bytes 600, drop events 0, multicast packets 4
    output packets 17, bytes 2091, multicast packets 17 broadcast packets 0

history:
    history index = 1
    data source ifindex = 5001
    buckets requested = 50
    buckets granted = 50
    Interval = 1800
    Owner RMON_SNMP

event:
    event Index = 1
       Description RMON_SNMP
       Event type Log
       Event community name RMON_SNMP
       Last Time Sent = 00:00:58
       Owner  RMON_SNMP

alarm:
    alarm Index = 1
      alarm status = VALID
        alarm Interval = 15
        alarm Type is Absolute
        alarm Value  = 0
        alarm Rising Threshold = 10
        alarm Rising Event = 1
        alarm Falling Threshold = 7
        alarm Falling Event = 1
        alarm Startup Alarm = 3
        alarm Owner is RMON_SNMP
```

4.14.7 Show RMON Ethernet statistical information group status

[Syntax]

show rmon statistics

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the settings and status of the RMON Ethernet statistical information group.

The following items are shown.

- Index
- Applicable interface
- Input packets
- Output packets

[Example]

```
SWX3220>show rmon statistics
    rmon collection index 1
    stats->ifindex = 5001
    input packets 7, bytes 600, drop events 0, multicast packets 4
    output packets 17, bytes 2091, multicast packets 17 broadcast packets 0
```

4.14.8 Show RMON history group status

[Syntax]

show rmon history

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the settings and status of the RMON history group.

The following items are shown.

- Index
- Applicable interface
- Number of history group items to maintain
- Interval at which to save history group items
- Owner name

[Example]

```
SWX3220>show rmon history
        history index = 1
        data source ifindex = 5001
        buckets requested = 50
        buckets granted = 50
        Interval = 1800
        Owner RMON_SNMP
```

4.14.9 Show RMON event group status

[Syntax]

show rmon event

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the settings and status of the RMON event group.

The following items are shown.

- Index
- Description of event
- Type of event
- Community name when sending trap
- Time of executing event
- Owner name

[Example]

```
SWX3220>show rmon event
    event Index = 1
       Description RMON_SNMP
       Event type Log
       Event community name RMON_SNMP
       Last Time Sent = 00:00:58
       Owner  RMON_SNMP
```

4.14.10 Show RMON alarm group status

[Syntax]

show rmon alarm

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the settings and status of the RMON alarm group.

The following items are shown.

- Index
- Alarm status
- MIB object to be monitored
- Sampling interval
- Sampling type
- Measured value
- Upper threshold value
- Event for upper threshold value
- Lower threshold value
- Event for lower threshold value
- Startup alarm
- Owner name

[Example]

```
SWX3220>show rmon alarm
      alarm Index = 1
        alarm status = VALID
          alarm Interval = 15
          alarm Type is Absolute
          alarm Value  = 0
          alarm Rising Threshold = 10
          alarm Rising Event = 1
          alarm Falling Threshold = 7
          alarm Falling Event = 1
          alarm Startup Alarm = 3
          alarm Owner is RMON_SNMP
```

4.14.11 Clear counters of the RMON Ethernet statistical information group

[Syntax]

rmon clear counters

[Input mode]

interface mode

[Description]

Clears the counters of the RMON Ethernet statistical information group for the applicable interface.

[Example]

Clear the counters of the RMON Ethernet statistical information group for port1.1.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#rmon clear counters
```

4.15 sFlow

4.15.1 Set sFlow function

[Syntax]

sflow *switch*
no sflow

[Parameter]

switch : sFlow function operation

Setting value	Description
enable	Enable sFlow function
disable	Disable sFlow function

[Initial value]

sflow disable

[Input mode]

global configuration mode

[Description]

This sets the sFlow function operation.

If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

Enable the sFlow function.

```
SWX3220(config)#sflow enable
```

4.15.2 Set sFlow agent

[Syntax]

sflow agent *address*
no sflow agent

[Parameter]

address : A.B.C.D
IPv4 address
: X:X::X:X
IPv6 address

[Initial value]

None

[Input mode]

global configuration mode

[Description]

Sets the IP address for the sFlow agent.

The IP address set with this command is used in the sFlow header of the sFlow datagram.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

An IPv6 address cannot specified if the stack function is enabled.

[Example]

Sets the IP address for the sFlow agent to "192.168.100.240".

```
SWX3220(config)#sflow agent 192.168.100.240
```

4.15.3 Set sFlow collector

[Syntax]

sflow collector *address* [*port*]
no sflow collector

[Parameter]

address	:	A.B.C.D IPv4 address
	:	X:X::X:X IPv6 address
port	:	<1 - 65535> Destination UDP port number for sFlow collector Default value is 6343

[Initial value]

None

[Input mode]

global configuration mode

[Description]

Sets the IP address and destination UDP port number for the sFlow collector.
If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

An IPv6 address cannot specified if the stack function is enabled.

[Example]

Sets the IP address for the sFlow collector to "192.168.100.240".

```
SWX3220(config)#sflow collector 192.168.100.240
```

4.15.4 Set maximum size of sFlow datagram

[Syntax]

sflow collector max-datagram-size *size*
no sflow collector max-datagram-size

[Parameter]

size	:	<512 - 1452> (bytes)

[Initial value]

sflow collector max-datagram-size 1400

[Input mode]

global configuration mode

[Description]

This sets the maximum size of datagrams transmitted from the sFlow agent to the sFlow collector.
If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

Set maximum size to 1000 bytes for sFlow datagrams.

```
SWX3220(config)#sflow collector max-datagram-size 1000
```

4.15.5 Set sampling rate of packet flow sampling

[Syntax]

sflow sampling-rate *rate*
no sflow sampling-rate

[Parameter]

rate : <256 - 1000000000>

[Initial value]

None

[Input mode]

interface mode

[Description]

Sets the sampling rate used for packet flow on the applicable port when executing packet flow sampling.

If this command is not set, packet flow sampling is not implemented.

This command can be specified only for LAN/SFP port.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

On the SWX3220-30MC and SWX3220-30TCs, the following limitations apply.

- This can be set for up to five LAN/SFP port.
- When constructing a stack, this can be set for up to five LAN/SFP port per member switch.
- The same port cannot be used for both this command and the **mirror** command.

[Example]

Sets the sampling rate of packet flow sampling to 10000.

```
SWX3220(config-if)#sflow sampling-rate 10000
```

4.15.6 Set maximum Ethernet frame header size for packet flow sampling

[Syntax]

sflow max-header-size *size*
no sflow max-header-size

[Parameter]

size : <14 - 256> (bytes)

[Initial value]

sflow max-header-size 128

[Input mode]

interface mode

[Description]

Sets the maximum Ethernet frame header size used for packet flow sampling on the applicable port.

If this command is executed with the "no" syntax, the setting returns to the default.

This command can be specified only for LAN/SFP port.

[Example]

This sets the maximum Ethernet frame header size for packet flow sampling to 100.

```
SWX3220(config-if)#sflow max-header-size 100
```

4.15.7 Set polling interval for counter sampling

[Syntax]

sflow polling-interval *interval*

no sflow polling-interval

[Parameter]

interval : <1 - 86400> (seconds)

[Initial value]

None

[Input mode]

interface mode

[Description]

Sets the polling interval used when executing counter sampling on the applicable port.

If this command is not set, counter sampling is not implemented.

This command can be specified only for LAN/SFP port.

If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

Sets the counter sampling interval to 100 seconds.

```
SWX3220(config-if)#sflow polling-interval 100
```

4.15.8 Show sFlow status

[Syntax]

show sflow

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

Shows the status of sFlow.

[Example]

This shows the status of sFlow.

```
SWX3220#show sflow
sFlow Global Configuration:
  sFlow Feature      : Enabled
  Agent Address      : 192.168.100.240
  Collector Address  : 192.168.100.2
  Collector UDP Port : 6343
  Max Datagram Size  : 1400(bytes)

sFlow Port Configuration:

            Sampling-Rate    Polling-Interval
  Port      (1 in N pkts)    (secs)
  ----------------------------------------------------------
  port1.1   300              30
  port1.5   500              (NOT SET)

sFlow Drop Sampling Count : 0
```

4.15.9 Show sFlow sampling information

[Syntax]

show sflow sampling [*ifname*]

[Parameter]

ifname : LAN/SFP port interface name

Interface to show

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

Shows sFlow sampling information for the interface specified by *ifname*.

If *ifname* is omitted, information is shown for all interfaces.

[Note]

This command cannot be executed on non-main member switches when the stack function is enabled.

When the stack function is enabled, this information is not synchronized between main and members.

On SWX3220-30MC and SWX3220-30TCs, the remaining number of packets until the next packet is sampled during packet flow sampling is not displayed.

[Example]

Shows the sFlow sampling information.

```
SWX3220#show sflow sampling
sFlow sampling information:

  Interface port1.1:
    Packet-Flow-Sampling:
      Sampling count : 40
      Number of packets remaining until next sampling:
        Ingress : 208
        Egress  : 590
    Counter-Sampling:
      Sampling count : 65
      Number of seconds remaining until next sampling : 15

  Interface port1.5:
    Packet-Flow-Sampling:
      Sampling count : 15
      Number of packets remaining until next sampling:
        Ingress : 876
        Egress  : 870
    Counter-Sampling:
      (NOT SET)
```

4.16 Telnet server

4.16.1 Start Telnet server and change listening port number

[Syntax]

telnet-server enable [*port*]
telnet-server disable
no telnet-server

[Keyword]

enable	:	Telnet server is enabled
disable	:	Telnet server is disable

[Parameter]

port	:	<1-65535> Listening port of the Telnet server (if omitted: 23)

[Initial value]

telnet-server disable

[Input mode]

global configuration mode

[Description]

Enables the Telnet server. You can also specify the listening TCP port number.

If this command is executed with the "no" syntax, the function is disabled.

[Example]

Start the Telnet server with 12345 as the listening port number.

```
SWX3220(config)#telnet-server enable 12345
```

4.16.2 Show Telnet server settings

[Syntax]

show telnet-server

[Input mode]

privileged EXEC mode

[Description]

Shows the settings of the Telnet server. The following items are shown.

- Telnet server function enabled/disabled status
- Listening port number
- VLAN interface that is permitted to access the TELNET server
- Filter that controls access to the TELNET server

[Example]

Show the settings of the Telnet server.

```
SWX3220#show telnet-server
Service:Enable
Port:23
Management interface(vlan): 1
Interface(vlan):1, 2, 3
Access:
    deny   192.168.100.5
    permit 192.168.100.0/24
```

4.16.3 Set host that can access the Telnet server

[Syntax]

telnet-server interface *interface*
no telnet-server interface *interface*

[Parameter]

interface	:	VLAN interface name

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Sets the VLAN interface that allows access to the Telnet server.

If this command is executed with the "no" syntax, the specified interface is deleted.

This command can be used to specify up to eight items, which are applied in the order that they are specified.

If this command is not set, access is permitted only from the management VLAN.

[Note]

If **telnet-server enable** is not specified, this command does not function.

[Example]

Allow access to the Telnet server from the hosts connected to VLAN #1 and VLAN #2.

```
SWX3220(config)#telnet-server interface vlan1
SWX3220(config)#telnet-server interface vlan2
```

4.16.4 Restrict access to the TELNET server according to the IP address of the client

[Syntax]

telnet-server access *action info*
no telnet-server access [*action info*]

[Parameter]

action : Specifies the action for the access condition

Setting value	Description
deny	"Deny" the condition
permit	"Permit" the condition

info : Specifies the transmission-source IPv4 address or IPv6 address that is the condition.

Setting value	Description
A.B.C.D	Specifies an IPv4 address (A.B.C.D)
A.B.C.D/M	Specifies an IPv4 address (A.B.C.D) with subnet mask length (Mbit)
X:X::X:X	Specifies an IPv6 address (X:X::X:X)
X:X::X:X/M	Specifies an IPv6 address (X:X::X:X) with subnet mask length (Mbit)
any	Applies to all IPv4 addresses and IPv6 addresses

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Restrict access to the TELNET server according to the client terminal's IPv4/IPv6 address.

Up to eight instances of this command can be set, and those that are specified earlier take priority for application.

If this command is set, all access that does not satisfy the registered conditions is denied.

However, if this command is not set, all access is permitted.

If this command is executed with the "no" syntax, the specified setting is deleted.

If this command is executed with the "no" syntax, and parameter is omitted, all settings are deleted.

[Note]

If **telnet-server enable** is not specified, this command does not function.

[Example]

Permit access to the TELNET server only from 192.168.1.1 and the 192.168.10.0/24 segment.

```
SWX3220(config)#telnet-server access permit 192.168.1.1
SWX3220(config)#telnet-server access permit 192.168.10.0/24
```

Deny only access to the TELNET server from the segment 192.168.10.0/24.

```
SWX3220(config)#telnet-server access deny 192.168.10.0/24
SWX3220(config)#telnet-server access permit any
```

4.17 Telnet client

4.17.1 Start Telnet client

[Syntax]

telnet *host* [*port*]

[Parameter]

host : Remote host name, IPv4 address (A.B.C.D), or IPv6 address(X:X::X:X)

If you specify an IPv6 link local address, you must also specify the output interface (fe80::X%vlanN format)

port : <1-65535>

Port number to use (if omitted: 23)

[Initial value]

none

[Input mode]

privileged EXEC mode

[Description]

Connects to the specified host via Telnet.

[Example]

Connect via Telnet to port number 12345 of the host at IPv4 address 192.168.100.1.

```
SWX3220#telnet 192.168.100.1 12345
```

Connect via Telnet to port number 12345 of the host at IPv6 address fe80::2a0:deff:fe11:2233.

```
SWX3220#telnet fe80::2a0:deff:fe11:2233%vlan1 12345
```

4.17.2 Enable Telnet client

[Syntax]

telnet-client *switch*
no telnet-client

[Parameter]

switch : Whether to enable TELNET client

Setting value	Description
enable	Enable
disable	Disable

[Initial value]

telnet-client disable

[Input mode]

global configuration mode

[Description]

Enables use of the telnet command as a Telnet client.

If this command is executed with the "no" syntax, the Telnet client is disabled.

[Example]

Enable the Telnet client.

```
SWX3220(config)#telnet-client enable
```

4.18 TFTP server

4.18.1 Start TFTP server and change listening port number

[Syntax]

tftp-server enable [*port*]
tftp-server disable
no tftp-server

[Keyword]

enable	:	TFTP server is enabled
disable	:	TFTP server is disable

[Parameter]

port	:	<1-65535> Listening port number of the TFTP server (if omitted: 69)

[Initial value]

tftp-server disable

[Input mode]

global configuration mode

[Description]

Enables the TFTP server. You can also specify the listening TCP port number.

If this command is executed with the "no" syntax, the TFTP server is disabled.

[Example]

Start the TFTP server with 12345 as the listening port number.

```
SWX3220(config)#tftp-server enable 12345
```

4.18.2 Show TFTP server settings

[Syntax]

show tftp-server

[Input mode]

privileged EXEC mode

[Description]

Shows the settings of the TFTP server. The following items are shown.

- TFTP server function enabled/disabled status
- Listening port number
- VLAN interface that is permitted to access the TFTP server

[Example]

Show the settings of the TFTP server.

```
SWX3220#show tftp-server
Service:Enable
Port:69
Management interface(vlan): 1
Interface(vlan):1, 2, 3
```

4.18.3 Set hosts that can access the TFTP server

[Syntax]

tftp-server interface *interface*
no tftp-server interface *interface*

[Parameter]

interface	:	VLAN interface name

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Sets the VLAN interface that allows access to the TFTP server.

If this command is executed with the "no" syntax, the specified interface is deleted

This command can be used to specify up to eight items, which are applied in the order that they are specified.

If this command is not set, access is permitted only from the management VLAN.

[Example]

Allow access to the TFTP server from the hosts connected to VLAN #1 and VLAN #2.

```
SWX3220(config)#tftp-server interface vlan1
SWX3220(config)#tftp-server interface vlan2
```

4.19 HTTP server

4.19.1 Start HTTP server and change listening port number

[Syntax]

http-server enable [*port*]
http-server disable
no http-server

[Keyword]

enable	:	HTTP server is enabled
disable	:	HTTP server is disabled

[Parameter]

port	:	<1-65535> Listening port number of the HTTP server (if omitted: 80)

[Initial value]

http-server disable

[Input mode]

global configuration mode

[Description]

Enables the HTTP server. You can also specify the listening TCP port number.

If this command is executed with the "no" syntax, the function is disabled.

[Example]

Start the HTTP server with 8080 as the listening port number.

```
SWX3220(config)#http-server enable 8080
```

4.19.2 Start secure HTTP server and change listening port number

[Syntax]

http-server secure enable [*port*]
http-server secure disable
no http-server secure

[Keyword]

enable	:	Enable the secure HTTP server
disable	:	Disable the secure HTTP server

[Parameter]

port	:	<1-65535> Listening port number of the secure HTTP server (if omitted: 443)

[Initial value]

http-server secure disable

[Input mode]

global configuration mode

[Description]

Enables the secure HTTP server. You can also specify the listening TCP port number.

If this command is executed with the "no" syntax, the function is disabled.

If the secure HTTP server is enabled, encryption is performed in software, meaning that depending on the amount of traffic, the CPU usage rate will rise.

To avoid a high usage rate, it is desirable to avoid access by multiple users to an automatically updated web page such as the dashboard or the LAN map.

[Example]

Start the secure HTTP server with 8080 as the listening port number.

```
SWX3220(config)#http-server secure enable 8080
```

4.19.3 Show HTTP server settings

[Syntax]

show http-server

[Input mode]

privileged EXEC mode

[Description]

Shows the settings of the HTTP server. The following items are shown.

- HTTP server function enabled/disabled status
- HTTP server's listening port number
- VLAN interface that is permitted to access the HTTP server
- Filter that controls access to the HTTP server
- Secure HTTP server function enabled/disabled status
- Log-in timeout time

[Example]

Show the settings of the HTTP server.

```
SWX3220#show http-server
HTTP :Enable(80)
HTTPS:Disable
Management interface(vlan): 1
Interface(vlan):1
Access:None
Login timeout:30 min 51 sec
```

4.19.4 Set hosts that can access the HTTP server

[Syntax]

http-server interface *interface*
no http-server interface *interface*

[Parameter]

interface	:	VLAN interface name

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Sets the VLAN interface that allows access to the HTTP server.

If this command is executed with the "no" syntax, the specified interface is deleted.

This command can be used to specify up to eight items, which are applied in the order that they are specified.

If this command is not set, access is permitted only from the management VLAN.

[Example]

Allow access to the HTTP server from the hosts connected to VLAN #1 and VLAN #2.

```
SWX3220(config)#http-server interface vlan1
SWX3220(config)#http-server interface vlan2
```

4.19.5 Restrict access to the HTTP server according to the IP address of the client

[Syntax]

http-server access *action info*
no http-server access [*action info*]

[Parameter]

action : Specifies the action for the access condition

Setting value	Description
deny	"Deny" the condition
permit	"Permit" the condition

info : Specifies the transmission-source IPv4 address or IPv6 address that is the condition.

Setting value	Description
A.B.C.D	Specifies an IPv4 address (A.B.C.D)
A.B.C.D/M	Specifies an IPv4 address (A.B.C.D) with subnet mask length (Mbit)
X:X::X:X	Specifies an IPv6 address (X:X::X:X)
X:X::X:X/M	Specifies an IPv6 address (X:X::X:X) with subnet mask length (Mbit)
any	Applies to all IPv4 addresses and IPv6 addresses

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Restrict access to the HTTP server according to the client terminal's IPv4/IPv6 address.

Up to eight instances of this command can be set, and those that are specified earlier take priority for application.

If this command is set, all access that does not satisfy the registered conditions is denied.

However, if this command is not set, all access is permitted.

If this command is executed with the "no" syntax, the specified setting is deleted.

If this command is executed with the "no" syntax, and parameter is omitted, all settings are deleted.

[Note]

If **http-server enable** or **http-server secure enable** are not specified, this command does not function.

[Example]

Permit access to the HTTP server only from 192.168.1.1 and the 192.168.10.0/24 segment.

```
SWX3220(config)#http-server access permit 192.168.1.1
SWX3220(config)#http-server access permit 192.168.10.0/24
```

Deny access to the HTTP server only from 192.168.10.0/24 segment.

```
SWX3220(config)#http-server access deny 192.168.10.0/24
SWX3220(config)#http-server access permit any
```

4.19.6 Web GUI display language

[Syntax]

http-server language *lang*
no http-server language

[Parameter]

lang : Specify the language

Setting value	Description
japanese	Japanese
english	English

[Initial value]

http-server language japanese

[Input mode]

global configuration mode

[Description]

Sets the Web GUI display language.

If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

Set the Web GUI display language to English.

```
SWX3220(config)#http-server language english
```

4.19.7 Set log-in timeout time for HTTP server

[Syntax]

http-server login-timeout *min* [*sec*]
no http-server login-timeout

[Parameter]

min : <0-35791>

Timeout time (minutes)

sec : <0-2147483>

Timeout time (seconds)

[Initial value]

http-server login-timeout 5

[Input mode]

global configuration mode

[Description]

Specify the time until automatic logout when there has been no access to the HTTP server.

If sec is omitted, 0 is specified.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

The smallest value that can be specified is one minute.

[Example]

Set the timeout time for the HTTP server to 2 minutes 30 seconds.

```
SWX3220(config)#http-server login-timeout 2 30
```

4.20 HTTP Proxy

4.20.1 Enable HTTP Proxy function

[Syntax]

http-proxy *switch*
no http-proxy

[Parameter]

switch : Whether to enable HTTP Proxy function

Setting value	Description
enable	Enable
disable	Disable

[Initial value]

http-proxy disable

[Input mode]

global configuration mode

[Description]

Enables the HTTP Proxy function of the HTTP server.

If this command is executed with the "no" syntax, the function is disabled.

[Example]

Enable the HTTP Proxy function of the HTTP server.

```
SWX3220(config)#http-proxy enable
```

4.20.2 Set HTTP Proxy function timeout

[Syntax]

http-proxy timeout *time*
no http-proxy timeout [*time*]

[Parameter]

time : <1-180>

Time (seconds) until timeout occurs

[Initial value]

http-proxy timeout 60

[Input mode]

global configuration mode

[Description]

Specifies the timeout time when acquiring the Web GUI of an L2MS agent.

If this command is executed with the "no" syntax, the setting will be 60 seconds.

[Example]

Set HTTP Proxy function's timeout duration to two minutes.

```
SWX3220(config)#http-proxy timeout 120
```

4.20.3 Show HTTP Proxy function settings

[Syntax]

show http-proxy

[Input mode]

privileged EXEC mode

[Description]

Shows the settings of the HTTP Proxy function. The following items are shown.

- HTTP Proxy function enabled/disabled status
- Timeout time

[Example]

Show the settings of the HTTP Proxy function.

```
SWX3220#show http-proxy
Service:Enable
Timeout:60
```

4.21 SSH server

4.21.1 Start SSH server and change listening port number

[Syntax]

ssh-server enable [*port*]
ssh-server disable
no ssh-server

[Keyword]

enable	:	SSH server is enabled
disable	:	SSH server is disable

[Parameter]

port	:	<1-65535> Listening port of the SSH server (if omitted: 22)

[Initial value]

ssh-server disable

[Input mode]

global configuration mode

[Description]

Enables the SSH server. You can also specify the listening TCP port number.

In order to enable the SSH server, the host key must be created in advance (ssh-server host key generate).

If this command is executed with the "no" syntax, disable the SSH server.

[Note]

In order to log in from the SSH client, the user name and password must be registered in advance (username).

[Example]

Start the SSH server with 12345 as the listening port number.

```
SWX3220#ssh-server host key generate
SWX3220#configure terminal
SWX3220(config)#ssh-server enable 12345
```

4.21.2 Show SSH server settings

[Syntax]

show ssh-server

[Input mode]

privileged EXEC mode

[Description]

Shows the settings of the SSH server.

The following items are shown.

- SSH server function enabled/disabled status

- Listening port number
- Whether SSH server host key exists
- VLAN interface permitted to access the SSH server
- Filter that controls access to the SSH server

[Example]

Show the settings of the SSH server.

```
SWX3220#show ssh-server
Service:Enable
Port:23
Hostkey:Generated
Management interface(vlan): 1
Interface(vlan):1, 2, 3
Access:
    deny   192.168.100.5
    permit 192.168.100.0/24
```

4.21.3 Set host that can access the SSH server

[Syntax]

ssh-server interface *ifname*
no ssh-server interface *ifname*

[Parameter]

ifname : VLAN interface name

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Sets the VLAN interface that allows access to the SSH server.

If this command is executed with the "no" syntax, delete the specified interface.

Up to eight instances of this command can be set, and those that are specified earlier take priority for application.

If this command is not set, access is permitted only from the maintenance VLAN.

[Example]

Allow access to the SSH server from the hosts connected to VLAN #1 and VLAN #2.

```
SWX3220(config)#ssh-server interface vlan1
SWX3220(config)#ssh-server interface vlan2
```

4.21.4 Set client that can access the SSH server

[Syntax]

ssh-server access *action info*
no ssh-server access [*action info*]

[Parameter]

action : Specifies the action for the access condition

Setting value	Description
deny	"Deny" the condition
permit	"Permit" the condition

info : Specifies the transmission-source IPv4 address or IPv6 address that is the condition

Setting value	Description
A.B.C.D	Specifies an IPv4 address (A.B.C.D)
A.B.C.D/M	Specifies an IPv4 address (A.B.C.D) with subnet mask length (Mbit)
X:X::X:X	Specifies an IPv6 address (X:X::X:X)
X:X::X:X/M	Specifies an IPv6 address (X:X::X:X) with subnet mask length (Mbit)
any	Applies to all IPv4 addresses and IPv6 address

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Restrict access to the SSH according to the client terminal's IPv4/IPv6 address.

Up to eight instances of this command can be set, and those that are specified earlier take priority for application.

If this command is set, all access that does not satisfy the registered conditions is denied.

However, if this command is not set, all access is permitted.

If this command is executed with the "no" syntax, the specified setting is deleted.

If parameters are omitted with the "no" syntax, the all setting are deleted.

[Note]

If **ssh-server enable** command is not specified, this command does not function.

[Example]

Permit access to the SSH server only from 192.168.1.1 and the 192.168.10.0/24 segment.

```
SWX3220(config)#ssh-server access permit 192.168.1.1
SWX3220(config)#ssh-server access permit 192.168.10.0/24
```

Deny only access to the SSH server from the segment 192.168.10.0/24.

```
SWX3220(config)#ssh-server access deny 192.168.10.0/24
SWX3220(config)#ssh-server access permit any
```

4.21.5 Generate SSH server host key

[Syntax]

ssh-server host key generate [bit *bit*]

[Parameter]

bit : 1024, 2048

Bit length of RSA key

[Initial value]

none

[Input mode]

privileged EXEC mode

[Description]

Sets the host RSA key and host DSA key of the SSH server.

For the RSA key, the *bit* parameter can be used to specify the number of bits in the generated key. The DSA key generates a 1024-bit key.

[Note]

In order to use the SSH server function, this command must be executed in advance to generate the host keys.

If this command is executed when the host keys have already been specified, the user is asked to confirm whether to update the host keys.

It might take several minutes of time to generate the host keys.

This command can be executed only if the SSH server is disabled.

[Example]

Generate a 2048-bit RSA key and a DSA key.

```
SWX3220#ssh-server host key generate bit 2048
```

4.21.6 Clear SSH server host key

[Syntax]

clear ssh-server host key

[Input mode]

privileged EXEC mode

[Description]

Deletes the host RSA key and host DSA key of the SSH server.

[Note]

This command can be executed only if the SSH server is disabled.

[Example]

Delete the host RSA key and host DSA key.

```
SWX3220#clear ssh-server host key
```

4.21.7 Show SSH server public key

[Syntax]

show ssh-server host key [fingerprint]

[Keyword]

fingerprint	:	Show key fingerprint

[Input mode]

privileged EXEC mode

[Description]

Shows the public key of the SSH server.

If the "fingerprint" keyword is specified, the public key's key length, key fingerprint, and ASCII art are shown.

[Note]

Both the MD5 and SHA256 key fingerprint hash algorithms are shown.

[Example]

Show the public key.

```
SWX3220#show ssh-server host key
ssh-dss XXXXXXXXXX1kc3MAAAEBAPTB9YYdgvE+4bbhF4mtoIJri+ujdAIfgr4hL/0w7Jlvc50eXg
sXJoCqlPlsLRGHOOzxVYbOouPCUV/jPFCatgOIii8eJNzUqSB1e6MOFtGjmESrdYiafyIUhps+YWqd
TlIo0AFnVUKMqAbYODA3Cy7kNVptYRK8rcKWk1ChbatWnT/Z7RcmEVEou0qlOyp79b3DcpFM7ofa4d
9ySb6mj06Y/Ok8lL5qFhCHmGOGtqJTKZsqb5VnPz8FYC8t1s6/tpyrUa5aG2af/yTEa5U5BDYAuc88
wNIUG9alGo/8WIHiBJAm432o7UPqTHWO/5nYEQu44gmEPQrPGJ65GT8AAAAVAOpjE0Jyei+4c5qWSF
PXUgrLf5HAAABAQCnnPO+ZjWZcZwGa6LxTGMczAjDy5uwD4DWBbRxsPKaXlsicJGC0aridnTthIGa8
ARypDjhpL1a37SDezx8yClQ5vh+4SPLdS1hdSSzXXE+MXIICXnOVPdiKC4ia10n81tMxW/EPw4SqFP
77r7VvCE/JpXv82AN2JTJ/HAn3X7lvMyCsKZLoWrEcEcBH5anvAQKByVt7RerToZ4vSgodskv7nyXX
XXXXXXX

ssh-rsa XXXXXXXXXX1yc2EAAAABIwAAAQEAwvAZK18jKTCHIHQfRV4r7UOYChX0oeKjBbuuLSDhSH
WmhpG3xxJO0pDIedSF3Knb7LX2SfymQYJ7XYIqMjmU0oziv/zi+De/z3M7wJHQUwfMZEDAdR6Mx39w
6Q04/ehQcaszjXi+0Al2wG/kk56lAU23CW/i21o//5GZTzkFKyEJUtWauHWEW9glF5Yy7F64PesqoH
6h5oDNK7LhlT7s4QXRnUJphIlINrW278Dnvyry3liR+tgTJAq3cGHfYsaQCdankDilIQhUazUY0vJO
/gjYCjMuWH6Ek/cst+PCtgnt0XV5Bl079uRUmcACs2pDX5EWrwbPXXXXXXXXXX==
```

Show the key fingerprint of the public key.

```
SWX3220#show ssh-server host key fingerprint
ssh-dss
1024 MD5:XX:XX:a8:b9:51:93:9d:d2:ec:40:1a:43:66:3a:XX:XX
+---[DSA 1024]----+
|   .* .          |
|=*=+. o          |
|E+X+   o         |
| o . + = + .     |
|.. ..O X .       |
|oo=.B.*.o        |
|  o +   S o      |
|   . o           |
|    E            |
+------[MD5]------+
1024 SHA256:XXXXearwsCXvYTfIKrS6yYSrjMh0fW6W0Bw7aAOXXXX
+---[DSA 1024]----+
|  . +E.          |
|   o o           |
|    o X S        |
|   + = * .       |
|  o . B * .      |
|       + o .     |
|      * * +      |
|X+.@ +o=         |
|@*o.= o.         |
+----[SHA256]-----+

ssh-rsa
2048 MD5:XX:XX:b8:07:e3:5e:57:b8:80:e3:fc:b3:24:17:XX:XX
+---[RSA 2048]----+
|                 |
|...*             |
|*+.              |
|    .            |
|   .   +         |
|                 |
|        E        |
|     . B..       |
|      . oo       |
+------[MD5]------+
2048 SHA256:XXXXMkUuEbkJggPD68UoR+gobWPhgu7qqXzE8iUXXXX
+---[RSA 2048]----+
|*.==+            |
|*o+= . .         |
|*=o.  . S        |
|      * S . .    |
|     + B * o     |
| = = . . .       |
|    o            |
|     .           |
|. * *            |
+----[SHA256]-----+
```

4.21.8 Set SSH client alive checking

[Syntax]

ssh-server client alive enable [*interval* [*count*]]
ssh-server client alive disable
no ssh-server client alive

[Parameter]

interval	:	<1-2147483647>
		Client alive checking interval (seconds, if omitted: 100)
count	:	<1-2147483647>
		Maximum count for client alive checking (if omitted: 3)

[Initial value]

ssh-server client alive disable

[Input mode]

global configuration mode

[Description]

Sets whether to perform client alive checking.

A message requesting a response is sent to the client at intervals of the number of seconds specified by "interval". If there is no response for a successive number of times specified by "count", the connection with this client is cut and the session is ended.

If this command is executed with the "no" syntax, the setting returns to the default.

4.22 SSH client

4.22.1 Start SSH client

[Syntax]

ssh [*user@*] *host* [*port*]

[Parameter]

user	:	User name used when logging in to the remote host
host	:	Remote host name, IPv4 address (A.B.C.D), or IPv6 address (X:X::X:X) If you specify an IPv6 link local address, you must also specify the output interface (fe80::X%vlanN format)
port	:	<1-65535> Port number to use (if omitted: 22)

[Initial value]

none

[Input mode]

privileged EXEC mode

[Description]

Connects to the specified host via SSH.

If *user* is omitted, access the SSH server using the currently logged-in user name.

If *user* is omitted when logged in as an unnamed user, "root" is used.

[Note]

The escape character is the tilde (~). The escape character is recognized only if it is input at the beginning of the line.

If the escape character is input twice in succession at the beginning of the line, the escape character is used as input to the server.

If the escape character followed by a period (.) is input, the connection is forcibly closed.

If the escape character followed by a question mark (?) is input, a list of escape inputs is shown.

[Example]

To the host at IPv4 address 192.168.100.1, connect via SSH using user name "uname" and port number 12345.

```
SWX3220#ssh uname@192.168.100.1 12345
```

To the host at IPv6 address fe80::2a0:deff:fe11:2233, connect via SSH using user name "uname" and port number 12345.

```
SWX3220#ssh uname@fe80::2a0:deff:fe11:2233%vlan1 12345
```

4.22.2 Enable SSH client

[Syntax]

ssh-client *switch*
no ssh-client

[Parameter]

switch : Whether to enable SSH client

Setting value	Description
enable	Enable
disable	Disable

[Initial value]

ssh-client disable

[Input mode]

global configuration mode

[Description]

Enables use of the **ssh** command as an SSH client.

If this command is executed with the "no" syntax, the SSH client is disabled.

[Example]

Enable the SSH client.

```
SWX3220(config)#ssh-client enable
```

4.22.3 Clear SSH host information

[Syntax]

clear ssh host *host*

[Parameter]

host : Remote host name, IPv4 address (A.B.C.D), or IPv6 address (X:X::X:X)

[Input mode]

privileged EXEC mode

[Description]

Delete the public key of the SSH server that is connected as an SSH client.

[Example]

Clear the SSH host information.

```
SWX3220#clear ssh host 192.168.100.1
```

4.23 E-mail notification

4.23.1 SMTP e-mail server settings

[Syntax]

mail server smtp *id* **host** *host* [**port** *port*] [**encrypt** *method*] [**auth** *username password*]
no mail server smtp *id*

[Keyword]

port : Specifying a port number for the e-mail server

encrypt : Specifying an encryption method

auth : Specifying the account information to use for SMTP authentication

[Parameter]

id : <1-10>

Mail server ID

host : Mail server address or host name

IPv4 address (A.B.C.D), IPv6 address (X:X::X:X)

When specifying an IPv6 link local address, the transmitting interface also needs to be specified (in fe80::X%vlanN format).

Host name (64 characters or less, Single-byte alphanumeric characters - . and :)

port : <1-65535>

Port number for e-mail server (this is 25 when omitted, and 465 when over-ssl is specified as *method*)

method : Encryption method

Setting value	Description
over-ssl	Encrypting communication (over SSL)
starttls	Encrypting communication (STARTTLS)

username : User name used for SMTP authentication

(64 characters or less, ? " | > and aingle-byte alphanumeric characters and symbols other than spaces)

password : Passwords used for SMTP authentication

(64 characters or less,? " | > and aingle-byte alphanumeric characters and symbols other than spaces)

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Sets server information used when sending e-mails.

[Note]

When performing SMTP authentication, the AUTH LOGIN command is used for authentication.

For the SSL/TLS version, TLSv1, TLSv1.1 and TLSv1.2 are supported.

When setting an IPv6 address as the e-mail server address, encryption using SSL/TLS cannot be used.

[Example]

Sets the e-mail transmission server to “smtp-server-test.com”.

```
SWX3220(config)#mail server smtp 1 host smtp-server-test.com
```

Specify “smtp-server-test2.com” as the e-mail transmission server, and configures settings for using encryption and SMTP authentication.

```
SWX3220(config)#mail server smtp 1 host smtp-server-test2.com encrypt over-ssl auth
test_user test_password
```

4.23.2 SMTP e-mail server name settings

[Syntax]

mail server smtp *id* **name** *server_name*
no mail server smtp *id*

[Parameter]

id : <1-10>

E-mail server ID

server_name : Mail server name

(64 characters or less, single-byte alphanumeric characters and symbols other than ?)

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Sets the name of the server used when sending e-mails.

[Example]

Sets the e-mail transmission server name to “test_mail_server”.

```
SWX3220(config)#mail server smtp 1 name test_mail_server
```

4.23.3 E-mail notification trigger settings

[Syntax]

mail notify *temp-id* **trigger** lan-map [*type* [*type* ...]]
mail notify *temp-id* **trigger** terminal
mail notify *temp-id* **trigger** stack
no mail notify *temp-id* **trigger** lan-map
no mail notify *temp-id* **trigger** terminal
no mail notify *temp-id* **trigger** stack

[Keyword]

lan-map	:	Notify events related to the LAN map
terminal	:	Notify events related to the terminal monitoring function
stack	:	Notify events related to the stack function

[Parameter]

temp-id : <1-10>

E-mail template ID

Specify a template to use for event notification

type : Types of LAN map related events

Setting value	Description
hardware	Main unit abnormality
loop	Loop detection
sfp-power	SFP light reception level abnormality
queue-usage	Transmission queue monitoring
poe	PoE power supply
snapshot	Snapshot
l2ms	Duplication of L2MS managers

[Initial value]

None

[Input mode]

global configuration mode

[Description]

Configures the settings for e-mail notification of event information for the specified function.

If lan-map is specified and *type* is specified, you will only be notified of events related to the specified LAN map.

If *type* is omitted, you will be notified of all events related to LAN maps.

[Note]

Event notifications related to the stack function are only for models that support the stack function.

[Example]

Sets the LAN map error detection event trigger for e-mail template #1.

```
SWX3220(config)#mail notify 1 trigger lan-map
```

4.23.4 E-mail transmission template settings mode

[Syntax]

mail template *temp-id*
no template

[Parameter]

temp-id	:	<1-10> E-mail template ID

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Switches to the mode for setting the template used when sending e-mails.

The following items can be configured after switching to template mode. Up to 10 templates can be created.

- E-mail transmission destination address
- E-mail transmission source address
- Subject of e-mails sent
- Wait time settings for e-mail transmission (only event notification used)

[Example]

Switches to the mode for setting e-mail template #1.

```
SWX3220(config)#mail template 1
SWX3220(config-mail)#
```

4.23.5 E-mail transmission server ID settings

[Syntax]

send server *server-id*
no send server

[Parameter]

server-id	:	<1-10> E-mail template ID

[Initial value]

no send server

[Input mode]

E-mail template mode

[Description]

Sets the ID of the e-mail server to be used.

[Example]

Specifies server ID #1 for the e-mail server used in e-mail template #1.

```
SWX3220(config)#mail template 1
SWX3220(config-mail)#send server 1
```

4.23.6 E-mail transmission source address setting

[Syntax]

send from *address*
no send from *address*

[Parameter]

address	:	Source e-mail address

(256 characters or less, single-byte alphanumeric characters and _ - . @)

[Initial value]

no send from

[Input mode]

E-mail template mode

[Description]

Sets the source e-mail address.

[Example]

Specifies “sample@test.com” as the source e-mail address for e-mail template #1.

```
SWX3220(config)#mail template 1
SWX3220(config-mail)#send from sample@test.com
```

4.23.7 Destination e-mail address setting for e-mail transmission

[Syntax]

send to *address*
no send to

[Parameter]

address : Destination e-mail address

(256 characters or less, single-byte alphanumeric characters and _ - . @)

[Initial value]

no send to

[Input mode]

E-mail template mode

[Description]

Sets the destination e-mail addresses (maximum of four).

[Note]

This setting is used as the destination for event notifications, and is not used for the destinations when distributing certificates or sending notifications.

[Example]

Specifies “user@test.com” as the destination e-mail address for e-mail template #1.

```
SWX3220(config)#mail template 1
SWX3220(config-mail)#send to user@test.com
```

4.23.8 Setting for subject used when sending e-mails

[Syntax]

send subject *subject*
no send subject

[Parameter]

temp-id : Subject used when sending e-mails

(128 characters or less, single-byte alphanumeric characters and symbols other than the characters ? | >)

[Initial value]

no send subject

[Input mode]

E-mail template mode

[Description]

Specifies the subject for e-mails that are sent.

[Note]

The subject shown below will be used if this is not set.

- Event notification : Notification from SWX3220
- Certificate distribution : Certification publishment
- Certificate notification : Certification expiration

[Example]

Sets the subject to “TestMail” for e-mails sent using e-mail template #1.

```
SWX3220(config)#mail template 1
SWX3220(config-mail)#send subject TestMail
```

4.23.9 Wait time settings for e-mail transmission

[Syntax]

send notify wait-time *time*
no send notify wait-time

[Parameter]

time	:	<1-86400>
		Transmission wait time (seconds)

[Initial value]

send notify wait-time 30

[Input mode]

E-mail template mode

[Description]

Sets the wait time before actually sending event-related notification e-mails.

[Note]

This setting is used as the wait time before event-related notification e-mails are sent.

[Example]

Sets the transmission wait time for e-mail template #1 to 60 seconds.

```
SWX3220(config)#mail template 1
SWX3220(config-mail)#send notify wait-time 60
```

4.23.10 E-mail settings when sending certificates

[Syntax]

mail send certificate *temp-id*
no mail send certificate

[Parameter]

temp-id	:	<1-10>
		E-mail template ID

[Initial value]

no mail send certificate

[Input mode]

RADIUS configuration mode

[Description]

Specifies the template ID to use when sending RADIUS server client certificates.

The RADIUS server client certificate is sent to the e-mail address specified by the “user” command of the RADIUS server function.

[Note]

Example of e-mail body text used when sending RADIUS server client certificates
---
Certification is published.
Name : [Name] - Setting value for the NAME option in the “user” command
Account : [User name] - USERID value for the “user” command
MAC address : XX:XX:XX:XX:XX:XX
Expire : YYYY/MM/DD

[Example]

Specifies “#1” for the template ID to use when sending RADIUS server client certificates.

```
SWX3220(config-radius)#mail send certificate 1
```

4.23.11 E-mail settings for certificate notification

[Syntax]

mail send certificate-notify *temp-id*
no mail send certificate-notify

[Parameter]

temp-id : <1-10>
E-mail template ID

[Initial value]

no mail send certificate-notify

[Input mode]

RADIUS configuration mode

[Description]

Specifies the template to use when sending notifications of RADIUS server client certificates by e-mail.

[Note]

Example of e-mail body text used when sending notifications beforehand about expired term of validity for RADIUS server client certificates
---
Your certificate will expire in [X] days.
Name : [Name] - Setting value for the NAME option in the “user” command
Account : [User name] - USERID value for the “user” command
MAC address : XX:XX:XX:XX:XX:XX
Expire : YYYY/MM/DD

[Example]

Specifies “#2” for the template to use when sending notifications of RADIUS server client certificates by e-mail.

```
SWX3220(config-radius)#mail send certificate-notify 2
```

4.23.12 Notification timing settings for expired certificates

[Syntax]

mail certificate expire-notify *day* [*day*] [*day*]
no mail certificate expire-notify

[Parameter]

day : <1-90>
No. of days remaining for notification of expired term of validity

[Initial value]

mail certificate expire-notify 30

[Input mode]

RADIUS configuration mode

[Description]

Specifies the number of days to notify beforehand about expired term of validity for RADIUS server client certificates.

Up to three numbers of days for notifications can be specified.

[Note]

The *day* is displayed in descending order, regardless of the order in which it was inputted.

[Example]

Sets the number of days to notify beforehand about expired term of validity for RADIUS server client certificates to “50 days before” and “10 days before”.

```
SWX3220(config-radius)#mail certificate expire-notify 50 10
```

4.23.13 Show e-mail transmission information

[Syntax]

show mail information [*temp-id*]

[Parameter]

temp-id	:	<1-10> E-mail template ID

[Input mode]

privileged EXEC mode

[Description]

Shows e-mail transmission information for the specified template ID.

If the template ID is omitted, this displays all e-mail information.

[Example]

Shows e-mail information for e-mail template #1.

```
SWX3220#show mail information 1
 Template ID         : 1
 Notify trigger      : lan-map, terminal, stack
 LAN map notices     : hardware/loop/sfp-power/queue-usage/poe/snapshot/l2ms
 Server host         : smtp-server.com
 Server port         : 25
 Encryption          : STARTTLS
 Wait time           : 30 sec
 Mail address (from) : sample@test.com
 Mail address (to)   : user1@test.com
                       user2@test.com
                       user3@test.com
                       user4@test.com
```

4.24 LLDP

4.24.1 Enable LLDP function

[Syntax]

lldp run
no lldp run

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Enable the LLDP function for the entire system.

If this command is executed with the "no" syntax, disable the LLDP function for the entire system.

[Note]

In order to enable the LLDP function for a port, the following command must be set.

Set the **set lldp enable** command's *type* (LLDP agent mode) to "txrx", "txonly", or "rxonly" as necessary.

- **lldp run** (global configuration mode)
- **lldp-agent** (interface mode)
- **set lldp enable** *type* (LLDP agent mode)

[Example]

Enable LLDP function transmission and reception for LAN port #1.

```
SWX3220#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWX3220(config)#lldp run
SWX3220(config)#interface port1.1
SWX3220(config-if)#lldp-agent
SWX3220(lldp-agent)#set lldp enable txrx
```

4.24.2 Set system description

[Syntax]

lldp system-description *line*
no lldp system-description

[Parameter]

line	:	System description text string (255 characters or less)

[Initial value]

no lldp system-description

[Input mode]

global configuration mode

[Description]

Sets the system description used by the LLDP function.

If this command is executed with the "no" syntax, the setting returns to the default.

By default, this is "model name + firmware revision".

[Example]

Set the system description to SWITCH1_POINT_A.

```
SWX3220(config)#lldp system-description SWITCH1_POINT_A
```

4.24.3 Set system name

[Syntax]

lldp system-name *name*
no lldp system-name

[Parameter]

name	:	System name text string (255 characters or less)

[Initial value]

no lldp system-name

[Input mode]

global configuration mode

[Description]

Sets the system name used by the LLDP function.

If this command is executed with the "no" syntax, the setting returns to the default.

By default, this is "model name".

The specified value is set in "LLDP System Name TLV".

[Example]

Set the system name to SWITCH1.

```
SWX3220(config)#lldp system-name SWITCH1
```

4.24.4 Create LLDP agent

[Syntax]

lldp-agent
no lldp-agent

[Initial value]

none

[Input mode]

interface mode

[Description]

Create an LLDP agent, and transition to LLDP agent mode.

If this command is executed with the "no" syntax, delete the LLDP agent.

[Note]

When you delete the LLDP agent, the commands specified in LLDP agent mode are also deleted.

[Example]

Create an LLDP agent on port1.1, and transition to LLDP agent mode.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#lldp-agent
SWX3220(lldp-agent)#
```

4.24.5 Set automatic setting function by LLDP

[Syntax]

lldp auto-setting *switch*
no lldp auto-setting

[Parameter]

switch : Set automatic setting function by LLDP

Setting value	Description
enable	Enable automatic setting function by LLDP
disable	Disable automatic setting function by LLDP

[Initial value]

lldp auto-setting disable

[Input mode]

global configuration mode

[Description]

Enables the function by which LLDP frames transmitted by specific Yamaha devices can automatically modify the settings of a switch.

Also enables the notification function of the power supply stop timing for the **power-inline disable delay** command.

The following features are configured in LLDP frames.

- Flow control
- QoS
- IGMP snooping
- EEE
- RADIUS server host
- Terminal monitoring

If this command is executed with the "no" syntax, the setting returns to the default.

This can be set only for a physical interface.

[Note]

In order to use this function, you must use the **set lldp enable** command to enable reception of LLDP frames.

[Example]

Enable automatic setting function by LLDP.

```
SWX3220(config)#lldp auto-setting enable
```

4.24.6 Set LLDP transmission/reception mode

[Syntax]

set lldp enable *type*
set lldp disable
no set lldp enable

[Parameter]

type : Transmission/reception mode

Setting value	Description
rxonly	Set receive-only mode
txonly	Set transmit-only mode
txrx	Set transmit and receive

[Initial value]

set lldp disable

[Input mode]

LLDP agent mode

[Description]

Sets the LLDP frame transmission/reception mode for the applicable interface.

If you specify **set lldp disable**, LLDP frames are not transmitted or received.

If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

Set the LLDP transmission/reception mode of LAN port #1 to receive-only.

```
SWX3220(config)#lldp run
SWX3220(config)#interface port1.1
SWX3220(config-if)#lldp-agent
SWX3220(lldp-agent)#set lldp enable rxonly
```

4.24.7 Set type of management address

[Syntax]

set management-address-tlv *type*
no set management-address-tlv

[Parameter]

type : Type of management address

Setting value	Description
ip-address	Set IP address as the management address
mac-address	Set MAC address as the management address

[Initial value]

set management-address-tlv ip-address

[Input mode]

LLDP agent mode

[Description]

Sets the type of port management address used by LLDP.

If this command is executed with the "no" syntax, the setting returns to the default.

The specified value is set in "LLDP Management Address TLV".

[Example]

Set the MAC address as the type of management address for LAN port #1.

```
SWX3220(config)#lldp run
SWX3220(config)#interface port1.1
SWX3220(config-if)#lldp-agent
SWX3220(lldp-agent)#set management-address mac-address
```

4.24.8 Set basic management TLVs

[Syntax]

tlv-select basic-mgmt
no tlv-select basic-mgmt

[Initial value]

none

[Input mode]

LLDP agent mode

[Description]

Adds basic management TLVs to transmitted frames.

If this command is executed with the "no" syntax, exclude basic management TLVs from transmitted frames.

This command adds the following TLVs to LLDP frames.

<Basic management TLV>

(1) Port Description TLV : Description of port

(2) System Name TLV : Name of system

(3) System Description TLV : Description of system

(4) System Capabilities TLV : System capabilities

(5) Management Address TLV : Management address of port (MAC address or IP address)

[Example]

Add basic management TLVs to the LLDP frames that are transmitted on LAN port #1.

```
SWX3220(config)#lldp run
SWX3220(config)#interface port1.1
SWX3220(config-if)#lldp-agent
SWX3220(lldp-agent)#tlv-select basic-mgmt
```

4.24.9 Set IEEE-802.1 TLV

[Syntax]

tlv-select ieee-8021-org-specific
no tlv-select ieee-8021-org-specific

[Initial value]

none

[Input mode]

LLDP agent mode

[Description]

Adds IEEE-802.1 TLVs to transmitted frames.

If this command is executed with the "no" syntax, exclude IEEE-802.1 TLVs from transmitted frames.

This command adds the following TLVs to LLDP frames.

<IEEE-802.1 TLV>

(1) Port VLAN ID : ID of port VLAN

(2) Port and Protocol VLAN ID : ID of protocool VLAN

(3) Protocol Identity : List of supported protocols

(4) Link Aggregation : Link aggregation information

(5) VLAN Name : Name of port VLAN

[Example]

Add IEEE-802.1 TLVs to the LLDP frames that are transmitted on LAN port #1.

```
SWX3220(config)#lldp run
SWX3220(config)#interface port1.1
SWX3220(config-if)#lldp-agent
SWX3220(lldp-agent)#tlv-select ieee-8021-org-specific
```

4.24.10 Set IEEE-802.3 TLV

[Syntax]

tlv-select ieee-8023-org-specific
no tlv-select ieee-8023-org-specific

[Initial value]

none

[Input mode]

LLDP agent mode

[Description]

Adds IEEE-802.3 TLVs to transmitted frames.

If this command is executed with the "no" syntax, exclude IEEE-802.3 TLVs from transmitted frames.

This command adds the following TLVs to LLDP frames.

<IEEE-802.3 TLV>

(1) MAC/PHY Configuration/Status : Auto-negotiation support information

(2) Power Via MDI : PoE information (only for models with PoE function)

(3) Link Aggregation : Link aggregation information

(4) Maximum Frame Size : Maximum frame size

[Example]

Add IEEE-802.3 TLVs to the LLDP frames that are transmitted on LAN port #1.

```
SWX3220(config)#lldp run
SWX3220(config)#interface port1.1
SWX3220(config-if)#lldp-agent
SWX3220(lldp-agent)#tlv-select ieee-8023-org-specific
```

4.24.11 Set LLDP-MED TLV

[Syntax]

tlv-select med
no tlv-select med

[Initial value]

none

[Input mode]

LLDP agent mode

[Description]

If this command is executed with the "no" syntax, exclude LLDP-MED TLVs from transmitted frames.

This command adds the following TLVs to LLDP frames.

<LLDP-MED TLV>

(1) Media Capabilities : Type of LLDP-MED TLV transmitted

(2) Network Policy : Voice VLAN information (Only ports for which voice VLAN is specified)

(3) Extended Power-via-MDI : Extended PoE information (only for models with PoE function)

[Note]

Location Identification TLV is set to a value of "Location".

[Example]

Add LLDP-MED TLVs to the LLDP frames that are transmitted on LAN port #1.

```
SWX3220(config)#lldp run
SWX3220(config)#interface port1.1
SWX3220(config-if)#lldp-agent
SWX3220(lldp-agent)#tlv-select med
```

4.24.12 Set LLDP frame transmission interval

[Syntax]

set timer msg-tx-interval *tx_interval*
no set timer msg-tx-interval

[Parameter]

tx_interval : <5-3600>

LLDP frame transmission interval (seconds)

[Initial value]

set timer msg-tx-interval 30

[Input mode]

LLDP agent mode

[Description]

Sets LLDP frame transmission interval.

If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

Set 60 seconds as the LLDP frame transmission interval on LAN port #1.

```
SWX3220(config)#lldp run
SWX3220(config)#interface port1.1
SWX3220(config-if)#lldp-agent
SWX3220(lldp-agent)#set timer msg-tx-interval 60
```

4.24.13 Set LLDP frame transmission interval for high speed transmission period

[Syntax]

set timer msg-fast-tx *fast_tx*
no set timer msg-fast-tx

[Parameter]

fast_tx : <1-3600>

LLDP frame transmission interval for high speed transmission period (seconds)

[Initial value]

set timer msg-fast-tx 1

[Input mode]

LLDP agent mode

[Description]

Sets the LLDP frame transmission interval during the high speed transmission period.

If this command is executed with the "no" syntax, the setting returns to the default.

The high speed transmission period is the period immediately after a port's connected device was newly found, and LLDP frames are transmitted according to the following commands for making high speed transmission period settings.

- **set timerx msg-fast-tx** *fast_tx* : Sets the transmission interval (seconds) during the high speed transmission period.
- **set tx-fast-init** *value* : Sets the number of LLDP frames transmitted during the high speed transmission period.

[Example]

Set 2 seconds as the LLDP frame transmission interval during the high speed transmission period on LAN port #1.

```
SWX3220(config)#lldp run
SWX3220(config)#interface port1.1
SWX3220(config-if)#lldp-agent
SWX3220(lldp-agent)#set timer msg-fast-tx 2
```

4.24.14 Set time from LLDP frame transmission stop until re-initialization

[Syntax]

set timer reinit-delay *reinit_delay*
no set timer reinit-delay

[Parameter]

reinit_delay : <1-10>

Time from LLDP frame transmission stop until re-initialization (seconds)

[Initial value]

set timer reinit-delay 2

[Input mode]

LLDP agent mode

[Description]

Sets the time from when LLDP frame transmission stops until re-initialization occurs.

If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

Set 10 seconds as the time from when LLDP frame transmission stops on LAN port #1 until re-initialization occurs.

```
SWX3220(config)#lldp run
SWX3220(config)#interface port1.1
SWX3220(config-if)#lldp-agent
SWX3220(lldp-agent)#set timer reinit-delay 10
```

4.24.15 Set multiplier for calculating time to live (TTL) of device information

[Syntax]

set msg-tx-hold *value*
no set msg-tx-hold

[Parameter]

value : <1-100>

Multiplier for calculating the time to live (TTL) value of device information

[Initial value]

set msg-tx-hold 4

[Input mode]

LLDP agent mode

[Description]

Sets the multiplier for calculating the time to live (TTL) of device information.

If this command is executed with the "no" syntax, the setting returns to the default.

This setting is multiplied with the LLDP frame transmission interval (msg-tx-interval), and then increased by +1 to become the TTL value (seconds).

The TTL value is set in "Time To Live TLV".

TTL = msg-tx-interval x msg-tx-hold + 1 (seconds)

[Example]

Set 2 as the multiplier used to calculate the time to live (TTL) for device information on LAN port #1.

```
SWX3220(config)#lldp run
SWX3220(config)#interface port1.1
SWX3220(config-if)#lldp-agent
SWX3220(lldp-agent)#set msg-tx-hold 2
```

4.24.16 Set number of LLDP frames transmitted during the high speed transmission period

[Syntax]

set tx-fast-init *value*
no set tx-fast-init

[Parameter]

value : <1-8>

Number of LLDP frames transmitted during the high speed transmission period

[Initial value]

set tx-fast-init 4

[Input mode]

LLDP agent mode

[Description]

Sets the number of LLDP frames transmitted during the high speed transmission period.

If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

Set 2 as the number of LLDP frames transmitted during the high speed transmission period on LAN port #1.

```
SWX3220(config)#lldp run
SWX3220(config)#interface port1.1
SWX3220(config-if)#lldp-agent
SWX3220(lldp-agent)#set tx-fast-init 2
```

4.24.17 Set maximum number of connected devices manageable by a port

[Syntax]

set too-many-neighbors limit *max_value*
no set too-many-neighbors limit

[Parameter]

max_value : <1-1000>

Maximum number of connected devices manageable by a port

[Initial value]

set too-many-neighbors limit 5

[Input mode]

LLDP agent mode

[Description]

Sets the maximum number of connected devices that can be managed by a port.

If this command is executed with the "no" syntax, the setting returns to the default.

If the maximum number of connected device for a port is exceeded, LLDP frames sent from new devices are ignored.

[Note]

When this command is set, the remote device management table is cleared once when the first LLDP frame is received on the applicable port.

[Example]

Set 10 as the maximum number of connected devices that can be managed by a port on LAN port #1.

```
SWX3220(config)#lldp run
SWX3220(config)#interface port1.1
SWX3220(config-if)#lldp-agent
SWX3220(lldp-agent)#set too-many-neighbors limit 10
```

4.24.18 Global interface setting for LLDP function

[Syntax]

lldp interface enable *type*
lldp interface disable

[Keyword]

enable : Enable LLDP function

disable : Disable LLDP function

[Parameter]

type : Transmission/reception mode

Setting value	Description
rxonly	Set receive-only mode
txonly	Set transmit-only mode
txrx	Set transmit and receive

[Input mode]

global configuration mode

[Description]

Enables or disables the LLDP function for all LAN/SFP port in a single operation.

If this setting is enabled, set the transmission and reception mode of the specified LLDP frames.

[Note]

This command can be executed only for global configuration mode.

This command is for making the LLDP setting of each interface, and is not shown in running-config.

[Example]

Enable the LLDP function of all LAN/SFP port, and set a mode that allows transmission and reception of LLDP frames.

```
SWX3220(config)#lldp interface enable txrx
```

4.24.19 Show interface status

[Syntax]

show lldp interface *ifname* [neighbor]

[Keyword]

neighbor : Shows information for connected devices.

[Parameter]

ifname : Interface name of the LAN/SFP port

Interface to show

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows LLDP information for the interface specified by *ifname*.

If "neighbor" is specified, information for the device connected to the interface is shown.

The following items are shown.

For **show lldp interface** *ifname*

- Interface and its statistical information

Agent Mode	Bridge mode (fixed as nearest bridge)
Enable (tx/rx)	Transmission mode/Reception mode (Y:enable, N:disable)
Message fast transmit time	LLDP frame transmission interval for high speed transmission period (seconds)
Message transmission interval	LLDP frame transmission interval (seconds)
Reinitialisation delay	Time from LLDP frame transmission stop until re-initialization (seconds)
MED Enabled	LLDP-MED TLV transmission enable/disable
Device Type	Device type (fixed as NETWORK_CONNECTIVITY)
Total frames transmitted	Number of LLDP frames transmitted
Total entries aged	Number of devices not received for more than TTL seconds, and deleted from management table
Total frames received	Number of LLDP frames received
Total frames received in error	Number of LLDP frame reception errors
Total frames discarded	Number of LLDP frames discarded
Total discarded TLVs	Number of TLV discarded
Total unrecognised TLVs	Number of TLVs that could not be recognized

For **show lldp interface** *ifname* neighbor

- Basic management information

Interface Name	Received interface name
System Name	System name
System Description	System description
Port Description	Port description
System Capabilities	System capabilities
Interface Numbering	Type of interface number
Interface Number	Number of interface
OID Number	OID number
Management Address	MAC address os IP addresss

- Mandatory TLV information

CHASSIS ID TYPE	CHASSIS ID TLV type and value
PORT ID TYPE	PORT ID TLV type and value
TTL (Time To Live)	Time to maintain device information (seconds)

- 8021 ORIGIN SPECIFIC TLV information

Port Vlan id	ID of port VLAN
PP Vlan id	ID of protocol VLAN
VLAN ID	ID of port VLAN
VLAN Name	Name of port VLAN
Remote Protocols Advertised	List of supported protocols
Remote VID Usage Digestt	VID Usage Digestt value
Remote Management Vlan	Name of management VLAN
Link Aggregation Status	Link aggregation enabled/disabled
Link Aggregation Port ID	ID of link aggregation port

- 8023 ORIGIN SPECIFIC TLV information

AutoNego Support	Auto negotiation enabled/disabled
AutoNego Capability	Communication methods that can be auto-negotiate
Operational MAU Type	Communication speed and duplex mode
MDI power support	Whether PoE function is supported
PSE power pair	PSE power pair
Power class	PoE power supply class
Type/source/priority	PoE power supply type, source, and priority order
PD requested power value	Power requested by PD device (0.1 mW units)
PSE allocated power value	Power that can be supplied by PSE device (0.1 mW units)
Link Aggregation Status	Link aggregation enabled/disabled
Link Aggregation Port ID	ID of link aggregation port
Max Frame Size	Maximum frame size

- LLDP-MED TLV information (shown if LLDP-MED TLV is received)

MED Capabilities	LLDP-MED TLV type list
MED Capabilities Dev Type	LLDP-MED media device type
MED Application Type	Application type
MED Vlan id	ID of VLAN
MED Tag/Untag	VLAN tagged or untagged
MED L2 Priority	L2 priority order
MED DSCP Val	DSCP value priority order
MED Location Data Format	Format of location data
Latitude Res	Resolution of latitude (number of significant upper bits)
Latitude	Latitude (34 bits)
Longitude Res	Resolution of longitude (number of significant upper bits)
Longitude	Longitude (34 bits)
AT	Altitude type
	1: meter
	2: floor of building
Altitude Res	Resolution of altitude (number of significant upper bits)
Altitude	Altitude (30 bits)

Datum	Geodetic datum
	0: USA's World Geodetic System (WGS 84)
	1: North American Datum (NAD 83)
	2: Average historical minimum sea level of North American Datum (NAD 83)
LCI length	Length of location information data
What	Place of reference location
	0: Location of the DHCP server
	1: Position of the network element thought to be nearest the client
	2: Location of client
Country Code	Country code
CA type	CA (Civic Address) type
MED Inventory	Inventory information list

Refer to RFC 3825 for details on location information.

[Example]

Show LLDP information for LAN port #1.

```
SWX3220#show lldp interface port1.1
Agent Mode                    : Nearest bridge
Enable (tx/rx)                : Y/Y
Message fast transmit time    : 1
Message transmission interval : 30
Reinitialisation delay        : 2
MED Enabled                   : Y
Device Type                   : NETWORK_CONNECTIVITY
LLDP Agent traffic statistics
  Total frames transmitted       : 0
  Total entries aged             : 0
  Total frames received          : 0
  Total frames received in error : 0
  Total frames discarded         : 0
  Total discarded TLVs           : 0
  Total unrecognised TLVs        : 0
SWX3220#
```

4.24.20 Show information for connected devices of all interfaces

[Syntax]

show lldp neighbors

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows information for connected devices of all interfaces.

(For the display format, refer to the **show lldp interface** *ifname neighbor* command)

[Example]

Show information for connected devices.

```
SWX3220#show lldp neighbors
Interface Name            : port1.1
System Name               : SWX3220-16MT
System Description        : SWX3220 Rev.4.02.02 (Mon Dec 14 12:07:35 2020)
Port Description          : port1.3
System Capabilities       : L2 Switching
Interface Numbering       : 2
Interface Number          : 5003
OID Number                :
Management MAC Address    : ac44.f230.0000
```

```
Mandatory TLVs
  CHASSIS ID TYPE
    IP ADDRESS           : 0.0.0.0
  PORT ID TYPE
    INTERFACE NAME       : port1.3
  TTL (Time To Live)     : 41
8021 ORIGIN SPECIFIC TLVs
  Port Vlan id                : 1
  PP Vlan id                  : 0
  Remote VLANs Configured
    VLAN ID                   : 1
    VLAN Name                 : default
  Remote Protocols Advertised :
    Multiple Spanning Tree Protocol
  Remote VID Usage Digestt    : 0
  Remote Management Vlan      : 0
  Link Aggregation Status     :
  Link Aggregation Port ID    :
8023 ORIGIN SPECIFIC TLVs
  AutoNego Support            : Supported Enabled
  AutoNego Capability         : 27649
  Operational MAU Type        : 30
  Power via MDI Capability (raw data)
    MDI power support         : 0x0
    PSE power pair            : 0x0
    Power class               : 0x0
    Type/source/priority      : 0x0
    PD requested power value  : 0x0
    PSE allocated power value : 0x0
  Link Aggregation Status     :
  Link Aggregation Port ID    :
  Max Frame Size              : 1522
LLDP-MED TLVs
  MED Capabilities            :
    Capabilities
    Network Policy
  MED Capabilities Dev Type   : End Point Class-3
  MED Application Type        : Reserved
  MED Vlan id                 : 0
  MED Tag/Untag               : Untagged
  MED L2 Priority             : 0
  MED DSCP Val                : 0
  MED Location Data Format    : ECS ELIN
    Latitude Res      : 0
    Latitude          : 0
    Longitude Res     : 0
    Longitude         : 0
    AT                : 0
    Altitude Res      : 0
    Altitude          : 0
    Datum             : 0
    LCI length        : 0
    What              : 0
    Country Code      : 0
    CA type           : 0
  MED Inventory

SWX3220#
```

4.24.21 Clear LLDP frame counters

[Syntax]

clear lldp counters

[Input mode]

privileged EXEC mode

[Description]

Clear the LLDP frame counter of all ports.

[Example]

Clear the LLDP frame counter.

```
SWX3220>clear lldp counters
```

4.25 L2MS (Layer 2 management service) settings

4.25.1 Move to L2MS mode

[Syntax]

l2ms configuration

[Input mode]

global configuration mode

[Description]

Moves to L2MS mode in order to make L2MS settings.

[Note]

To return from L2MS mode to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

[Example]

Move to L2MS mode.

```
SWX3220(config)#l2ms configuration
SWX3220(config-l2ms)#
```

4.25.2 Set L2MS function

[Syntax]

l2ms enable
l2ms disable
no l2ms

[Keyword]

enable	:	Use the L2MS function
disable	:	Don't use the L2MS function

[Initial value]

l2ms enable

[Input mode]

L2MS mode

[Description]

Sets whether to use the L2MS function.

If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

Use the L2MS function.

```
SWX3220(config)#l2ms configuration
SWX3220(config-l2ms)#l2ms enable
```

4.25.3 Set role of L2MS function

[Syntax]

l2ms role *role*
no l2ms role

[Parameter]

role	:	Role of L2MS function

Setting value	Description
manager	Operate as an L2MS manager that sets and controls SWR series or SWX series units that are connected subordinate to it
agent	Be managed from a Yamaha device that is operating as an L2MS manager, such as a router, firewall, or SWX series unit that is set as the L2MS manager

[Initial value]

l2ms role agent

[Input mode]

L2MS mode

[Description]

Sets the role when using the L2MS function.

If this command is executed with the "no" syntax, operate as a agent.

[Note]

If the same network includes multiple Yamaha routers or firewalls on which L2MS (switch controller function) is enabled, or multiple SWX series units that are set to be L2MS managers, the L2MS function will not operate correctly.

Ensure that a single network has only one device that is the L2MS manager.

[Example]

Use the L2MS function as manager.

```
SWX3220(config)#l2ms configuration
SWX3220(config-l2ms)#l2ms enable
SWX3220(config-l2ms)#l2ms role manager
```

4.25.4 Set L2MS agent watch interval

[Syntax]

agent-watch interval *time*
no agent-watch interval

[Parameter]

time : <2-10>
Watch interval (seconds)

[Initial value]

agent-watch interval 3

[Input mode]

L2MS mode

[Description]

Specifies the time interval at which to transmit an L2MS agent query frame.

If this command is executed with the "no" syntax, the setting returns to the default.

If you set *time* to a high value, the query frame is transmitted less often, but it will take longer from when the L2MS agent is connected until the L2MS manager recognizes it. If you set *time* to a low value, the opposite will be the case; the query frame is transmitted more often, but it will take less time from when the L2MS agent is connected until the L2MS manager recognizes it.

[Note]

L2MS agent watch is performed only if L2MS is operating as manager.

[Example]

Set the watch interval to five seconds.

```
SWX3220(config)#l2ms configuration
SWX3220(config-l2ms)#l2ms enable
```

```
SWX3220(config-l2ms)#l2ms role manager
SWX3220(config-l2ms)#agent-watch interval 5
```

4.25.5 Set number of times that is interpreted as L2MS agent down

[Syntax]

agent-watch down-count *count*
no agent-watch down-count

[Parameter]

count	:	<2-10>
		Number of times that is interpreted as down

[Initial value]

agent-watch down-count 3

[Input mode]

L2MS mode

[Description]

Sets the number of query frames that are transmitted without receiving a response frame from the agent until it is determined that the L2MS agent is down.

If this command is executed with the "no" syntax, the setting returns to the default.

If the number of query frames specified by *count* have been transmitted without receiving a response frame from the agent, it is determined that the corresponding L2MS agent is down.

[Note]

If the port to which the L2MS agent is connected is in a link-down state, determining that the L2MS agent is down might take a shorter time than the setting of this command.

Agent watch is performed only if L2MS is operating as manager.

[Example]

Specify "8" as the count used to determine that the agent is down.

```
SWX3220(config)#l2ms configuration
SWX3220(config-l2ms)#l2ms enable
SWX3220(config-l2ms)#l2ms role manager
SWX3220(config-l2ms)#agent-watch down-count 8
```

4.25.6 Set terminal management function

[Syntax]

terminal-watch enable
terminal-watch disable
no terminal-watch

[Keyword]

enable	:	Enable terminal management function
disable	:	Disable terminal management function

[Initial value]

terminal-watch disable

[Input mode]

L2MS mode

[Description]

Enables the terminal management function. If this is enabled, information about the devices existing on the network is obtained at regular intervals.

If this command is executed with the "no" syntax, disable terminal management function.

[Note]

Terminal management is performed only if L2MS is operating as manager.

[Example]

Enable the terminal management function.

```
SWX3220(config)#l2ms configuration
SWX3220(config-l2ms)#l2ms enable
SWX3220(config-l2ms)#l2ms role manager
SWX3220(config-l2ms)#terminal-watch enable
```

4.25.7 Set the device information acquisition time interval

[Syntax]

terminal-watch interval *time*
no terminal-watch interval

[Parameter]

time	:	<1800-86400> Acquisition interval (seconds)

[Initial value]

terminal-watch interval 1800

[Input mode]

L2MS mode

[Description]

Specifies the time interval at which network device information is acquired. Information for the devices existing on the network is acquired when the time specified by *time* has elapsed.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

If the terminal management function is not enabled, terminal information is not acquired, regardless of the setting of this command.

[Example]

Set the watch interval to 3,600 seconds.

```
SWX3220(config)#l2ms configuration
SWX3220(config-l2ms)#l2ms enable
SWX3220(config-l2ms)#l2ms role manager
SWX3220(config-l2ms)#terminal-watch enable
SWX3220(config-l2ms)#terminal-watch interval 3600
```

4.25.8 Set L2MS control frame transmit/receive

[Syntax]

l2ms filter enable
l2ms filter disable
no l2ms filter

[Keyword]

enable	:	L2MS control frames cannot be transmitted or received
disable	:	L2MS control frames can be transmitted or received

[Initial value]

l2ms filter disable

[Input mode]

interface mode

[Description]

Prevents L2MS control frames from being transmitted or received.

If this command is executed with the "no" syntax, L2MS control frames can be transmitted and received.

[Note]

This command cannot be specified for the following interfaces.

- VLAN interface
- A physical interface inside a logical interface

A physical interface inside a logical interface operates according to the setting of this command on the interface inside which it exists. If the physical interface is inside the logical interface, the setting of the physical interface returns to the default.

Regardless of the setting of this command, L2MS control frames might not be transmitted or received if any of the following conditions exist.

- The interface is in the Blocking status due to STP or the loop detection function
- The **switchport trunk native vlan none** command has been specified
- It is inside a logical interface

[Example]

Prevent port1.5 from transmitting or receiving L2MS control frames.

```
SWX3220(config)#interface port1.5
SWX3220(config-if)#l2ms filter enable
```

4.25.9 Reset agent management

[Syntax]

l2ms reset

[Input mode]

privileged EXEC mode

[Description]

Removes all L2MS agents managed by the L2MS manager from management, and searches for L2MS agents once again.

[Note]

This can be executed only if L2MS is operating as manager.

When this command is executed, L2MS agents that were being managed also remove themselves from the state of being managed by the L2MS manager.

After this command is executed, the timing at which L2MS agent watching resumes will depend on the time specified by the **agent-watch interval** command.

[Example]

Reset L2MS agent management.

```
SWX3220#l2ms reset
```

4.25.10 Show L2MS information

[Syntax]

show l2ms [detail]

[Keyword]

detail	:	Also show detailed information

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the following information according to the L2MS operating state.

- If L2MS is operating as manager
  - Number of L2MS agents being managed
  - Information for the L2MS agents being managed
    - MAC address
    - Model name
    - Device name
    - Route
    - Uplink port
    - Settings applied

- If L2MS is operating as manager and "detail" is specified
  - L2MS manager information
    - Number of terminals connected to the L2MS manager
    - Information of terminals connected to the L2MS manager
      - MAC address
      - Ports connected
      - Time at which terminal was discovered
  - Number of L2MS agents being managed
  - Information for the L2MS agents being managed
    - MAC address
    - Model name
    - Device name
    - Route
    - Linked-up ports
    - Uplink port
    - Downlink port
    - Settings applied
    - Number of terminals connected to the L2MS agent
    - Information of terminals connected to the L2MS agent (in the case of a switch)
      - MAC address
      - Ports connected
      - Time at which terminal was discovered
    - Information of terminals connected to the L2MS agent (in the case of an AP)
      - SSID connected
      - Frequency connected
      - Time at which terminal was discovered
- If L2MS is operating as agent
  - Whether managed by the L2MS manager
  - MAC address of L2MS manager (if managed)

[Note]

Information is not shown if L2MS is not operating.

Specifying "detail" is valid only if L2MS is operating as manager.

[Example]

If L2Ms is operating as manager, show detailed L2MS information.

```
SWX3220>show l2ms detail
Role : Manager

[Manager]
 Number of Terminals   : 0

[Agent]
 Number of Agents      : 2
  [ac44.f230.00a5]
   Model name          : SWX2100-24G
   Device name         : SWX2100-24G_Z5301050WX
   Route               : port2.1
   LinkUp              : 1, 3, 9
     Uplink            : 1
     Downlink          : 3
   Config              : None
   Appear time         : Tue Mar 13 18:43:18 2018
   Number of Terminals : 1
    [bcae.c5a4.7fb3]
     Port              : 9
     Appear time       : Wed Mar 14 14:01:18 2018

  [00a0.deae.b8bf]
   Model name          : SWX2300-24G
   Device name         : SWX2300-24G_S4L000401
   Route               : port2.1-3
   LinkUp              : 1
```

```
    Uplink             : 1
    Downlink           : None
  Config               : None
  Appear time          : Tue Mar 13 18:43:18 2018
  Number of Terminals  : 0
```

4.25.11 Show L2MS agent config information

[Syntax]

show l2ms agent-config [*agent*]

[Parameter]

agent : MAC address (HHHH.HHHH.HHHH) or route (portD.D-D.D)

Specify the MAC address or route of the applicable L2MS agent terminal. If omitted, this applies to all L2MS agent terminals.

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Show the config information of the L2MS agent terminal (SWX2200).

The following content is shown.

Item	Description
system-name name	Set name of device
energy-saving mode	Set whether to use the energy-saving mode
led-brightness mode	Adjust LED brightness
port-speed port speed	Set port communication speed and operating mode
port-use port mode	Set whether to use the port
port-auto-crossover port mode	Set whether to use the auto crossover function
port-speed-downshift port mode	Set whether to use the speed downshift function
port-flow-control port mode	Set whether to use flow control
vlan-id vlan_register_num vid	Set VLAN ID
vlan-port-mode port mode	Set the port's VLAN operation mode
vlan-access port vlan_register_num	Set access port
vlan-trunk port vlan_register_num mode	Set trunk port
vlan-multiple-use mode	Set whether to use multiple VLAN
vlan-multiple port group_num mode	Set multiple VLAN group
qos-dscp-remark-type port type	Set DSCP remarking method
qos-dscp-remark-class port class	Set class categorization of received packets
qos-speed-unit unit	Set speed unit when performing bandwidth control
qos-policing-use port mode	Set whether to perform policing of reception traffic
qos-policing-speed port level	Set bandwidth of reception traffic
qos-shaping-use port mode	Set whether to perform shaping of transmission traffic
qos-shaping-speed port level	Set bandwidth of transmission traffic
mirroring-use mode	Set whether to use the mirroring function
mirroring-dest port	Set port that transmits mirroring packets
mirroring-src-rx port mode	Set whether received packets are mirrored
mirroring-src-tx port mode	Set whether transmitted packets are mirrored

Item	Description
counter-frame-rx-type port counter type	Set type of frames counted by reception frame counter
counter-frame-tx-type port counter type	Set type of frames counted by transmission frame counter
loopdetect-count count	Set threshold value per second at which to determine that a loop has occurred
loopdetect-linkdown action	Set operation when loop occurs
loopdetect-recovery-timer time	Set time until recovery after a port's link goes down
loopdetect-port-use port mode	Set whether to use the loop detection function
poe-class port class	Set upper limit for class of power supplied from each port

[Example]

Show the config information of all L2MS agent terminals.

```
SWX3220>show l2ms agent-config

[port1.23-1.23-8]
 system-name TEST3_SWX2200-8G
 vlan-id 2 2
 vlan-id 3 3
 vlan-port-mode 1 hybrid
 vlan-access 5 2
 vlan-access 6 3
 vlan-trunk 1 2 join
 vlan-trunk 1 3 join

[00a0.de00.0001]
 system-name TEST2_SWX2200-8G
 vlan-id 2 2
 vlan-id 3 3
 vlan-port-mode 1 hybrid
 vlan-port-mode 8 hybrid
 vlan-trunk 1 2 join
 vlan-trunk 1 3 join
 vlan-trunk 8 2 join
 vlan-trunk 8 3 join

[00a0.de00.0002]
 system-name TEST1_SWX2200-24G
 port-speed 7 100-hdx
 port-auto-crossover 7 off
 port-speed-downshift 7 off
 port-flow-control 7 on
 vlan-id 2 2
 vlan-id 3 3
 vlan-port-mode 1 hybrid
 vlan-port-mode 23 hybrid
 vlan-trunk 1 2 join
 vlan-trunk 1 3 join
 vlan-trunk 23 2 join
 vlan-trunk 23 3 join
 loopdetect-count 5
 loopdetect-linkdown linkdown-recovery
 loopdetect-recovery-timer 600
 loopdetect-port-use 7 off
```

Show the config information of the L2MS agent terminal whose MAC address is 00a0.de00.0001.

```
SWX3220>show l2ms agent-config 00a0.de00.0001

[00a0.de00.0001]
 system-name TEST2_SWX2200-8G
 vlan-id 2 2
 vlan-id 3 3
 vlan-port-mode 1 hybrid
 vlan-port-mode 8 hybrid
 vlan-trunk 1 2 join
 vlan-trunk 1 3 join
 vlan-trunk 8 2 join
 vlan-trunk 8 3 join
```

Show the config information of the L2MS agent terminal whose route is 1.23-1.23-8.

```
SWX3220>show l2ms agent-config port1.23-1.23-8

[port1.23-1.23-8]
 system-name TEST3_SWX2200-8G
 vlan-id 2 2
 vlan-id 3 3
 vlan-port-mode 1 hybrid
 vlan-access 5 2
 vlan-access 6 3
 vlan-trunk 1 2 join
 vlan-trunk 1 3 join
```

4.25.12 Set the device information acquisition time interval for downstream of a wireless AP

[Syntax]

wireless-terminal-watch interval *time*
no wireless-terminal-watch interval

[Parameter]

time	:	<10-86400>
		Acquisition interval (seconds)

[Initial value]

wireless-terminal-watch interval 60

[Input mode]

L2MS mode

[Description]

Specifies the time interval at which device information for a device downstream of a wireless AP is acquired. Information for the devices existing downstream the wireless AP is acquired when the time specified by *time* has elapsed.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

If device watch is not operating, device information is not acquired, regardless of the setting of this function.

[Example]

Set the device information acquisition time interval to 3,600 seconds.

```
SWX3220(config)#l2ms configuration
SWX3220(config-l2ms)#l2ms enable
SWX3220(config-l2ms)#l2ms role manager
SWX3220(config-l2ms)#terminal-watch enable
SWX3220(config-l2ms)#wireless-terminal-watch interval 3600
```

4.25.13 Set event monitoring function

[Syntax]

event-watch enable
event-watch disable
no event-watch

[Keyword]

enable	:	Enable the event monitoring function
disable	:	Disable the event monitoring function

[Initial value]

event-watch enable

[Input mode]

L2MS mode

[Description]

Sets whether to disable or enable the event monitoring function. If enabled, event information for the L2MS agents existing on the network is acquired at regular intervals.

If this command is executed with the "no" syntax, the event monitoring function is enabled.

[Note]

Event monitoring is performed only if L2MS is operating as manager.

[Example]

Disable the event monitoring function.

```
SWX3220(config)#l2ms configuration
SWX3220(config-l2ms)#l2ms enable
SWX3220(config-l2ms)#l2ms role manager
SWX3220(config-l2ms)#event-watch disable
```

4.25.14 Set event information acquisition time interval

[Syntax]

event-watch interval *time*
no event-watch interval

[Parameter]

time	:	<60-1800> Acquisition time interval (seconds)

[Initial value]

event-watch interval 300

[Input mode]

L2MS mode

[Description]

Sets the time interval at which event information is acquired from L2MS agents existing on the network. When the time specified by *time* elapses, event information is acquired from L2MS agents existing on the network

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

If the event monitoring function is not enabled, event information is not acquired, regardless of the setting of this command.

[Example]

Set the monitoring time interval to 60 seconds.

```
SWX3220(config)#l2ms configuration
SWX3220(config-l2ms)#l2ms enable
SWX3220(config-l2ms)#l2ms role manager
SWX3220(config-l2ms)#event-watch interval 60
```

4.25.15 Set whether to use the L2MS agent's zero config function

[Syntax]

config-auto-set enable
config-auto-set disable
no config-auto-set

[Keyword]

enable	:	Use the L2MS agent's zero config function
disable	:	Don't use the L2MS agent's zero config function

[Initial value]

config-auto-set enable

[Input mode]

L2MS mode

[Description]

Sets whether to use the L2MS agent device's zero config function.

If the zero config function is enabled, and the L2MS agent's Yamaha switch or wireless AP settings (config) are saved, the saved settings (config) are automatically applied when the L2MS agent in its factory-set state is connected to the network.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

Synchronization of settings for a agent SWX2200 is performed regardless of this setting.

[Example]

Use the L2MS agent's zero config function.

```
SWX3220(config)#l2ms configuration
SWX3220(config-l2ms)#l2ms enable
SWX3220(config-l2ms)#l2ms role manager
SWX3220(config-l2ms)#config-auto-set enable
```

4.26 Snapshot

4.26.1 Set snapshot function

[Syntax]

snapshot enable
snapshot disable
no snapshot

[Keyword]

enable	:	Snapshot function is enabled
disable	:	Snapshot function is disable

[Initial value]

snapshot disable

[Input mode]

global configuration mode

[Description]

Enables the snapshot function.

If this command is executed with the "no" syntax, disables the snapshot function.

[Note]

This command is valid only if L2MS is operating as manager.

[Example]

Enable the snapshot function.

```
SWX3220(config)#snapshot enable
```

4.26.2 Set whether to include terminals in the snapshot comparison

[Syntax]

snapshot trap terminal [except-wireless]
no snapshot trap terminal

[Keyword]

except-wireless	:	Information for wirelessly connected terminals is excluded from the snapshot comparison.

[Initial value]

no snapshot trap terminal

[Input mode]

global configuration mode

[Description]

Terminal information is included in the snapshot comparison.

If the except-wireless option is specified, information for terminals that are wirelessly connected below a wireless access point are excluded from the snapshot comparison.

If this command is executed with the "no" syntax, terminal information is excluded from the snapshot comparison.

[Note]

This command is valid only when operating as the manager and the **terminal-watch enable** command and **snapshot enable** command have also been set.

[Example]

Include terminal information in the snapshot comparison.

```
SWX3220(config)#snapshot trap terminal
```

4.26.3 Create snapshot

[Syntax]

snapshot save [after-update]

[Keyword]

after-update	:	After updating the network's connection state, save it as a snapshot

[Input mode]

privileged EXEC mode

[Description]

Saves a snapshot file that is the base for the LAN map's snapshot function.

If the after-update option is not included, the network connection state currently maintained by the manager is saved as the snapshot file.

If the after-update option is included, the network connection state information is updated to the latest information, and then saved as the snapshot file.

[Note]

If the after-update option is included, the network connection state information is updated to the latest information, but depending on the configuration of the network, it might take some time for this update to be completed.

[Example]

After updating the network's connection state, save the snapshot file.

```
SWX3220#snapshot save after-update
```

4.26.4 Delete snapshot

[Syntax]

snapshot delete

[Input mode]

privileged EXEC mode

[Description]

Deletes the snapshot file.

[Example]

Delete the snapshot file.

```
SWX3220#snapshot delete
```

4.27 Firmware update

4.27.1 Set firmware update site

[Syntax]

firmware-update url *url*
no firmware-update url

[Parameter]

url : Single-byte alphanumeric characters and single-byte symbols (255 characters or less)

URL at which the firmware is located

[Initial value]

Model	Initial value
SWX3220-16MT, SWX3220-16TMs	firmware-update url http://www.rtpro.yamaha.co.jp/firmware/revision-up/swx3220.bin
SWX3220-30MC	firmware-update url http://www.rtpro.yamaha.co.jp/firmware/revision-up/swx3220-30mc.bin
SWX3220-30TCs	firmware-update url http://www.rtpro.yamaha.co.jp/firmware/revision-up/swx3220-30tcs.bin

[Input mode]

global configuration mode

[Description]

Specify the download source URL used when updating the firmware from a firmware file located on a web server.

The input syntax is "http://server IP address or hostname/pathname".

IPv6 addresses must be enclosed in "[]", as shown here: "[IPv6 address]".

When specifying an IPv6 link-local address, the sending interface must also be specified (fe80::X%vlanN syntax).

If the server's port number is other than 80, you must specify this within the URL, using the syntax "http://server IP address or hostname:port number/path name".

[Example]

Specify http://192.168.100.1/swx3220.bin as the firmware download URL.

```
SWX3220(config)#firmware-update url http://192.168.100.1/swx3220.bin
```

4.27.2 Configure the HTTP proxy server used for firmware updates

[Syntax]

firmware-update http-proxy *server port*
no firmware-update http-proxy

[Parameter]

server : A.B.C.D

IPv4 address of the HTTP proxy server

server : [X:X::X:X]

IPv6 address of the HTTP proxy server

Must be enclosed in "[]", as shown here: "[X:X::X:X]"

When specifying an IPv6 link-local address, the sending interface must also be specified (fe80::X%vlanN syntax).

: Alphanumeric characters and symbols (up to 255 characters)

The HTTP proxy server FQDN

port : <1-65535>

The HTTP proxy server listening port number

[Initial value]

no firmware-update http-proxy

[Input mode]

global configuration mode

[Description]

Configure the HTTP proxy server used when updating firmware using a firmware file located on the web server.

If no HTTP proxy server is configured, the firmware update will be performed without going through the HTTP proxy server.

The port number must also be explicitly configured.

If this command is executed with the "no" syntax, the HTTP proxy server setting is cleared.

[Example]

Set the HTTP proxy server to 192.168.100.1 (port number 8080).

```
SWX3220(config)#firmware-update http-proxy 192.168.100.1 8080
SWX3220(config)#
```

4.27.3 Execute firmware update

[Syntax]

firmware-update execute [no-confirm] [no-reboot]

[Keyword]

no-confirm	:	Don't confirm the firmware update
no-reboot	:	Does not reboot after updating firmware

[Input mode]

privileged EXEC mode

[Description]

Compares the firmware file located on the web server with the revision of the currently-running firmware, and executes the update if rewriting is possible.

If firmware of a revision that can be rewritten exists, you will be asked for confirmation; enter "y" if you want to update, or enter "n" if you don't want to update.

If you specify "no-confirm," the update is executed without asking you for confirmation.

When no-reboot is specified, the system does not reboot after performing a revision update. It will boot with the updated firmware on the next boot.

[Note]

You can use the **firmware-update url** command to change the download source URL.

If you execute the **firmware-update revision-down enable** command, it will be possible to downgrade to an older revision.

When no-reboot is specified, the system will not reboot at the specified time, even if the **firmware-update revision-time** command is configured.

[Example]

Update the firmware using a firmware file located on a web server.

```
SWX3220#firmware-update execute
Found the new revision firmware
Current Revision: Rev.4.02.01
New Revision:     Rev.4.02.03
Downloading...
Update to this firmware? (y/n)y
Updating...
Finish
SWX3220#
```

4.27.4 Set firmware download timeout duration

[Syntax]

firmware-update timeout *time*
no firmware-update timeout

[Parameter]

time	:	<100-86400>
		Timeout time (seconds)

[Initial value]

firmware-update timeout 300

[Input mode]

global configuration mode

[Description]

Specifies the timeout duration when downloading firmware from a web server.

If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

Set the firmware download timeout duration to 120 seconds.

```
SWX3220(config)#firmware-update timeout 120
SWX3220(config)#
```

4.27.5 Allow revision-down

[Syntax]

firmware-update revision-down enable
no firmware-update revision-down

[Initial value]

no firmware-update revision-down

[Input mode]

global configuration mode

[Description]

When using a firmware file from a web server to update the firmware, this allows the firmware to be changed to a revision that is older than the current revision.

If this is executed with the "no" syntax, revision-down is not allowed.

[Example]

Allow revision-down.

```
SWX3220(config)#firmware-update revision-down enable
SWX3220(config)#
```

4.27.6 Show firmware update function settings

[Syntax]

show firmware-update

[Input mode]

privileged EXEC mode

[Description]

Shows the current settings of the firmware update function.

The following items are shown.

- Download source URL
- Proxy server URL
- Download timeout duration
- Permit revision-down
- Firmware revision on next boot
- Reboot time after update
- Reboot method in stack configuration

[Example]

Shows the setting state of the firmware update function.

```
SWX3220#show firmware-update
url: http://www.rtpro.yamaha.co.jp/firmware/revision-up/swx3220.bin
http-proxy: -
timeout: 300 (seconds)
revision-down: Disable
firmware revision for next boot: -
reload-time: -
reload-method: Normal
SWX3220#
```

4.27.7 Update firmware from SD card

[Syntax]

firmware-update sd execute [no-confirm] [no-reboot] [sd-unmount]

[Keyword]

no-confirm	:	Don't check for firmware update and SD card mount continuity
no-reboot	:	Does not reboot after updating firmware
sd-unmount	:	Unmount the SD card without checking before firmware update

[Input mode]

privileged EXEC mode

[Description]

Execute firmware update using a firmware file stored on the SD card.

If the parameter is not specified, and rewritable firmware exists on the SD card, you will be asked whether to update and maintain the mounted state of the SD card.

If you want to update the firmware, enter "y"; if you don't want to update, enter "n".

If you want to maintain the mounted state of the SD card, enter "y"; if you want to unmount, enter "n".

If you specify no-confirm, the mounted state of the SD card is maintained and the firmware is updated without asking for confirmation.

When no-reboot is specified, the system does not reboot after performing a revision update. It will boot with the updated firmware on the next boot.

If you specify sd-unmount, the SD card is unmounted without asking for confirmation.

[Note]

The firmware file references the "/swx3220/firmware/swx3220.bin" file on the SD card.

A revision check is not performed for the firmware file in the SD card and the currently-running firmware.

If you do not remove the SD card, the unit starts up the next time using the firmware that is in the SD card as specified by the **boot prioritize sd** command.

The firmware update continues even if you unmount and remove the SD card.

When no-reboot is specified, the system will not reboot at the specified time, even if the **firmware-update revision-time** command is configured.

[Example]

Update the firmware using the firmware file on the SD card.

```
SWX3220#firmware-update sd execute
Update the firmware.
Current Revision: Rev.4.02.01
New Revision:     Rev.4.02.03

Update to this firmware? (y/n)y
Continue without unmounting the SD card? (y/n)n
Unmounted the SD card.  Pull out the SD card.
Updating...
Finish
SWX3220#
```

4.27.8 Set firmware update reload time

[Syntax]

firmware-update reload-time *hour* [*min*]
no firmware-update reload-time

[Parameter]

hour	:	<0-23>
		Firmware update reload time (hour)
min	:	<0-59>
		Firmware update reload time (minutes)

[Input mode]

global configuration mode

[Description]

Sets the time at which the new firmware is applied by restarting after a firmware update.

If this command is executed with the "no" syntax, the new firmware is applied by restarting immediately after the firmware is updated.

[Example]

Specify AM 1:30 as the restart time for updating the firmware.

```
SWX3220(config)#firmware-update reload-time 1 30
SWX3220(config)#
```

4.27.9 Set reload method for firmware update of stack configuration

[Syntax]

firmware-update reload-method *method*
no firmware-update reload-method

[Parameter]

method : Reload method for firmware update of stack configuration

Setting value	Description
normal	Reload main switch and member switches simultaneously
sequential	Reload main switch and member switches sequentially

[Initial value]

firmware-update reload-method normal

[Input mode]

global configuration mode

[Description]

Sets the method of restarting after a firmware update when using a stack configuration.

"normal" restarts the main switch and member switches simultaneously. With the "sequential" setting, the main switch finishes restarting, and then the member switches are restarted, thereby applying the new firmware in a way that does not affect the currently-operating network service.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be specified only when the stack function is enabled.

[Example]

Specify sequential as the restart method of updating the firmware.

```
SWX3220(config)#firmware-update reload-method sequential
SWX3220(config)#
```

4.28 Stack

4.28.1 Set stack function

[Syntax]

stack *switch*
no stack

[Parameter]

switch : Operation of the stack function

Setting value	Description
enable	Enable stack function
disable	Disable stack function

[Initial value]

stack disable

[Input mode]

global configuration mode

[Description]

Enables or disables the stack function.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be executed only for models that support stacking.

If the unit started up using the config saved on the SD card, and the SD card is subsequently unmounted, executing this command produces an error.

[Example]

Enable stack function.

```
SWX3220(config)#stack enable
```

Disable stack function.

```
SWX3220(config)#stack disable
```

4.28.2 Changing the stack ID

[Syntax]

stack *stack_id* **renumber** *new_stack_id*

[Parameter]

stack_id : <1-2>

Stack ID of the member switch to be changed. An error will occur if the specified ID does not exist

new_stack_id : <1-2>

Stack ID after change

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Changes the stack ID of the specified member switch.

[Note]

This command can be executed only for models that support stacking.

This command can be executed only if the stack function is disabled.

Only your own stack ID can be changed.

If the unit started up using the config saved on the SD card, and the SD card is subsequently unmounted, executing this command produces an error.

[Example]

Change the member switch with stack ID:1 to ID:2.

```
SWX3220(config)#stack 1 renumber 2
```

4.28.3 Show stack information

[Syntax]

show stack

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows stack-related settings and status information.

The following content is shown.

- Set stack function (Stack)
- The unit's own stack ID [set value] (Configured ID)
- The unit's own stack ID [operating value] (Running ID)
- The unit's own status (Status)
- Range of IP addresses used by the unit's own stack port (Subnet on stack port)
- MAC Address during stacking(Virtual MAC-Address)
- Information for each member switch
  - Stack ID [operating value] (ID)
  - Model name (Model)
  - Status (Status)
  - Role (Role)
  - Serial Number(Serial)
  - Physical Address(MAC-Address)
  - Device ID(Device ID)
- Information for each stack port
  - Interface Number (Interface)
  - Status (Status)

The status (Status) of each member switch displays one of the following.

Status	Explanation
Setting	Status for carrying out necessary settings to configure stacks between member switches.
Active	Status when stacks are configured between member switches.
Inacive	Status when a fault has occurred on a stacked switch, where this switch is separated from the virtualized switch.
Standalone	Although the stack functions for this switch are enabled, negotiation cannot be made with the member switches, and this switch is thus operating on its own. Indicates that a stack has not been configured once since booting.
Standalone(separated)	Although the stack functions for this switch are enabled, negotiation cannot be made with the member switches, and this switch is thus operating on its own. Indicates that a stack has been configured since booting.
Disable	Status when stack functions are disabled.

[Note]

This command can be executed only for models that support stacking.

[Example]

Show stack information.

```
SWX3220#show stack
Stack: Enable

Configured ID        : 1
Running ID           : 1
Status               : Active
Subnet on stack port : Auto-ip
Virtual MAC-Address  : 00a0.de00.0000
```

```
ID  Model          Status      Role     Serial       MAC-Address
                                        Device ID
----------------------------------------------------------------------
1   SWX3220-16MT   Active      Main     S000000000   00a0.de00.0000
                                        0000000-0000000-0000000-00000

2   SWX3220-16MT   Active      Member   S000000001   00a0.de00.0001
                                        0000000-0000000-0000000-00001

Interface    Status
----------------------------------------------------------------------
port1.15     up
port1.16     up
port2.15     up
port2.16     up
```

4.28.4 Set range of IP addresses used by the stack port

[Syntax]

stack subnet *NETWORK_ADDR*
stack subnet auto-ip
no stack subnet

[Parameter]

NETWORK_ADDR : A.B.C.D

IP address space (A.B.C.0)

[Initial value]

stack subnet auto-ip

[Input mode]

global configuration mode

[Description]

This command can be executed only for models that support stacking.

This command specifies the IP address space used between stacked devices.

The fixed subnet 255.255.255.0 is applied to NETWORK_ADDR. In the case of auto-ip, the Auto IP function is used between the stacked devices.

If this command is executed with the "no" syntax, the setting returns to the default.

The IP address space specified by this command cannot be used by ports other than the stack port.

A restart is required in order to apply the settings of this command to operation.

The IP address spaces of the stacked devices must be set to the same parameters. If different parameters are specified, communication cannot occur correctly between the stacked devices.

[Example]

Set "192.168.101.0" as the IP address range of the stack port.

```
SWX3220(config)#stack subnet 192.168.101.0
```

4.28.5 Remote login to a member switch

[Syntax]

remote-login *stack_id*

[Parameter]

stack_id : <1-2>

Stack ID

[Initial value]

none

[Input mode]

privileged EXEC mode

[Description]

Remotely log in to a specified member switch from the main switch in a stack configuration.

When remote login succeeds, the stack ID is automatically shown added to the prompt.

[Example]

Remotely log in to a member switch (ID:2) from the main switch.

```
SWX3220#remote-login 2

...

SWX3220-2>
```

4.29 Schedule

4.29.1 Schedule settings

[Syntax]

schedule *id* **time** *date time template_id*
schedule *id* **event** *event template_id*
no schedule *id*

[Parameter]

id : <1-10>

Schedule number

date : <1-12> or * / <1-12> or sun, mon, ... , sat or *

Month/day

Month setting examples	Setting contents
1	January
1.2	January and February
2-	From February to December
2-7	From February to July
-7	From January to July
*	Monthly

Day setting examples	Setting contents
1	One day
1.2	The 1st and the 2nd
2-	From the 2nd to the 12th
2-7	From the 2nd to the 7th
-7	From the 1st to the 7th
mon	Monday
sat,sun	Saturday and Sunday
mon-fri	From Monday to Friday
-fri	From Sunday to Friday
*	Daily

time : <0-23> or * : <0-59> or * : <0-59>

h:m:s (the seconds can be omitted)

Hour setting examples	Setting contents
12	12:00
12.13	12:00 and 13:00
12-	From 12:00 to 23:00
10-20	From 10:00 to 20:00
-20	From 0:00 to 20:00
*	Hourly

Minute setting examples	Setting contents
30	30 minutes
15.45	15 minutes and 45 minutes
30-	From 30 minutes to 59 minutes
15-45	From 15 minutes to 45 minutes
-45	From 0 minutes to 45 minutes
*	Each minute

event : Event

Setting value	Description
startup	When booting
sd-attached	When attaching a microSD card

template_id : <1-10>

Schedule template number

[Initial value]

None

[Input mode]

global configuration mode

[Description]

When setting the schedule using “time,” this executes the actions listed in the specified schedule template at the specified time(s).

When setting the schedule using “event,” this executes the actions listed in the specified schedule template when the specified events occur.

If this command is executed with the "no" syntax, the schedule with the specified ID is deleted.

[Note]

When multiple schedules are executed at the same time, they are executed beginning with the schedule with the smallest ID.

When specifying the day, you cannot specify using a mix of numbers and weekdays.

If the seconds are omitted, the settings will be the same as when specifying “00” seconds.

For the month and days settings, you can specify ranges using “-” and “,” characters, and you can specify all dates using the “*” character. Note that for the seconds setting, you cannot specify ranges using “-” and “,” characters, nor can you specify all dates using the “*” character.

[Example]

This sets schedule #1 to execute schedule template #1 every Monday at exactly 0:00, 1:00, 2:00, 12:00, 21:00, 22:00 and 23:00.

```
SWX3220(config)#schedule time */mon -2,12-14,21-:0 1
```

4.29.2 Schedule template description text settings

[Syntax]

description *line*
no description

[Parameter]

line : Single-byte alphanumeric characters and single-byte symbols (64 characters or less)

Schedule template description text

[Initial value]

no description

[Input mode]

Schedule template mode

[Description]

Sets the schedule template description text.

If this command is executed with the "no" syntax, the description text in the specified schedule template is deleted.

[Example]

This sets the description text for schedule template #1.

```
SWX3220(config)#schedule template 1
SWX3220(config-schedule)#description Get tech-support
```

4.29.3 Settings to enable/disable schedule template

[Syntax]

action *switch*
no action

[Parameter]

switch : Schedule template settings

Setting value	Description
enable	Enable schedule template
disable	Disable schedule template

[Initial value]

action enable

[Input mode]

Schedule template mode

[Description]

This enables or disables the schedule template.

Specifying “disable” with this command makes it possible to stop execution of actions due to trigger startup.

If this command is executed with the "no" syntax, the schedule template is enabled.

[Example]

Disables schedule template #1.

```
SWX3220(config)#schedule template 1
SWX3220(config-schedule)#action disable
```

4.29.4 Schedule template settings

[Syntax]

schedule template *template_id*

no schedule template

[Parameter]

template_id	:	<1-10>
		Schedule template number

[Initial value]

None

[Input mode]

global configuration mode

[Description]

Switches to the mode for setting the schedule template.

If this command is executed with the "no" syntax, the specified schedule template is deleted.

[Example]

This switches to the mode for setting schedule template #1.

```
SWX3220(config)#schedule template 1
SWX3220(config-schedule)#
```

4.29.5 Schedule template command execution settings

[Syntax]

cli-command *id command*
no cli-command *id*

[Parameter]

id	:	<1-20>
		Command no.
command	:	Command

[Initial value]

None

[Input mode]

Schedule template mode

[Description]

This sets the commands to be executed when the trigger for a schedule function starts.

If this command is executed with the "no" syntax, commands with the specified numbers are deleted.

[Note]

If both the “cli-command” command and “script” command are configured for the same schedule template, the “script” command will be executed, and the “cli-command” will not operate.

If multiple commands are specified, the commands are executed beginning with the command with the smallest command number.

If multiple commands are specified, the remaining commands will still be executed even if the command results in an execution error while running.

As commands are executed in privileged EXEC mode when the trigger starts, some commands may need to be configured along with commands that switch to an appropriate mode.

The last “write” command must be executed to save the settings.

Commands cannot be specified in abbreviated form. For instance, you must write “interface port1.1” and not “int port1.1” when entering the input mode for Port1.1 of the interface.

The following commands cannot be executed.

backup system, baudrate select, boot prioritize sd, no boot prioritize sd, certificate user, commands beginning with “clock,” cold start, copy radius-server local, crypto pki generate ca, no crypto pki generate ca, disable, enable password, exit, firmware-update execute, firmware-update sd execute, logout, commands beginning with “ntpdate,” password-encryption, no

password encryption, ping, ping6, quit, reload, remote-login, restart, restore system, schedule, no schedule, schedule template, no schedule template, commands beginning with “show,” ssh , ssh-server host key generate, commands beginning with “stack,” commands beginning with “no stack,” startup-config select, no startup-config select, system-diagnostics on-demand execute(*1), telnet, traceroute, traceroute6, unregister yno, yno enable, yno disable

(*1): system-diagnostics on-demand execute no-confirm can be executed

[Example]

This registers the “copy tech-support sd” command in number #1 of schedule template #1.

```
SWX3220(config)#schedule template 1
SWX3220(config-schedule)#cli-command 1 copy tech-support sd
```

4.29.6 Schedule template script execution settings

[Syntax]

script *ref*
no script

[Parameter]

ref : Location of script file

Setting value	Description
sd	microSD card

[Initial value]

no script

[Input mode]

Schedule template mode

[Description]

This enables/disables execution of scripts when a trigger starts.

If this command is executed with the "no" syntax, script execution is disabled.

[Note]

When a trigger starts for the schedule function, the text located in the /[model name]/schedule/script.txt file on the microSD card will be executed as commands, from the beginning and up through line 100.

If both the “cli-command” command and “script” command are configured for the same schedule template, the “script” command will be executed, and the “cli-command” will not operate.

Commands that are prohibited from being executed through the “cli-command” command cannot be executed.

[Example]

This enables script execution on schedule template #1.

```
SWX3220(config)#schedule template 1
SWX3220(config-schedule)#script sd
```

4.30 Buzzer

4.30.1 Buzzer system settings

[Syntax]

buzzer *switch*
no buzzer

[Parameter]

switch : Enable or disable the buzzer system settings

Setting value	Description
enable	Enables the buzzer system settings.
disable	Disables the buzzer system settings.

[Initial value]

buzzer disable

[Input mode]

global configuration mode

[Description]

Enable or disable the buzzer system settings.

If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

Enables the buzzer system settings.

```
SWX3220(config)#buzzer enable
```

Disables the buzzer system settings.

```
SWX3220(config)#buzzer disable
```

4.30.2 Buzzer trigger settings

[Syntax]

buzzer trigger *trigger_type* [*trigger_type*]
no buzzer trigger *trigger_type* [*trigger_type*]

[Parameter]

trigger_type : Buzzer triggers

Trigger	Description
temperature	Sounds the buzzer when an abnormal temperature is detected.
fan	Sounds the buzzer when a fan abnormality is detected.
psu	Sounds the buzzer when a PSU abnormality is detected.
poe	Sounds the buzzer when a PoE power supply control abnormality is detected.
loop	Sounds the buzzer when a port shuts down due to a loop or a blocking error.
sfp	Sounds the buzzer when there is an SFP reception level error.
startup	Sounds the buzzer after startup is complete.
sd	Sounds the buzzer when mounting/unmounting an SD card.
all	Sets all of the above at once.

[Initial value]

no buzzer trigger all

[Input mode]

global configuration mode

[Description]

Enables any trigger.

If this command is executed with the "no" syntax, any trigger is disabled.

"psu" can only be set on models that support the power redundancy function.

poe can only be run on PoE power supply compatible models.

[Example]

Enable the startup sound.

```
SWX3220(config)#buzzer trigger startup
```

4.30.3 Executing the buzzer check command

[Syntax]

beep buzzer *beep_type*

[Parameter]

beep_type : Type of buzzer sound

Type	Description
system-error	System error sound
port-error	Port error sound
startup	Startup sound
sd-mount	SD card mounting sound
sd-unmount	SD card unmounting sound
mute	Mute sound
unmute	Unmute sound
find-switch	"Find this switch” execution sound

[Input mode]

privileged EXEC mode

[Description]

Execute the buzzer check command.

[Note]

The "Find this switch" execution sound, the system error sound, and the port error sound are repeated three times and automatically stopped.

If the system setting is enabled and mute is disabled, this command can be used even if buzzer trigger is disabled.

This command also causes an execution error if a buzzer sound is already being emitted.

[Example]

Check the port error sound.

```
SWX3220#beep buzzer port-error
```

4.30.4 Mute

[Syntax]

mute buzzer

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Executes mute.

[Note]

If the buzzer system settings are disabled with the **buzzer disable** command when mute is enabled, it will be unmuted.

This command is not saved in config.

[Example]

Executes mute.

```
SWX3220>mute buzzer
```

4.30.5 Unmute

[Syntax]

unmute buzzer

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Clears mute.

[Example]

Clears mute.

```
SWX3220>unmute buzzer
```

4.30.6 Display buzzer information

[Syntax]

show buzzer

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

Displays the settings and status of the buzzer.

[Example]

Displays the settings and status of the buzzer.

```
SWX3220>show buzzer
System           : Enable
Mute             : Disable
Status           : Standby
Enabled trigger  : Startup SD FAN Temperature Loop SFP
```

4.31 Yamaha Network Organizer (YNO)

4.31.1 Set YNO agent function

[Syntax]

yno enable
yno disable

[Keyword]

enable	:	Enables the YNO agent function
disable	:	Disables the YNO agent function

[Initial value]

yno disable

[Input mode]

global configuration mode

[Description]

This enables/disables the YNO agent function.

If the YNO agent function is enabled, the connection with the YNO manager starts automatically.

[Note]

YNO license registration is required to use the YNO function, and the user must agree that they are using the device only within Japan, as well as agree to the YNO terms of use.

[Example]

This enables the YNO agent function.

```
SWX3220(config)#yno enable
YNO is a service intended for use within Japan only.
Please do NOT use this Service if
 - you or a user of the Service resides outside Japan.
 - the network device is installed outside of Japan.
Are all users and this device located in Japan? (y/n): y

To activate this function, you have to
 - purchase a YNO license.
 - agree the terms and conditions before purchasing.
http://www.rtpro.yamaha.co.jp/RT/docs/yno/license.pdf
Have you purchased a license and agreed the terms and conditions? (y/n): y
```

This disables the YNO agent function.

```
SWX3220(config)#yno disable
```

4.31.2 Set keepalive time interval with YNO server

[Syntax]

yno keepalive xmpp **interval** *time*
yno keepalive gfw **interval** *time*
no yno keepalive xmpp **interval**
no yno keepalive gfw **interval**

[Keyword]

xmpp	:	XMPP server (Extensible Messaging and Presence Protocol server)
gfw	:	GFW server (GUI Forwarder server)

[Parameter]

time	:	<30-300>
		XMPP keepalive time interval (seconds)
time	:	<3-60>
		GFW keepalive time interval (seconds)

[Initial value]

yno keepalive xmpp interval 300

yno keepalive gfw interval 30

[Input mode]

global configuration mode

[Description]

Sets the time interval for communicating keepalive messages with the YNO server.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

If this command is executed while connecting to the YNO manager, the connection with the YNO manager will automatically be reconnected in order to apply the settings.

[Example]

Sets the keepalive time interval with the YNO server (XMPP server) to 60 seconds.

```
SWX3220(config)#yno keepalive xmpp interval 60
```

Sets the keepalive time interval with the YNO server (GFW server) to 10 seconds.

```
SWX3220(config)#yno keepalive gfw interval 10
```

4.31.3 Set HTTPS proxy server for YNO

[Syntax]

yno https-proxy *server port*
no yno https-proxy

[Parameter]

server	:	HTTPS proxy server host name or IP address Up to 255 single-byte alphanumeric characters and symbols, except for spaces and these characters: ? " ' \
port	:	<1-65535> Port number of HTTPS proxy server

[Initial value]

None

[Input mode]

global configuration mode

[Description]

Sets the HTTPS proxy server used by YNO.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

Only HTTPS proxy servers that use the HTTP/1.1 CONNECT method are supported. HTTPS proxy servers that require user authentication cannot be used.

If this command is executed while connecting to the YNO manager, the connection with the YNO manager will automatically be reconnected in order to apply the settings.

[Example]

Sets the HTTPS proxy server used by YNO.

```
SWX3220(config)#yno https-proxy 192.168.100.1 8080
```

4.31.4 Unregister YNO

[Syntax]

unregister yno

[Input mode]

privileged EXEC mode

[Description]

Forcibly deregisters this device from the YNO.

[Note]

For this command, the YNO agent function must be enabled, and communication must be possible with the YNO manager.

This command cannot be used if the stack is enabled.

[Example]

Forcibly deregisters this device from the YNO.

```
SWX3220(config)#unregister yno
Unregister this device from YNO Manager? (y/n):y
```

4.31.5 Show the operating status of the YNO agent

[Syntax]

show yno

[Input mode]

privileged EXEC mode

[Description]

Shows the operating status of the YNO agent.

The following items are shown.

- YNO agent setting status
- Status of connection with YNO manager

Display	Description
Online	Connection status
Offline (reason for abnormality)	Disconnected status (reason for abnormality) • Connection with ACS failed • Cannot be managed due to insufficient licenses • Operator account is disabled • Operator account was deleted • Device not registered with YNO manager • Stack function is enabled, but setting on YNO manager is not assigned to stack group • Stack function is disabled, but is assigned to stack group due to YNO manager settings

- Time that connection was established with YNO manager
- Managing operator ID for the YNO agent device
- Connection status of each YNO manager server (ACS, XMPP, GFW server)

Display	Description
Connected	Connected
Not connected	Not connected
Abnormal	Abnormal

[Example]

Shows the operating status of the YNO agent.

```
SWX3220#show yno
[YNO Agent status]
  YNO Agent         : Enable
  Connection status : Online
  Connected date    : 2025/02/27 16:02:38
  Operator ID       : Sample00001

[Server connection status]
  ACS  : Connected
  XMPP : Connected
  GFW  : Connected
```

4.32 Yamaha Unified Network Operation Service (Y-UNOS)

4.32.1 Set Y-UNOS function

[Syntax]

y-unos enable
y-unos disable
no y-unos

[Keyword]

enable : Enable Y-UNOS function

disable : Disable Y-UNOS function

[Initial value]

y-unos enable

[Input mode]

global configuration mode

[Description]

Enables or disables Y-UNOS (Yamaha Unified Network Operation Service: a service which links devices together via a network).

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

The Y-UNOS function operates only with the management VLAN. When no IPv4 address is set in the management VLAN or the management VLAN is linked down, the Y-UNOS function is stopped.

If the management VLAN has been changed, the multicast frame forwarding settings (**l2-mcast flood 239.192.128.250**) of the Y-UNOS mutual automatic recognition function are applied to the maintenance VLAN.

It may take up to one second to enable or disable the Y-UNOS function.

This command cannot be used if the stack function is enabled.

[Example]

This enables the Y-UNOS function.

```
SWX3220(config)#y-unos enable
```

This disables the Y-UNOS function.

```
SWX3220(config)#y-unos disable
```

4.32.2 Show Y-UNOS information

[Syntax]

show y-unos

[Input mode]

privileged EXEC mode

[Description]

Shows Y-UNOS-related settings and status information.

The following content is displayed.

- Y-UNOS function settings (Y-UNOS)
- Y-UNOS function status (Status)
- Y-UNOS function IPv4 address (IPv4-Address)
  - View management VLAN IPv4 address and ID
- List of detected devices
  - Model name (Model)
  - Serial number (Serial)
  - Firmware version (Version)
  - MAC address (MAC-Address)
  - IPv4 address (IPv4-Address)
  - Host name (HostName)

One of the following items is displayed in the status (Status) for Y-UNOS.

Status	Description
Active	Operational status of Y-UNOS function
Inactive(stack enable)	Non-operational status of Y-UNOS function (stack function is enabled) *Only for devices that support stack functionality
Inactive(no ipv4 address)	Non-operational status of Y-UNOS function (IPv4 address not set for management VLAN, or management VLAN is linked down)
Disable	Y-UNOS function is disabled

[Example]

This shows the Y-UNOS information.

```
SWX3220#show y-unos
Y-UNOS        : Enable
Status        : Active
```

```
IPv4 address : 192.168.10.6 (vlan1)

Model           Serial     Version     MAC-Address    IPv4-Address    HostName
-------------------------------------------------------------------------------
RM-CR           RMCR00001  V2.0.0      0000.0000.0000 192.168.10.5    RMCR-hostname
SWX3220-16MT    Z740000000 Rev.4.02.11 0000.0000.0000 192.168.10.4    SWX3220
SWX2310-28GT    Z610000000 Rev.2.04.15 0000.0000.0000 192.168.10.28   SW-Hostname002
```

4.33 General maintenance and operation functions

4.33.1 Set host name

[Syntax]

hostname *hostname*
no hostname [*hostname*]

[Parameter]

hostname	:	Single-byte alphanumeric characters and single-byte symbols (63characters or less) Host name

[Initial value]

hostname SWX3220

[Input mode]

global configuration mode

[Description]

Specifies the host name.

The host name specified by this command is used as the command prompt. If SNMP access is possible, this is used as the value of the MIB variable sysName.

If this command is executed with the "no" syntax, the setting returns to the default value.

[Example]

Set the host name as "yamaha."

```
SWX3220(config)#hostname yamaha
yamaha(config)#
```

4.33.2 Reload system

[Syntax]

reload [**stack-member ID**]
restart [**stack-member ID**]

[Keyword]

stack_member	:	Specify stack member to restart in stack configurationIf omitted, all stack members restart

[Parameter]

ID	:	<1-2> Stack ID

[Input mode]

privileged EXEC mode

[Description]

Reboots the system.

[Note]

If the currently-running settings (running configuration) have been changed from the settings at the time of boot (startup configuration), reboot will discard those changes. Therefore, if necessary, you should execute the **copy running-config startup-config** command, the **write** command or the **save** command before you execute the **reload** command.

The "stack-member" option can be specified only when the stack function is enabled.

[Example]

Reboot the system.

```
SWX3220#reload
reboot system? (y/n): y
```

4.33.3 Initialize settings

[Syntax]

cold start

[Input mode]

privileged EXEC mode

[Description]

Reboots with the factory settings. SYSLOG is also initialized.

[Note]

You must enter the privileged password when executing this command.

This command cannot be executed when the privileged password is in the default state. The privileged password must be changed first.

[Example]

Initialize the settings.

```
SWX3220#cold start
Password:
```

4.33.4 Mount SD card

[Syntax]

mount sd

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Mounts the SD card.

When you insert an SD card, this command is executed automatically, so you do not need to execute it. If you have unmounted the card by the **unmount sd** command, you will need to execute this.

[Note]

The SD card cannot be used if the SD card is in an unmounted state.

[Example]

Mount the SD card.

```
SWX3220>mount sd
```

4.33.5 Unmount SD card

[Syntax]

unmount sd

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Unmounts the SD card.

If this command is not executed, or if the SD card is removed from the SD card slot without executing the unmount process from the Web GUI, there are some cases in which the operating system will generate a warning to repair the card's file system.

[Note]

The SD card cannot be used if the SD card is in an unmounted state.

[Example]

Unmount the SD card.

```
SWX3220>unmount sd
```

4.33.6 Set default LED mode

[Syntax]

led-mode default *mode*
no led-mode default

[Parameter]

mode : Default LED mode

Setting value	Description
link-act	LINK/ACT mode
off	OFF mode

[Initial value]

led-mode default link-act

[Input mode]

global configuration mode

[Description]

Set the default LED mode.

When you execute this command, the LEDs are lit in the specified mode.

If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

Set the default LED mode to OFF mode.

```
SWX3220(config)#led-mode default off
```

4.33.7 Show LED mode

[Syntax]

show led-mode

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the LED mode setting and status.

The following items are shown.

- Default LED mode setting
- Current LED mode status

[Example]

Show the LED mode setting and status.

```
SWX3220>show led-mode
default mode : off
current mode : link-act
```

4.33.8 Show port error LED status

[Syntax]

show error port-led

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the ID of ports that are generating an error, and the following error causes.

Item	Description
loop-detected (blocking)	Detected a loop, and are currently blocking
loop-detected (shutdown)	Detected a loop, and are currently shutdown
sfp rx-power error (low)	SFP optical reception level is below the normal range
sfp rx-power error (high)	SFP optical reception level is above the normal range

[Example]

Show the port error status.

```
SWX3220>show error port-led
 ID             error
----------------------------------------
 port1.1        loop-detected (blocking)
```

4.33.9 Show DIP switches status

[Syntax]

show dipsw

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Show status of the DIP switches at startup and the current status.

- Preset type : preset type to apply
- L2MS : enable/dusable the L2MS function
- LED : set whether the LED is lit/unlit

[Example]

Show the status of the DIP switches.

```
SWX3220>show dipsw
[Startup status]
   DIPSW  |   1   2   3   4   5   6   7   8
-------------------------------------------
   Status | OFF OFF OFF OFF OFF OFF  ON  ON
-------------------------------------------
     Preset type : Normal
     L2MS        : ON
     LED         : ON

[Current status]
   DIPSW  |   1   2   3   4   5   6   7   8
-------------------------------------------
   Status | OFF OFF OFF OFF OFF OFF  ON  ON
-------------------------------------------
     Preset type : Normal
     L2MS        : ON
     LED         : ON
```

[Models]

SWX3220-30MC, SWX3220-30TCs

4.33.10 Starting the "Find this switch" function

[Syntax]

find switch start *sec method* [*method*]

[Parameter]

sec : <5-3600>

“Find this switch” time (seconds)

method : Method

Parameter	Description
buzzer	Sounds the buzzer with the "Find this switch" execution sound.
led	Blinks the port LED in amber.

[Input mode]

privileged EXEC mode

[Description]

Executes the “Find this switch” function with the specified number of seconds and method.

[Note]

If the buzzer system settings are disabled or it is muted, the buzzer will not sound.

Also, if the current LED mode is OFF mode, the LED cannot blink.

[Example]

Start the "Find this switch" function with buzzer and LED for 10 seconds only.

```
SWX3220#find switch start 10 buzzer led
```

4.33.11 Stop the “Find this switch” function

[Syntax]

find switch stop

[Input mode]

privileged EXEC mode

[Description]

Stops the 'Find this switch' function.

[Example]

Stops the 'Find this switch' function.

```
SWX3220#find switch stop
```

4.33.12 Backup system information

[Syntax]

backup system

[Input mode]

privileged EXEC mode

[Description]

Copy the following settings from the unit to the SD card.

- Startup configurations #0 - #1 and information that pertains to them
- **startup-config select** command values
- **boot prioritize sd** command values
- **boot auto-apply**Command setting value

If the SD card's "/swx3220/firmware" folder contains "swx3220.bin", copy it to the backup folder.

This can be executed only if the SD card is mounted.

[Note]

Do not edit or delete the files that are backed up to the SD card.

[Example]

Execute a system information backup.

```
SWX3220#backup system
Succeeded to backup system files and firmware file.
```

4.33.13 Restore system information

[Syntax]

restore system

[Input mode]

privileged EXEC mode

[Description]

System information previously backed up to SD card is restored to the unit.

If a firmware file exists in the backup folder of the SD card, the firmware will also be updated using that file.

After restore, restart will occur.

This can be executed only if the SD card is mounted.

[Note]

This command cannot be used if the stack function is enabled.

[Example]

Restore system information into the unit.

```
SWX3220# restore system
restore and reboot system? (y/n) y
Update the firmware.
Current Revision: 4.02.01
New Revision:     4.02.03

Update to this firmware? (y/n) y
Unmounted the SD card.  Pull out the SD card.
Updating...
Finish
Succeeded to restore system files.
SWX3220#
```

4.33.14 Set ProAV profile type

[Syntax]

proav profile-type *type* [**name** *name*]
no proav profile-type

[Parameter]

type : ProAV profile type

Setting value	Description
dante-primary	Dante primary
dante-secondary	Dante secondary
extron-nav	Extron NAV
ipmx	IPMX
ndi	NDI
sdvoe	SDVoE
smpte-st-2110-ptp-tc	SMPTE ST 2110 with PTP TC

name : Profile identifier name

Up to 32 single-byte alphanumeric characters and symbols, other than the ? (question mark) character and spaces

[Initial value]

None

[Input mode]

interface mode

[Description]

Sets the ProAV profile type.

This command is used with the the ProAV settings page in the Web GUI, to select the compatible ProAV profile type for the VLAN.

[Note]

This command can be specified only for VLAN interfaces.

Executing this command via CLI does not apply the ProAV profile settings.

This command cannot be used if the stack function is enabled.

Chapter 5

Interface control

5.1 Interface basic settings

5.1.1 Set description

[Syntax]

description *line*
no description

[Parameter]

line	:	Single-byte alphanumeric characters and single-byte symbols (80characters or less) Description of the applicable interface

[Initial value]

no description

[Input mode]

interface mode

[Description]

Specifies a description of the applicable interface. If this command is executed with the "no" syntax, the description is deleted.

[Example]

Specify a description for LAN port #1.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#description Connected to rtx1210-router
```

5.1.2 Shutdown

[Syntax]

shutdown
no shutdown

[Initial value]

no shutdown

[Input mode]

interface mode

[Description]

Shut down the applicable interface so that it is not used.

An interface for which this command is specified will not link-up even if it is connected.

If this command is executed with the "no" syntax, the applicable interface can be used.

[Note]

This command can be specified only for LAN/SFP port and logical interface.

If this command is applied to logical interface, the settings of all LAN/SFP port units belonging to that interface are changed.

[Example]

Shut down LAN port #1 so that it is not used.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#shutdown
```

5.1.3 Set communication speed and communication mode

[Syntax]

speed-duplex *type*

no speed-duplex

[Parameter]

type : Communication speed and communication mode types

Communication speed and communication mode types	Description
auto	Auto negotiation
25000-full	25Gbps/Full
10000-full	10Gbps/Full
100-full	100Mbps/Full
100-half	100Mbps/Half

[Initial value]

speed-duplex auto

[Input mode]

interface mode

[Description]

Sets the communication speed and communication mode.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

When this command is used to change the settings, link-down temporarily occurs for the corresponding interface.

This command can be specified only for LAN/SFP port.

When “auto” is specified for “type,” a communication type supported by auto negotiation can be set using the auto negotiation type settings.

The configurable communication speed/mode will differ depending on the port type. Configurable communication speeds/modes are shown below.

Communication speed and communication mode types	LAN port	SFP+ port	SFP28 port	QSFP28 port
auto	○	○	○	○
25000-full	-	-	○	-
10000-full	-	○	-	-
5000-full	-	-	-	-
2500-full	-	-	-	-
1000-full	-	-	-	-
100-full	○	-	-	-
100-half	○ (*1)	-	-	-

*1: Cannot be set to 100Mbps/Half on the SWX3220-30MC and SWX3220-30TCs.

Note that when connecting a SFP module to an SFP+ port and specifying 10000-full, the module will run at 1000-full.

When connecting the SFP module to an SFP28 port and specifying 25000-full, the module will run at 1000-full.

[Example]

Set the communication speed and communication mode for LAN port #1 to 100Mbps/Full.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#speed-duplex 100-full
```

5.1.4 Auto negotiation type settings

[Syntax]

negotiation *type* [*type*..]
no negotiation

[Parameter]

type : Communication type

Communication type	Explanation
10000-full	10Gbps/Full
5000-full	5Gbps/Full
2500-full	2.5Gbps/Full
1000-full	1000Mbps/Full
100-full	100Mbps/Full
100-half	100Mbps/Half

[Initial value]

Model	Default setting
SWX3220-16MT, SWX3220-16TMs	negotiation 10000-full 5000-full 2500-full 1000-full 100-full 100-half
SWX3220-30MC, SWX3220-30TCs	negotiation 10000-full 5000-full 2500-full 1000-full 100-full

[Input mode]

interface mode

[Description]

Sets the communication type supported by auto negotiation.

If this command is executed with the "no" syntax, the setting returns to the default.

This command can be specified only for a LAN port.

[Note]

When this command is used to change the settings, link-down temporarily occurs for the corresponding interface.

If a setting other than auto negotiation is specified in the communication speed/communication mode settings, this function will not operate.

[Example]

This sets the communication type supported by auto negotiation of LAN port #1 to 1Gbps/Full and 100Mbps/Full.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)negotiation 1000-full 100-full
```

5.1.5 Changing forward error correction (FEC)

[Syntax]

fec *mode*
no fec

[Parameter]

mode : Forward error correction mode

Setting value	Description
auto	Sets the FEC method automatically, depending on the module
cl74	Enables FEC (Clause 74 FC-FEC, KR-FEC, 25G)
cl91	Enables FEC (Clause 91 RS-FEC, 100G)
cl108	Enables FEC (Clause 108 RS-FEC, 25G)
off	Disables FEC

[Initial value]

fec auto

[Input mode]

interface mode

[Description]

Sets forward error correction (FEC) on the targeted interface.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

The forward error correction settings need to match those of the opposing device.

This command can be specified only for a SFP28 and QSFP28 port.

When this command is used to change the settings, link-down temporarily occurs for the corresponding interface.

When connecting the SFP/SFP+ module to an SFP28 port, FEC is disabled during operations.

The parameter to specify varies depending on the interface used to specify the command.

Interface	auto	cl74	cl91	cl108	off
LAN port	-	-	-	-	-
SFP+ port	-	-	-	-	-
SFP28 port	○	○	-	○	○
QSFP28 port	○	-	○	-	○

When "auto" is specified, the FEC method is used according to the connected module.

Module	FEC
YSFP-25G-SR	Enabled (Clause 108, RS-FEC)
YSFP-25G-LR	Enabled (Clause 108, RS-FEC)
YAOC-25G-1M	Enabled (Clause 108, RS-FEC)
YAOC-100G-1M	Enabled (Clause 91, RS-FEC)

[Example]

This sets forward error correction on the port1.29 to cl91.

```
SWX3220(config)#interface port1.29
SWX3220(config-if)#fec cl91
```

[Models]

SWX3220-30MC, SWX3220-30TCs

5.1.6 Auto negotiation information display

[Syntax]

show interface negotiation [*ifname*]

[Parameter]

ifname : The interface name of the LAN/SFP port. If this is omitted, the command applies to all interfaces.

Interface to show

[Input mode]

unprivileged EXEC mode、 privileged EXEC mode

[Description]

Displays the auto negotiation information for the interface.

The following items are shown.

Item	Explanation
Interface	Interface name
Nego	Auto negotiation enable/disable
Link Advertisement	Communication speed and communication mode supported by auto negotiation

[Example]

Displays the auto negotiation information.

```
SWX3220#show interface negotiation
Codes: Nego - Auto-negotiation
       All  - 10000-full, 5000-full, 2500-full, 1000-full, 100-full, 100-half

Interface  Nego      Link Advertisement
----------------------------------------------------------------------
port1.1    Enabled   All
port1.2    Enabled   10000-full, 5000-full, 2500-full, 1000-ful, 100-full
port1.3    Enabled   100-full, 100-half
port1.4    Enabled   All
port1.5    Enabled   --
port1.6    Enabled   --
port1.7    Enabled   --
port1.8    Enabled   --
```

5.1.7 Set MRU

[Syntax]

mru *mru*

no mru

[Parameter]

mru : <64-10240>

Maximum frame size that can be received (the specified value must be an even number)

[Initial value]

mru 1522

[Input mode]

interface mode

[Description]

Specifies the maximum frame size that can be received.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be specified only for LAN/SFP port.

[Example]

Set the LAN port #1 mru to 9000 bytes.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#mru 9000
```

5.1.8 Set cross/straight automatic detection

[Syntax]

mdix auto *action*
no mdix auto

[Parameter]

type : Cross/straight automatic detection operations

Setting value	Description
enable	Enable cross/straight automatic detection
disable	Disable cross/straight automatic detection

[Initial value]

mdix auto enable

[Input mode]

interface mode

[Description]

Enables cross/straight automatic detection. If this is enabled, the necessary cable connection type (straight or cross) is automatically detected, and the connection is specified appropriately.

If this is executed with the "no" syntax, automatic detection is disabled, and MDI is used.

[Note]

This command can be specified only for LAN port.

When this command is used to change the settings, link-down temporarily occurs for the corresponding interface.

[Example]

Disable cross/straight automatic detection for LAN port #1.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#mdix auto disable
```

5.1.9 Set EEE

[Syntax]

eee *action*
no eee

[Parameter]

type : Behavior of the EEE

Setting value	Description
enable	Enable EEE
disable	Disable EEE

[Initial value]

eee disable

[Input mode]

interface mode

[Description]

Enables Energy Efficient Ethernet (EEE).

If this command is executed with the "no" syntax, EEE is disabled.

[Note]

This command can be specified only for LAN port.

When this command is used to change the settings, link-down temporarily occurs for the corresponding interface.

[Example]

Enable EEE for LAN port #1.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#eee enable
```

5.1.10 Show EEE capabilities

[Syntax]

show eee capabilities interface *ifname*

[Parameter]

ifname : LAN port interface name

Interface to show

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows whether the specified interface supports EEE.

The following items are shown.

Item	Description
interface	Interface name
EEE(efficient-ethernet)	Whether the unit supports EEE
Link Partner	Whether the other unit supports EEE

[Note]

If another unit is not connected, the display indicates that EEE is not supported.

[Example]

Show EEE capabilities for LAN port #1.

[If the other unit supports EEE]

```
SWX3220#show eee capabilities interface port1.1
interface:port1.1
  EEE(efficient-ethernet):  yes (1000-T, 100-TX)
  Link Partner           :  yes (1000-T, 100-TX)
```

[If the other unit does not support EEE]

```
SWX3220#show eee capabilities interface port1.1
interface:port1.1
  EEE(efficient-ethernet):  yes (1000-T, 100-TX)
  Link Partner           :  not enabled
```

5.1.11 Show EEE status

[Syntax]

show eee status interface *ifname*

[Parameter]

ifname : LAN port interface name

Interface to show

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the EEE status of the specified interface.

The following items are shown.

Item	Description
interface	Interface name

Item	Description
EEE(efficient-ethernet)	Whether EEE is enabled
Rx LPI Status	Low-power mode status of the receiving unit
Tx LPI Status	Low-power mode status of the transmitting unit
Wake Error Count	Error count

[Example]

Show EEE status of LAN port #1.

[If EEE is disabled]

```
SWX3220#show eee status interface port1.1
interface:port1.1
  EEE(efficient-ethernet):  Disabled
  Rx LPI Status          :  None
  Tx LPI Status          :  None
  Wake Error Count       :  0
```

[If EEE is enabled]

```
SWX3220#show eee status interface port1.1
interface:port1.1
  EEE(efficient-ethernet):  Operational
  Rx LPI Status          :  Received
  Tx LPI Status          :  Received
  Wake Error Count       :  0
```

[If EEE is enabled and is transitioning to low-power mode]

```
SWX3220#show eee status interface port1.1
interface:port1.1
  EEE(efficient-ethernet):  Operational
  Rx LPI Status          :  Interrupted
  Tx LPI Status          :  Interrupted
  Wake Error Count       :  0
```

[If EEE is enabled and has transitioned to low-power mode]

```
SWX3220#show eee status interface port1.1
interface:port1.1
  EEE(efficient-ethernet):  Operational
  Rx LPI Status          :  Low Power
  Tx LPI Status          :  Low Power
  Wake Error Count       :  0
```

5.1.12 Set port mirroring

[Syntax]

mirror interface *ifname* direction *direct*
no mirror interface *ifname* [direction *direct*]

[Keyword]

direction : Specify the direction of traffic that is mirrored

[Parameter]

ifname : LAN/SFP port interface name

Interface whose traffic is mirrored

direct : Direction of traffic that is mirrored

Traffic direction	Description
both	Both receiver and transmitter
receive	Receiver
transmit	Transmitter

[Initial value]

none

[Input mode]

interface mode

[Description]

Mirrors the traffic specified by *direct*, with the applicable interface as the sniffer port and *ifname* as the monitored port.

If this command is executed with the "no" syntax, the mirroring setting is deleted.

[Note]

This command can be specified only for LAN/SFP port.

Only one interface can be specified as the sniffer port.

[Example]

With LAN port #1 as the sniffer port, mirror the transmitted and received frames of LAN port #4 and the transmitted frames of LAN port #5.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#mirror interface port1.4 direction both
SWX3220(config-if)#mirror interface port1.5 direction transmit
```

5.1.13 Show port mirroring status

[Syntax]

show mirror [interface *ifname*]

[Keyword]

interface	:	Specify the monitored port to show

[Parameter]

ifname	:	Interface name of the LAN/SFP port Monitored port to show

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the port mirroring setting. If interface is omitted, the settings for all monitored ports are shown.

The following items are shown for each monitored port.

Item	Description
Monitored Port	Interface name of the monitored port
Sniffer Port	Interface name of the sniffer port
Direction	>Direction of traffic that is mirrored

[Example]

Show the mirroring port settings.

```
SWX3220#show mirror
Sniffer Port   Monitored Port  Direction
=============  ==============  ==========
port1.1        port1.4         both
port1.1        port1.5         transmit
```

5.1.14 Show interface status

[Syntax]

show interface [*type* [*index*]]

[Parameter]

type	:	Interface type

Interface type	Description
port	physical interface
vlan	VLAN interface
sa	static logical interface
po	LACP logical interface

index : Index number

Interface ID	Description
S.X	Specifies the stack ID (S) of the physical interface, and the number printed on the chassis (X).@ stack_message2@
<1－4094>	Specifies the VLAN ID.
<1－96>	Specifies the static logical interface number.
<1－127>	Specifies the LACP logical interface number.

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the status of the interface specified by *ifname*. If *ifname* is omitted, shows the status of all interfaces.

The following items are shown.

Item	Description
Interface	Interface name
Link is	Link status *2 (if shutdown, shows the cause) • If shutdown is specified : (by shutdown) • If port error is detected : (by err-disable)
Hardware is	Interface type (e.g., Ethernet, VLAN)
HW addr	Physical (MAC) address *1
Description	Description of interface
ifIndex	Interface index number
MRU	Maximum Receive Unit *4
ARP ageing timeout	ARP timeout time (time that ARP entries are maintained) *3
Speed-Duplex	Communication speed and communication mode settings, and operating status *1
Fec	Forward Error Correction setting value and operating status *6
Auto MDI/MDIX	Auto MDI/MDIX enabled/disabled *1
IPv4 address	IP address/mask length *3 (shown only if IP address is set)
broadcast	IP broadcast address *3 (shown only if IP address is set)

Item		Description
Switchport mode		Switchport mode • access : untagged • trunk : tagged
Ingress filter		Input filtering status • enable : enabled • disable : disabled
Acceptable frame types		Frame types that can be received • all : all frames are received (regardless of whether they are tagged or untagged) • vlan-tagged only : only frames with a VLAN tag are received
Default Vlan		VLAN ID that handles untagged frames • For an untagged port : VLAN specified by the **switchport access vlan** command • For a tagged port : Native VLAN • For a tagged port and set to receive only tagged packets : None • If unspecified : vlan1
Configured Vlans		List of the VLAN IDs that belong to the corresponding interface
input	packets	Number of packets received *2
	bytes	Number of bytes received *2
	multicast packets	Number of multicast packets received *2
	drop packets	Number of buffer overflowed packets received *2, *5
output	packets	Number of packets transmitted *2
	bytes	Number of bytes transmitted *2
	multicast packets	Number of multicast packets transmitted *2
	broadcast packets	Number of broadcast packets transmitted *2
	drop packets	Number of tail-dropped packets transmitted * 2, *5

*1 Shown only for physical interface
*2 Shown only for physical interface and logical interface
*3 Shown only for VLAN interface
*4 In the case of logical interface and VLAN interface, shows the minimum value for the physical interface belonging to that interface
*5 Shows the transmission information when tail dropping is enabled, and the information only for reception when tail dropping is disabled.
*6 Shown only for SFP28 and QSFP28 ports.

[Example]

Show the status of LAN port #1.

```
SWX3220# show interface port 1.1
Interface port1.1
  Link is UP
  Hardware is Ethernet
  HW addr: 00a0.de00.0000
  Description: Connected to router
  ifIndex 5001, MRU 1522
```

```
  Speed-Duplex: auto(configured), 1000-full(current)
  Auto MDI/MDIX: on
  Vlan info:
    Switchport mode         : access
    Ingress filter          : enable
    Acceptable frame types  : all
    Default Vlan            :    1
    Configured Vlans        :    1
  Interface counter:
    input  packets          : 320
           bytes            : 25875
           multicast packets: 301
    output packets          : 628
           bytes            : 129895
           multicast packets: 628
           broadcast packets: 0
           drop packets     : 0
```

Show the status of VLAN #1.

```
SWX3220#show interface vlan 1
Interface vlan1
  Hardware is VLAN
  Description: Connected to router(VLAN)
  ifIndex 301, ARP ageing timeout 1200
  IPv4 address 192.168.100.240/24 broadcast 192.168.100.255
                                                (u)-Untagged, (t)-Tagged
VLAN ID  Name                             State   Member ports
======= ================================ ======= ======================
1       default                           ACTIVE  port1.1(u) port1.2(u)
                                                  port1.3(u) port1.4(u)
                                                  port1.5(u) port1.6(u)
                                                  port1.7(u) port1.8(u)
```

5.1.15 Show brief interface status

[Syntax]

show interface brief

[Input mode]

unprivileged EXEC mode, privileged EXEC mode, individual configuration mode

[Description]

Shows brief interface status.

The following items are shown.

Item	Description
Interface	Interface name
Type	Interface type *2
PVID	VLAN ID that handles untagged frames *2
Mode	Mode of the switchport *2 • access : untagged • trunk : tagged
Status	Link status
Reason	Cause of link down • AD: If shutdown is specified • ED: If port error is detected • PD: Other than above
Speed	Communication speed operating status *2

Item	Description
Port Ch	Type of associated logical interface *1 • (S) : Static logical interface • (P) : LACP logical interface ID of associated logical interface
Description	Description of interface

*1 Shown only for physical interface
*2 hown only for physical interface and logical interface

[Example]

Show brief interface status.

```
SWX3220#show interface brief

Codes: ETH - Ethernet, AGG - Aggregate , PVID - Port Vlan-id
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down



-------------------------------------------------------------------------------
Ethernet   Type  PVID  Mode       Status  Reason  Speed Port    Description
Interface                                                Ch #
-------------------------------------------------------------------------------
port1.1    ETH   1     access     up      --      1g    (S)1    --
port1.2    ETH   1     access     up      --      1g    --      --
port1.3    ETH   1     access     down    PD      auto  --      --
port1.4    ETH   1     access     down    AD      auto  --      --
port1.5    ETH   1     access     up      --      1g    --      --
port1.6    ETH   1     access     up      --      1g    --      --
port1.7    ETH   1     access     up      --      1g    --      --
port1.8    ETH   1     access     up      --      1g    --      --


-------------------------------------------------------------------------------
Interface    Status   Reason  Description
-------------------------------------------------------------------------------
vlan1        up       --      --
vlan2        down     PD      --


-------------------------------------------------------------------------------
Port-channel  Type  PVID  Mode       Status   Reason  Speed  Description
Interface
-------------------------------------------------------------------------------
sa1           AGG   1     access     up       --      1g     --
```

5.1.16 Resetting an interface

[Syntax]

interface reset *ifname*

[Parameter]

ifname : LAN/SFP port or logical interface

Interface to reset

[Input mode]

privileged EXEC mode

[Description]

This resets the specified interface.

[Note]

The link status for the specified interface will be reset, and the link is re-established.

Note that linkdown will momentarily occur in order to reset.

This cannot be executed for LAN/SFP port that belong to logical interface

[Example]

Reset LAN port #1

```
SWX3220#interface reset port1.1
```

5.1.17 Show frame counter

[Syntax]

show frame-counter [*ifname*]

[Parameter]

ifname : Interface name of the LAN/SFP port

Interface to show

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows frame counter information for the interface specified by *ifname*. If *ifname* is omitted, shows information for all interfaces.

The following items are shown.

Item	Description
Packets	Number of packets transmitted/received
Octets	Number of octets transmitted/received
Broadcast packets	Number of broadcast packets transmitted/received
Multicast packets	Number of multicast packets transmitted/received
Unicast packets	Number of unicast packets transmitted/received
Undersize packets	Number of undersize packets received (packets smaller than 64 octets)
Oversize packets	Number of oversize packets received (packets larger than 1523 octets*1)
Fragments	Number of fragment packets received (packs smaller than 64 octets with abnormal CRC)
Jabbers	Number of jabber packets received (packs larger than 1523 octets with abnormal CRC*1)
FCS errors	Number of FCS error packets received
RX errors	Number of reception errors
TX errors	Number of transmission errors
Collisions	Number of collision occurrences
Drop packets	Number of tail-dropped packets transmitted, number of packets not received due to buffer overflow *2
64octet packets	Number of packets with 64 octet length transmitted/received
65-127octet packets	Number of packets with 65--127 octet length transmitted/received
128-255octet packets	Number of packets with 128--255 octet length transmitted/received
256-511octet packets	Number of packets with 256--511 octet length transmitted/received
512-1023octet packets	Number of packets with 512--1023 octet length transmitted/received
1024-MAXoctet packets	Number of packets with 1024--maximum octet length (*1) transmitted/received

*1 Varies depending on the MRU of each interface.
*2 Shows the transmission information when tail dropping is enabled, and the information only for reception when tail dropping is disabled.

[Example]

Show the frame counter of LAN port #1.

```
SWX3220#show frame-counter port1.1
Interface port1.1 Ethernet MAC counters:
  Received:
    Packets               : 84
    Octets                : 6721
    Broadcast packets     : 8
    Multicast packets     : 76
    Unicast   packets     : 0
    Undersize packets     : 0
    Oversize  packets     : 0
    Fragments             : 0
    Jabbers               : 0
    FCS errors            : 0
    RX errors             : 0

  Transmitted:
    Packets               : 91
    Octets                : 11193
    Broadcast packets     : 0
    Multicast packets     : 91
    Unicast   packets     : 0
    TX errors             : 0
    Collisions            : 0
    Drop packets          : 0

  Received and Transmitted:
    64octet       packets : 1
    65-127octet   packets : 166
    128-255octet  packets : 7
    256-511octet  packets : 1
    512-1023octet packets : 0
    1024-MAXoctet packets : 0
```

5.1.18 Clear frame counters

[Syntax]

clear counters *ifname*
clear counters all

[Keyword]

all	:	Clearing the frame counter information for all interfaces

[Parameter]

ifname	:	Interface name of LAN/SFP port or logical interface Applicable interface

[Input mode]

privileged EXEC mode

[Description]

This clears the frame counter for the interfaces.

If *ifname* is specified, the frame counter for that interface is cleared.

If logical interface is specified as the *ifname*, the frame counters of all LAN/SFP port port units associated with that interface are cleared.

[Example]

Clear the frame counters of LAN port #1.

```
SWX3220#clear counters port1.1
```

5.1.19 Show SFP module status

[Syntax]

show ddm status [interface *ifname*]

[Keyword]

interface	:	Specifies the SFP port to show

[Parameter]

ifname	:	SFP port interface name SFP port to show

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the status of the SFP module.

For each item, shows the current value, upper threshold value, and lower threshold value for each SFP port.

Item	Description
Temperature	Internal temperature of the module (°C)
Voltage	Voltage value (V)
Current	Current value (mA)
TX-Power	Strength of light produced (dBm)
RX-Power	Strength of light received (dBm)

[Example]

Show the status of the SFP module.

```
SWX3220#show ddm status
             Temperature  High Alarm   High Warning Low Warning  Low Alarm
Interface    (Celsius)    Threshold    Threshold    Threshold    Threshold
------------ ------------ ------------ ------------ ------------ ------------
 port1.25     42.7        100.0         85.0        -40.0        -55.0
 port1.26         -            -            -            -            -
 port1.27     40.7         95.0         90.0        -20.0        -25.0
 port1.28    Unsupported  Unsupported  Unsupported  Unsupported  Unsupported

             Voltage      High Alarm   High Warning Low Warning  Low Alarm
Interface    (V)          Threshold    Threshold    Threshold    Threshold
------------ ------------ ------------ ------------ ------------ ------------
 port1.25    3.37         3.62         3.46         3.13         2.97
 port1.26         -            -            -            -            -
 port1.27    3.34         3.89         3.70         2.89         2.70
 port1.28    Unsupported  Unsupported  Unsupported  Unsupported  Unsupported

             Current      High Alarm   High Warning Low Warning  Low Alarm
Interface    (mA)         Threshold    Threshold    Threshold    Threshold
------------ ------------ ------------ ------------ ------------ ------------
 port1.25      4.0         16.0         15.0          2.0          2.0
 port1.26         -            -            -            -            -
 port1.27      6.2         17.0         14.0          2.0          1.0
 port1.28    Unsupported  Unsupported  Unsupported  Unsupported  Unsupported

             TX-Power     High Alarm   High Warning Low Warning  Low Alarm
Interface    (dBm)        Threshold    Threshold    Threshold    Threshold
------------ ------------ ------------ ------------ ------------ ------------
 port1.25     -5.4806      0.4139       0.0000     -10.7058     -12.2184
 port1.26         -            -            -            -            -
 port1.27     -5.4714     -1.9997      -1.9997     -11.0237     -11.7392
 port1.28    Unsupported  Unsupported  Unsupported  Unsupported  Unsupported

             RX-Power     High Alarm   High Warning Low Warning  Low Alarm
Interface    (dBm)        Threshold    Threshold    Threshold    Threshold
------------ ------------ ------------ ------------ ------------ ------------
 port1.25     -7.5696      2.5527       0.0000     -16.9897     -40.0000
```

```
port1.26          -             -             -             -             -
port1.27     -8.7614       1.0002      -1.0017     -18.0134     -20.0000
port1.28    Unsupported  Unsupported  Unsupported  Unsupported  Unsupported
```

5.1.20 Set SFP module optical reception level monitoring

[Syntax]

sfp-monitor rx-power *action*
no sfp-monitor rx-power

[Parameter]

action : Operations for SFP module optical reception level monitoring

Setting value	Description
enable	Enables SFP module optical reception level monitoring
disable	Disables SFP module optical reception level monitoring

[Initial value]

sfp-monitor rx-power enable

[Input mode]

global configuration mode

[Description]

Sets the monitoring of SFP module optical reception levels.

[Example]

Disable SFP module optical reception level monitoring.

```
SWX3220(config)#sfp-monitor rx-power disable
```

5.1.21 Configuring transmission queue usage rate monitoring (system)

[Syntax]

tx-queue-monitor usage-rate *action*
no tx-queue-monitor usage-rate

[Parameter]

action : Configuration for system-wide transmission queue usage rate monitoring

Setting value	Description
enable	Enable system-wide transmission queue usage rate monitoring
disable	Disable system-wide transmission queue usage rate monitoring

[Initial value]

tx-queue-monitor usage-rate enable

[Input mode]

global configuration mode

[Description]

Enable or disable system-wide transmission queue usage rate monitoring.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

To enable transmission queue usage rate monitoring, in addition to this command, transmission queue usage rate monitoring must also be enabled on the interface.

[Example]

Disable system-wide transmission queue usage rate monitoring.

```
SWX3220(config)#tx-queue-monitor usage-rate disable
```

5.1.22 Configuring transmission queue usage rate monitoring (interface)

[Syntax]

tx-queue-monitor usage-rate *action*
no tx-queue-monitor usage-rate

[Parameter]

action : Configuration for transmission queue usage rate monitoring of the target interface

Setting value	Description
enable	Enable transmission queue usage rate monitoring of the target interface
disable	Disable transmission queue usage rate monitoring of the target interface

[Initial value]

tx-queue-monitor usage-rate enable

[Input mode]

interface mode

[Description]

Enable or disable transmission queue usage rate monitoring of the target interface.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can only be set for LAN/SFP port.

To enable transmission queue usage rate monitoring, in addition to this command, system-wide transmission queue usage rate monitoring must also be enabled.

[Example]

Disable transmission queue usage rate monitoring for LAN port #1.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#tx-queue-monitor usage-rate disable
```

5.1.23 Display configuration for transmission queue usage rate monitoring

[Syntax]

show tx-queue-monitor

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

Displays the transmission queue usage rate monitoring configuration.

The display details are as follows.

- Configuration for system-wide transmission queue usage rate monitoring
- Configuration by LAN/SFP port
  - Interface name (port)
  - Configure transmission queue usage rate monitoring for LAN/SFP port (usage-rate).

[Example]

Displays the transmission queue usage rate monitoring configuration.

```
SWX3220>show tx-queue-monitor
usage-rate: Enable

port      usage-rate
```

```
--------------------
port1.1       enable
port1.2       enable
port1.3       enable
port1.4       enable
port1.5       enable
port1.6       enable
port1.7      disable
   :            :
port2.1       enable
   :            :
```

5.2 Link aggregation

5.2.1 Set static logical interface

[Syntax]

static-channel-group *link-id*
no static-channel-group

[Parameter]

link-id : <1-96>

static logical interface number

[Input mode]

interface mode

[Description]

Associates the applicable interface with the static logical interface specified by *link-id*.

If this command is executed with the "no" syntax, the applicable interface is dissociated from the static logical interface.

[Note]

This command can be specified only for LAN/SFP port.

If a LAN/SFP port is associated to a *link-id* for which a static logical interface does not exist, the static logical interface is newly generated.

If the associated LAN/SFP port is no longer present because it was removed from the static logical interface, the static logical interface is deleted.

Up to eight LAN/SFP port units can be associated with one static logical interface.

If it is to be associated with an already-existing static logical interface, all of the following settings must match between the LAN/SFP port and the static logical interface. If the settings differ, an error occurs.

- VLAN setting
- Set QoS trust mode (including default CoS value and port priority)
- Set loop detection (enable/disable loop detection, enable/disable port blocking)

If a static logical interface is newly generated, the above settings of the LAN/SFP port are set to the default settings of the static logical interface.

If a LAN/SFP port is associated with a static logical interface, the MSTP settings return to the default values. The MSTP settings also return to the default values if the LAN/SFP port is removed from the static logical interface.

It is not possible to associate a single LAN/SFP port with multiple logical interface units. You must use the "no" syntax to first remove it before associating it with a different logical interface.

[Example]

Associate LAN port #1 with static logical interface #5.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#static-channel-group 5
```

5.2.2 Show static logical interface status

[Syntax]

show static-channel-group

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the static logical interface status.

The following items are shown for each static logical interface that exists.

- static logical interface name
- Load balance function rules
- Interface name of associated LAN/SFP port

For details on the load balance function rules, refer to the *type* parameter of the **port-channel load-balance** command.

[Example]

Show the static logical interface status.

```
SWX3220#show static-channel-group
% Static Aggregator: sa5
% Load balancing: src-dst-mac
% Member:
   port1.1
   port1.2
   port1.3
   port1.4
```

5.2.3 Set LACP logical interface

[Syntax]

channel-group *link-id* **mode** *mode*
no channel-group

[Parameter]

link-id : <1-127>

LACP logical interface number

mode : Operation mode

mode	**Description**
active	Operate LACP in active mode. In active mode, it actively sends LACP frames to the other device.
passive	Operate LACP in passive mode. In passive mode, it sends LACP frames only if LACP frames are received from the other device.

[Input mode]

interface mode

[Description]

Associates the applicable interface with the LACP logical interface specified by *link-id*.

If this command is executed with the "no" syntax, the applicable interface is dissociated from the LACP logical interface.

[Note]

This command can be specified only for LAN/SFP port.

If a LAN/SFP port is associated with a LACP logical interface, **lacp timeout long** command is specified for the corresponding LAN/SFP port.

If it is dissociated from the LACP logical interface, the **lacp timeout** command setting of the corresponding LAN/SFP port is deleted.

If you associate a LAN/SFP port to a *link-id* for which a LACP logical interface does not exist, the LACP logical interface is newly generated.

If the associated LAN/SFP port is no longer present because it was removed from the LACP logical interface, the LACP logical interface is deleted.

Up to twenty LAN/SFP port units can be associated with one LACP logical interface.

If up to eight associated LAN/SFP ports are combined into an LACP logical interface, they are immediately combined into the LACP logical interface; ports in excess of eight are standby ports used in case of a malfunction.

LAN/SFP port whose communication mode is half duplex do not support LACP link aggregation. (They can be assigned, but do not function as LACP link aggregation.)

If LAN/SFP port with different communication speeds are assigned to the same LACP logical interface, the operation depends on the settings for different-speed link aggregation. See the **lacp multi-speed** command for details.

If a LAN/SFP port is to be associated with an already-existing LACP logical interface, all of the following settings must match between the LAN/SFP port and the LACP logical interface. If the settings differ, an error occurs.

- Setting of VLAN
- Set QoS trust mode (including default CoS value and port priority)
- Loop detection settings (enable/disable loop detection, enable/disable port blocking)

If a LACP logical interface is newly generated, the above settings of the LAN/SFP port are set to the default settings of the LACP logical interface.

If a LAN/SFP port is associated with an LACP logical interface, the MSTP settings return to the default values.

The MSTP settings also return to the default values if the LAN/SFP port is removed from the LACP logical interface.

It is not possible to associate a single LAN/SFP port with multiple logical interface units.

You must use the "no" syntax to first remove it before associating it with a different logical interface.

[Example]

Associate LAN port #1 in ACTIVE mode with LACP logical interface #10.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#channel-group 10 mode active
```

5.2.4 Show LACP logical interface status

[Syntax]

show etherchannel [*ifname*]

[Parameter]

ifname : Interface name of the LAN/SFP port

Interfaces that make up the LACP logical interface

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

If *ifname* is omitted, shows the status of the LACP logical interface.

The following items are shown for each LACP logical interface that exists.

- LACP logical interface name
- Load balance function rules
- Interface name of associated LAN/SFP port

For details on the load balance function rules, refer to the *type* parameter of the **port-channel load-balance** command.

If *ifname* is specified, shows the status of the LAN/SFP port that make up the LACP logical interface.

The following items are shown.

Item	Description
Etherchannel portN.N	LAN/SFP port name
Physical admin key	Key that identifies physical characteristics (created from bandwidth, duplex, mru, and VLAN structure)
Receive machine state	Status of the LACP protocol Receive machine transition variable • "Invalid" • "Initialize" • "Port disabled" • "LACP disabled" • "Expired" • "Defaulted" • "Current"

Item	Description
Periodic Transmission machine state	Status of the LACP protocol Periodic Transmission transition variable • "Invalid" • "No periodic" • "Fast periodic" (transmitted at one-second intervals) • "Slow periodic" (transmitted at 30 second intervals) • "Periodic"
Mux machine state	Status of the LACP protocol Receive machine transition variable • "Detached" • "Waiting" • "Attached" • "Collecting/Distributing"
Selection	Usage status • "Selected" • "Unselectedic" • "Standby"
Information	Refer to the table below (Actor is self, Partner is other party)
Aggregator ID	Distinguishing ID on LACP

Information shows the following items.

Item	Description
LAG	LACP system ID (priority, MAC address)
Admin Key	ID that is the basis of the LACP key (logical port number)
Port priority	LACP port priority order
Ifindex	Interface number
Timeout	Timeout value ("Long"=90 seconds, "Short"=3 seconds)
Active	LACP operation mode("Active", "Passive")
Synchronized	Synchronization flag
Collecting	Collecting flag
Distributing	Distributing flag
Defaulted	Defaulted flag
Expired	Expired flag

[Example]

Shows the status of LACP logical interface.

```
SWX3220#show etherchannel
% Lacp Aggregator: po10
% Load balancing: src-dst-mac
% Member:
   port1.1
   port1.2
   port1.3
   port1.4
```

Shows the status of the LAN/SFP ports that make up the LACP logical interface.

```
SWX3220#show etherchannel port1.1
Etherchannel port1.1
 Physical admin key                          3
 Receive machine state                    Current
 Periodic Transmission machine state      Slow periodic
 Mux machine state                        Collecting/Distributing
 Selection                                Selected
```

```
Information    Actor                          Partner
 LAG           0x8000, 00-a0-de-e0-e0-e0      0x8000, 00-a0-de-11-11-11
 Admin Key       0001                           0001
 Port Priority  32768                          32768
 Ifindex         5001                           5001
 Timeout       Long                           Long
 Active             1                              1
 Synchronized       1                              1
 Collecting         1                              1
 Distributing       1                              1
 Defaulted          0                              0
 Expired            0                              0
```

5.2.5 Set LACP system priority order

[Syntax]

lacp system-priority *priority*
no lacp system-priority

[Parameter]

priority : <1-65535>

LACP system priority irder
Lower numbers have higher priority

[Initial value]

lacp system-priority 32768

[Input mode]

global configuration mode

[Description]

Sets the LACP system priority order.

If this command is executed with the "no" syntax, the setting returns to the default value.

[Note]

If an LACP logical interface is connected to the other device, the system priorities are compared, and control privilege is given to the device with the higher priority.

[Example]

Set the LACP system priority order to 100.

```
SWX3220(config)#lacp system-priority 100
```

5.2.6 Show LACP system priority

[Syntax]

show lacp sys-id

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the LACP system priority and the LACP system ID.

The following items are shown.

- LACP system priority (hexadecimal number starting with 0x)
- LACP system ID

[Note]

The LACP system priority can be set by the **lacp system-priority** command.

The LACP system ID is generated from the MAC address.

[Example]

Show the LACP system priority.

```
SWX3220>show lacp sys-id
% System 0x8000, 00-a0-de-e0-e0-e0
```

5.2.7 LACP different-speed link aggregation settings

[Syntax]

lacp multi-speed *switch*
no lacp multi-speed

[Parameter]

switch : Different-speed link aggregation function enable/disable settings

Setting value	Description
enable	Enabling different-speed link aggregation
disable	Disabling different-speed link aggregation

[Initial value]

lacp multi-speed disable

[Input mode]

global configuration mode

[Description]

Enables or disables different-speed link aggregation in an LACP.

If this command is executed with the "no" syntax, the setting returns to the default value.

[Note]

Operations when different-speed link aggregation is enabled

- All associated ports up to the maximum (eight ports) are set to active, regardless of communication speed.
- Load balancing is handled the same for all associated ports.
- If the opposing device does not accept a different communication speed, a list of associated ports is exchanged between this device and the opposing device, and the ports usable by both devices are enabled.

Operations when different-speed link aggregation is disabled

- Amongst the associated ports, only those with the same communication speed as the port initially linked up are made active.
  - Other ports with different communication speeds are left on standby.
  - When set to auto negotiation, only those ports amongst the associated ports with the same communication speed as that which resulted from the initial auto negotiation are made active.
- When the first group of linked-up ports all link down, the LACP logical interface also links down.

[Example]

This sets different-speed link aggregation to enabled.

```
SWX3220(config)#lacp multi-speed enable
```

5.2.8 Set LACP timeout

[Syntax]

lacp timeout *duration*

[Parameter]

duration : Specify the timeout

duration	Description
short	Sets the timeout to 3 seconds
long	Sets the timeout to 90 seconds

[Input mode]

interface mode

[Description]

Sets the LACP timeout.

[Note]

This command can be set only for a LAN/SFP port that is associated with an LACP logical interface.

If a LAN/SFP port is associated with an LACP logical interface, **lacp timeout long** command is specified for the corresponding LAN/SFP port.

If it is dissociated from the LACP logical interface, the **lacp timeout** command setting of the corresponding LAN/SFP port is deleted.

LACP timeout indicates the time since the last LACP frame received from the other device, after which it is determined that the link has gone down.

The LACP timeout setting is placed in a LACP frame and sent to the other device; after receiving this, the other device will transmit LACP frames at intervals of 1/3 of this LACP timeout.

The interval at which the device itself transmits LACP frames depends on the LACP timeout value inside the LACP frame sent from the other device.

[Example]

Set the LACP timeout of LAN port #1 to short.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#lacp timeout short
```

5.2.9 Clear LACP frame counters

[Syntax]

clear lacp [*link-id*] **counters**

[Parameter]

link-id	:	<1-127> LACP logical interface number

[Input mode]

privileged EXEC mode

[Description]

Clears the LACP frame counters.

If *link-id* is omitted, the frame counter of every existing LACP logical interface is cleared.

[Example]

Clear the frame counter for every LACP logical interface.

```
SWX3220#clear lacp counters
```

5.2.10 Show LACP frame counter

[Syntax]

show lacp-counter [*link-id*]

[Parameter]

link-id	:	<1-127> LACP logical interface number

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Show the LACP frame counter.

If *link-id* is omitted, the frame counter of every existing LACP logical interface is shown.

The following items are shown for each associated LAN/SFP port.

- LACP frames sent and received
- Marker protocol frames sent and received
- Error frames sent and received

[Example]

Show the frame counter for every LACP logical interface.

```
SWX3220#show lacp-counter
% Traffic statistics
Port       LACPDUs         Marker         Pckt err
        Sent    Recv    Sent    Recv    Sent    Recv
% Aggregator po1 , ID 4601
port1.1  297     298     0       0       0       0
port1.2  306     299     0       0       0       0
port1.3  305     298     0       0       0       0
port1.4  309     1350    0       0       0       0
port1.5  186     186     0       0       0       0
```

5.2.11 Set load balance function rules

[Syntax]

port-channel load-balance *type*
no port-channel load-balance

[Parameter]

type : Rules to specify the forwarding destination interface

type	Description
dst-ip	Destination IPv4/IPv6 address
dst-mac	Destination MAC address
dst-port	Destination TCP/UDP port number
src-dst-ip	Source and destination IPv4/IPv6 address
src-dst-mac	Source and destination MAC address
src-dst-port	Source and destination TCP/UDP port number
src-ip	Source IPv4/IPv6 address
src-mac	Source MAC address
src-port	Source TCP/UDP port number
rx-if	Receiving interface

[Initial value]

port-channel load-balance src-dst-mac

[Input mode]

global configuration mode

[Description]

Sets rules to specify the forwarding destination interface of the load balance function.

This uses the L2/L3/L4 information in the received frames to determine the forwarding destination.

Note that if a receiving interface is specified, the interface that always receives frames determines the forwarding destination.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command is a system-wide setting.

In the case of a frame that is not an IPv4/IPv6 packet, the forwarding destination interface is determined according to the forwarding source and destination MAC addresses, regardless of the rules that were specified.

[Example]

With the load balance function, set the system to determine the forwarding destination interface based on the transmission-source and destination IPv4/IPv6 address.

```
SWX3220(config)#port-channel load-balance src-dst-ip
```

5.2.12 Show protocol status of LACP logical interface

[Syntax]

show etherchannel status [*link-id*] [summary | detail]

[Keyword]

summary	:	Abbreviated display
detail	:	Detailed display

[Parameter]

link-id	:	<1-127> LACP logical interface number

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the status of the LACP logical interface specified by *link-id*.

If *link-id* is omitted, shows the status of all LACP logical interface.

If summary is specified, an abbreviated display is shown; if detail is specified, details are shown.

sIf both summary and detail are omitted, the result is as though summary was specified.

The following items are shown.

Item	Description
Aggregator	LACP logical interface
ID	Distinguishing ID on the LACP logical interface
Actor LAG	The actor's own LACP system ID (priority, MAC address)
Admin Key	The ID that is the basis of the actor's own LACP key (logical port number)
Status	Link aggregation status ("Not ready"/"Ready")
Partner LAG	The partner's LACP system ID (priority, MAC address)
Partner Key	The ID that is the basis of the partner's LACP key
Link count	Number of ports currently conveying data / Number of ports able to convey data
Link	List of the constituent LAN/SFP port (see table below for details)

Link shows the following items.

Usage status	Description
"Unselected"	Currently communicating with LACP control protocol.
"Selected"	Selected as a LAN/SFP port with LACP enabled.
"Standby"	Specified as a standby LAN/SFP port with LACP enabled.

Synchronization flag	Description
"no"	Synchronization flag is not set.
"yes"	Synchronization flag is set.

The state of the linked-up LAN/SFP ports are known from the usage status and the Synchronization flag.

Usage status	Synchronization	State of the linked-up LAN/SFP port
Unselected	no	Currently communicating with LACP control protocol.

Usage status	Synchronization	State of the linked-up LAN/SFP port
Selected	no	Selected as a LAN/SFP port with LACP enabled. Currently negotiating to combine for link aggregation.
Standby	no	Selected as a LAN/SFP port with LACP enabled, and specified as a standby port.
Selected	yes	Selected as a LAN/SFP port with LACP enabled. Combined as link aggregation,

[Example]

Show the status of the LACP logical interface.

```
SWX3220#show etherchannel status summary
Aggregator po1
 ID          4601
 Status       Ready
 Partner LAG  0x8000, 00-a0-de-11-11-11
 Partner Key    0001
 Link count    1/  1
Aggregator po2
 ID          4602
 Status       Not ready
 Partner LAG  0x8000, 00-a0-de-11-11-11
 Partner Key    0001
 Link count    0/  1
Aggregator po127
 ID          4727
 Status       Not ready
 Partner LAG  0x8000, 00-a0-de-11-11-11
 Partner Key    0001
 Link count    0/  1


SWX3220#show etherchannel status detail
Aggregator po1
 ID          4601
 Status       Ready
 Actor   LAG  0x8000, 00-a0-de-e0-e0-e0
 Admin Key      0001
 Partner LAG  0x8000, 00-a0-de-11-11-11
 Partner Key    0001
 Link count    1/  1
 Link
  port1.1     Selected     Synchronized  yes
Aggregator po2
 ID          4602
 Status       Ready
 Actor   LAG  0x8000, 00-a0-de-e0-e0-e0
 Admin Key      0002
 Partner LAG  0x8000, 00-a0-de-11-11-11
 Partner Key    0001
 Link count    0/  1
 Link
  port1.2     Selected     Synchronized  no
  port1.3     Unselected   Synchronized  no
Aggregator po127
 ID          4727
 Status       Ready
 Actor   LAG  0x8000, 00-a0-de-e0-e0-e0
 Admin Key      0127
 Partner LAG  0x8000, 00-a0-de-11-11-11
 Partner Key    0001
 Link count    0/  1
 Link
  port1.4     Selected     Synchronized  no
```

5.2.13 Set LACP port priority order

[Syntax]

lacp port-priority *priority*
no lacp port-priority

[Parameter]

priority	:	<1-65535>
		LACP port priority order
		Lower numbers have higher priority

[Initial value]

lacp port-priority 32768

[Input mode]

interface mode

[Description]

Sets the LACP port priority order.

If this command is executed with the "no" syntax, the setting returns to the default value.

[Note]

If up to eight LAN/SFP ports are combined into an LACP logical interface, they are immediately combined into the LACP logical interface; ports in excess of eight are standby ports used in case of a malfunction.

In such cases, the priority order between the LAN/SFP ports are evaluated, and they are combined starting with the highestpriority port.

The priority order is evaluated as follows.

1) Priority is given to ports with a lower LACP port priority.

2) If the LACP port priority is the same, priority is given to the lower interface number.

If an SFP port is to be given priority, its LACP port priority must be set lower than other ports.

[Example]

Set the LACP port priority order to 1024.

```
SWX3220(config-if)#channel-group 1 mode active
SWX3220(config-if)#lacp port-priority 1024
```

5.3 Port authentication

5.3.1 Configuring the IEEE 802.1X authentication function for the entire system

[Syntax]

aaa authentication dot1x
no aaa authentication dot1x

[Initial value]

no aaa authentication dot1x

[Input mode]

global configuration mode

[Description]

Enables IEEE 802.1X authentication for the entire system.

If this command is executed with the "no" syntax, disables IEEE 802.1X authentication for the entire system.

Use a RADIUS server for authentication on which the **radius-server host** command has been configured.

[Note]

In order to actually use IEEE 802.1X authentication, you need to enable IEEE 802.1X authentication on the applicable interface as well.(**dot1x port-control** command)

[Example]

Enable IEEE 802.1X authentication for the entire system.

```
SWX3220(config)#aaa authentication dot1x
```

5.3.2 Configuring the MAC authentication function for the entire system

[Syntax]

aaa authentication auth-mac
no aaa authentication auth-mac

[Initial value]

no aaa authentication auth-mac

[Input mode]

global configuration mode

[Description]

Enables MAC authentication for the entire system.

If this command is executed with the "no" syntax, disables MAC authentication for the entire system.

Use a RADIUS server for authentication on which the **radius-server host** command has been configured.

[Note]

In order to actually use MAC authentication, you need to enable MAC authentication on the applicable interface as well. (**auth-mac enable** command)

[Example]

Enable MAC authentication for the entire system.

```
SWX3220(config)#aaa authentication auth-mac
```

5.3.3 Configuring the Web authentication function for the entire system

[Syntax]

aaa authentication auth-web
no aaa authentication auth-web

[Initial value]

no aaa authentication auth-web

[Input mode]

global configuration mode

[Description]

Enables Web authentication for the entire system.

If this command is executed with the "no" syntax, Disables Web authentication for the entire system.

Use a RADIUS server for authentication on which the **radius-server host** command has been configured.

[Note]

In order to actually use Web authentication, you need to enable Web authentication on the applicable interface as well. (**auth-web enable** command)

[Example]

Enable Web authentication for the entire system.

```
SWX3220(config)#aaa authentication auth-web
```

5.3.4 Set operation mode for the IEEE 802.1X authentication function

[Syntax]

dot1x port-control *mode*
no dot1x port-control

[Parameter]

mode	:	Operation mode for IEEE 802.1X authentication

Operation mode	Description
auto	Operates as an authenticator for IEEE 802.1X authentication
force-authorized	Sets the authenticated port for IEEE 802.1X authentication to a fixed port
force-unauthorized	Sets the unauthenticated port for IEEE 802.1X authentication to a fixed port

[Initial value]

no dot1x port-control

[Input mode]

interface mode

[Description]

Configures the IEEE 802.1X authentication operation mode for the applicable interface.

If this command is executed with the "no" syntax, the IEEE 802.1X authentication function will be disabled for the applicable interface.

[Note]

This command can be specified only for both LAN/SFP port and logical interface.

[Example]

This command can be specified only for LAN/SFP port.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#dot1x port-control auto
```

5.3.5 Set for forwarding control on an unauthenticated port for IEEE 802.1X authentication

[Syntax]

dot1x control-direction *direction*
no dot1x control-direction

[Parameter]

direction : Sets the packet forwarding operation for unauthenticated ports

Forwarding operation	Description
both	Both send and receive packets are discarded.
in	Only receive packets are discarded.

[Initial value]

dot1x control-direction both

[Input mode]

interface mode

[Description]

Changes the packet forwarding operation for the applicable interface when the IEEE 802.1X authentication is unauthenticated.

If this command is executed with the "no" syntax, the setting returns to the default.

When "both" is specified, the packets received from the supplicant are discarded, and the broadcast/multicast packets to the interface to which the supplicant is connected from other ports are also discarded.

When "in" is specified, only packets received from the supplicant are discarded, and the broadcast/multicast packets to the interface to which the supplicant is connected from other ports are forwarded.

[Note]

This command can be specified only for both LAN/SFP port and logical interface.

If the host mode is set as multi-supplicant mode for the corresponding interface, or if it is used in conjunction with MAC authentication, the "in" setting is automatic.

When the guest VLAN is configured using the applicable interface, the settings for this command will be disabled.

Changing the settings for this command will make the authentication state return to the default.

To use this command, you must enable the port authentication function for the applicable interface. (**dot1x port-control** command)

[Example]

Discard received packets only for the packet forwarding operation on an unauthenticated port of LAN port #1.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#dot1x control-direction in
```

5.3.6 Set the EAPOL packet transmission count

[Syntax]

dot1x max-auth-req *count*
no dot1x max-auth-req

[Parameter]

count	:	<1-10>
		Maximum number of times EAPOL packets are transmitted

[Initial value]

dot1x max-auth-req 2

[Input mode]

interface mode

[Description]

Sets the maximum value for the EAPOL packet transmission count for the applicable interface.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be specified only for both LAN/SFP port and logical interface.

To use this command, you must enable the port authentication function for the applicable interface. (**dot1x port-control** command)

[Example]

Set the EAPOL packet transmission count for LAN port #1 to "3".

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#dot1x max-auth-req 3
```

5.3.7 Set the MAC authentication function

[Syntax]

auth-mac enable
auth-mac disable
no auth-mac

[Keyword]

enable	:	Enable MAC authentication
disable	:	Disable MAC authentication

[Initial value]

auth-mac disable

[Input mode]

interface mode

[Description]

Enables MAC authentication for the applicable interface.

When this command is executed with the "no" syntax or when disable is specified, MAC authentication is disabled.

[Note]

This command can be specified only for both LAN/SFP port and logical interface.

In order to actually use MAC authentication, you need to enable MAC authentication for the entire system as well. (**aaa authentication auth-mac** command)

[Example]

Enable the LAN port #1 MAC authentication function.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#auth-mac enable
```

5.3.8 Set MAC address format during MAC authentication

[Syntax]

auth-mac auth-user *type case*
no auth-mac auth-user

[Parameter]

type : Specify the format

Setting value	Format
hyphen	xx-xx-xx-xx-xx-xx
colon	xx:xx:xx:xx:xx:xx
unformatted	xxxxxxxxxxxx

case : Specify upper or lowercase

Setting value	Description
lower-case	Lower case(a～f)
upper-case	Upper case(A～F)

[Initial value]

auth-mac auth-user hyphen lower-case

[Input mode]

global configuration mode

[Description]

Changes the format of the user name and password used for authentication during MAC authentication.

During MAC authentication, the MAC address of the supplicant is used as a user name and password, and a request is sent to the RADIUS server for authentication.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

To use this command, you must enable the MAC authentication function for the applicable interface. (**auth-mac enable** command)

[Example]

Change the MAC address format used for MAC authentication to all uppercase format without hyphens.

```
SWX3220(config)#auth-mac auth-user unformatted upper-case
```

5.3.9 Configuring static registration for MAC authentication

[Syntax]

auth-mac static enable
auth-mac static disable
no auth-mac static

[Keyword]

enable : Enable static registration

disable	:	Disable static registration

[Initial value]

auth-mac static disable

[Input mode]

interface mode

[Description]

The MAC authentication feature registers the MAC address of a supplicant that has passed authentication as a static entry in the FDB.

Static registration is disabled when executed with the "no" syntax or when specified as disable.

[Note]

This command can only be set for LAN/SFP port and logical interface.

When the configuration of this command is changed, the authentication state returns to default.

Normally, MAC authentication is subject to aging timeout because it is registered as a dynamic entry in the FDB, but when this command is enabled, it is not subject to aging timeout because it is registered as a static entry.

Static registrations (authentication information) can be cleared with the **clear auth state** command or the **auth clear-state time** command.

To use this command, the MAC authentication function must be enabled on the target interface. (**auth-mac enable** command)

[Example]

Enable static registration of MAC authentication for LAN port #1.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#auth-mac static enable
```

5.3.10 Set the Web authentication function

[Syntax]

auth-web enable
auth-web disable
no auth-web

[Keyword]

enable	:	Enable Web authentication
disable	:	Disable Web authentication

[Initial value]

auth-web disable

[Input mode]

interface mode

[Description]

Enables Web authentication for the applicable interface.

When this command is executed with the "no" syntax or when disable is specified, Web authentication is disabled.

[Note]

This command can be specified only for both LAN/SFP port and logical interface.

In order to actually use Web authentication, you need to enable Web authentication for the entire system as well. (**aaa authentication auth-web** command)

You cannot enable the Web authentication function from any other mode besides multi-supplicant mode.

You cannot use this together with guest VLAN.

[Example]

Enable the LAN port #1 Web authentication function.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#auth-web enable
```

5.3.11 Set host mode

[Syntax]

auth host-mode *mode*
no auth host-mode

[Parameter]

mode : Operating mode for port authentication

Operation mode	Description
single-host	This mode allows communications for only one supplicant per port. Only the first supplicant that passes authentication is allowed.
multi-host	This mode allows communication with multiple supplicants for each port. If the first supplicant passes authentication, all other supplicants of the same port will be allowed to communicate without authentication.
multi-supplicant	This mode allows communication with multiple supplicants for each port. Communication is allowed or denied on a per-supplicant basis.

[Initial value]

auth host-mode single-host

[Input mode]

interface mode

[Description]

Changes the port authentication operation mode for the applicable interface.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be specified only for both LAN/SFP port and logical interface.

Changing the settings for this command will make the authentication state return to the default.

When using dynamic VLAN in multi-supplicant mode, the VLAN can be specified for individual supplicants.

When using dynamic VLAN in multi-host, the VLAN ID applied by the first supplicant will be applied to supplicants from the second onwards.

To use this command, you must enable the port authentication function for the applicable interface. (**dot1x port-control** command, **auth-mac enable** command, **auth-web enable** command)

[Example]

Change the LAN port #1 to multi supplicant mode.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#auth host-mode multi-supplicant
```

5.3.12 Configuring the authentication order

[Syntax]

auth order dot1x auth-mac
auth order auth-mac dot1x
no auth order

[Keyword]

dot1x : IEEE 802.1x authentication method

auth-mac : MAC authentication method

[Initial value]

auth order dot1x auth-mac

[Input mode]

interface mode

[Description]

Sets the order in which authentication occurs when authentication methods are used together in the port authentication function.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can only be set for LAN/SFP port and logical interface.

Regardless of this setting, Web authentication is performed when an ID/Password is entered on the Web authentication screen.

If the IEEE 802.1X authentication, MAC authentication, or Web authentication setting is disabled, that authentication method is not performed.

To use this command, the port authentication function must be enabled on the target interface. (**dot1x port-control** command,**auth-mac enable** command, **auth-web enable** command)

[Example]

Set the authentication method order for LAN port #1 as MAC authentication -> IEEE 802.1X authentication.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#auth order auth-mac dot1x
```

5.3.13 Set re-authentication

[Syntax]

auth reauthentication
no auth reauthentication

[Initial value]

no auth reauthentication

[Input mode]

interface mode

[Description]

Enables reauthentication of supplicants for the applicable interface.

If this is executed with the "no" syntax, the re-authentication is disabled.

When this setting is enabled, this periodically reauthenticates supplicants that have been successfully authenticated.

The reauthentication interval can be changed using the **auth timeout reauth-period** command.

[Note]

This command can be specified only for both LAN/SFP port and logical interface.

During IEEE 802.1X authentication, an EAPOL packet is transmitted to the supplicant at the timing for reauthentication to once again retrieve the user information, and an authentication request is sent to the RADIUS server.

During MAC authentication, the supplicant's MAC address is regarded as a user name and password at the timing for reauthentication, and a request is sent to the RADIUS server for authentication.

During Web authentication, the supplicant's authentication state is shifted to unauthorized at the timing of reauthentication.

To use this command, you must enable the port authentication function for the applicable interface. (**dot1x port-control** command, **auth-mac enable** command, **auth-web enable** command)

[Example]

Enable re-authenticatio of LAN port #1.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#auth reauthentication
```

5.3.14 Set dynamic VLAN

[Syntax]

auth dynamic-vlan-creation
no auth dynamic-vlan-creation

[Initial value]

no auth dynamic-vlan-creation

[Input mode]

interface mode

[Description]

Sets dynamic VLAN for the applicable interface.

If this is executed with the "no" syntax, the dynamic VLAN is disabled.

For interfaces on which dynamic VLAN is enabled, the associated VLAN is actively changed based on the property (Tunnel-Private-Group-ID) specified by the RADIUS server.

[Note]

This command can be specified only for both LAN/SFP port and logical interface.

Changing the settings for this command will make the authentication state return to the default.

When using dynamic VLAN in multi-supplicant mode, the VLAN can be specified for individual supplicants.

When using dynamic VLAN in multi-host, the VLAN ID applied by the first supplicant will be applied to supplicants from the second onwards.

To use this command, you must enable the port authentication function for the applicable interface. (**dot1x port-control** command, **auth-mac enable** command, **auth-web enable** command)

[Example]

Enable dynamic VLAN on LAN port #1.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#auth dynamic-vlan-creation
```

5.3.15 Set the guest VLAN

[Syntax]

auth guest-vlan *vlan-id*
no auth guest-vlan

[Parameter]

vlan-id	:	<1-4094>
		VLAN ID for guest VLAN

[Initial value]

no auth guest-vlan

[Input mode]

interface mode

[Description]

If the supplicant connected to the applicable interface is unauthorized or if authorization has failed, this specifies the guest VLAN to which the supplicant is associated.

If this command is executed with the "no" syntax, the guest VLAN setting is deleted.

[Note]

This command can be specified only for both LAN/SFP port and logical interface.

Changing the settings for this command will make the authentication state return to the default.

To use this command, you must enable the port authentication function for the applicable interface. (**dot1x port-control** command, **auth-mac enable** command)

This command cannot be set when Web authentication is enabled.

[Example]

This specifies guest VLAN #10 for LAN port #1.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#auth guest-vlan 10
```

5.3.16 Suppression period settings following failed authentication

[Syntax]

auth timeout quiet-period *time*

no auth timeout quiet-period

[Parameter]

time : <1-65535>

Period during which communication with a supplicant is refused after authentication fails (seconds)

[Initial value]

auth timeout quiet-period 60

[Input mode]

interface mode

[Description]

Sets the period during which authentication is suppressed for the applicable interface after authentication fails.

If this command is executed with the "no" syntax, the setting returns to the default.

All packets received during the authentication suppression period will be discarded.

[Note]

This command can be specified only for both LAN/SFP port and logical interface.

To use this command, you must enable the port authentication function for the applicable interface. (**dot1x port-control** command, **auth-mac enable** command, **auth-web enable** command)

[Example]

Set the suppression period for LAN port #1 to 300.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#auth timeout quiet-period 300
```

5.3.17 Set reauthentication interval

[Syntax]

auth timeout reauth-period *time*
no auth timeout reauth-period

[Parameter]

time : <300-86400>

Supplication reauthentication interval (seconds)

[Initial value]

auth timeout reauth-period 3600

[Input mode]

interface mode

[Description]

Sets the reauthentication interval of the supplicant for the applicable interface.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be specified only for both LAN/SFP port and logical interface.

To use this command, you must enable the port authorization function and the reauthentication function for the applicable interface. (**dot1x port-control** command, **auth-mac enable** command, **auth-web enable** command, **auth reauthentication** command)

[Example]

Set the reauthentication period for LAN port #1 to 1200.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#auth timeout reauth-period 1200
```

5.3.18 Set the reply wait time for the RADIUS server overall

[Syntax]

auth timeout server-timeout *time*

no auth timeout server-timeout

[Parameter]

time : <1-65535>

Reply wait time from the authentication server for the authentication request (seconds)

[Initial value]

auth timeout server-timeout 30

[Input mode]

interface mode

[Description]

Sets the reply wait time for the RADIUS server overall when authenticating a port of the applicable interface.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be specified only for both LAN/SFP port and logical interface.

The value for this setting must be at least equal to (setting of **radius-server timeout** command) x (setting of **radius-server retransmit** command + 1) x (number of radius servers).

To use this command, you must enable the port authentication function for the applicable interface. (**dot1x port-control** command, **auth-mac enable** command, **auth-web enable** command)

[Example]

This sets the reply wait time to the RADIUS server overall to 180 seconds, for authentication requests from LAN port #1.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#auth timeout server-timeout 180
```

5.3.19 Set supplicant reply wait time

[Syntax]

auth timeout supp-timeout *time*
no auth timeout supp-timeout

[Parameter]

time : <1-65535>

Supplicant reply wait time (seconds)

[Initial value]

auth timeout supp-timeout 30

[Input mode]

interface mode

[Description]

Sets the reply wait time from the supplicant during port authentication for the applicable interface.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be specified only for both LAN/SFP port and logical interface.

To use this command, you must enable the port authentication function for the applicable interface. (**dot1x port-control** command, **auth-mac enable** command, **auth-web enable** command)

[Example]

Set the reply wait time from the supplicant of LAN port #1 to 180 seconds.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#auth timeout supp-timeout 180
```

5.3.20 Set RADIUS server host

[Syntax]

radius-server host *host* [auth-port *port*] [timeout *time*] [retransmit *count*] [key *secret*]
no radius-server host

[Keyword]

auth-port	:	Sets the UDP port number used for authenticating the RADIUS server
timeout	:	Sets the reply standby time for requests sent to the RADIUS server
retransmit	:	Sets the number of times to resend the request to the RADIUS server
key	:	Sets the password used for communicating with the RADIUS server

[Parameter]

host	:	IPv4 address (A.B.C.D) or IPv6 address (X:X::X:X) When specifying an IPv6 link local address, the transmitting interface also needs to be specified (fe80::X%vlanN format).
port	:	<0-65535> UDP port number used for authentication (the default value of 1812 is used when this is omitted)
time	:	<1-1000> Reply standby time (in seconds; the settings for the radius-server timeout command--5 sec. at default are used if this is omitted)
count	:	<0-100> Number of times to resend (the settings for the radius-server retransmit command--3 times. at default are used if this is omitted)
secret	:	Single-byte alphanumeric characters, and single-byte symbols other than the characters '?' and spaces (128 characters or less) Shared password (the settings for the radius-server key command are used if this is omitted)

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Adds a server to the authentication server list.

The maximum number of entries is 8.

If this command is executed with the "no" syntax, this deletes the specified server from the authentication server list.

[Note]

The setting values should be adjusted so that the value of (setting value of **radius-server timeout** command) x (setting value of **radius-server retransmit** command + 1) x (number of RADIUS servers) is within the setting value of the **auth timeout server-timeout** command.

The **radius-server host** command configured with the LLDP auto-configuration feature is suffixed with the "dynamic" option that indicates it is a temporary setting. When the "dynamic" option is added, it will not be saved to the startup configuration even if the **write** command is executed.

[Example]

Add the server at IP address 192.168.100.100, with a reply standby time of 10 seconds and a number of times to resend requests of 5 seconds to the authentication server list.

```
SWX3220(config)#radius-server host 192.168.100.100 timeout 10 retransmit 5
```

Add the server at IP address 192.168.100.101, with an authentication UDP port of 1645 and a shared password of "abcde" to the authentication server list.

```
SWX3220(config)#radius-server host 192.168.100.101 auth-port 1645 key abcde
```

Adds the local RADIUS server to the authentication server list.

```
SWX3220(config)#radius-server host 127.0.0.1 key secret_local
```

5.3.21 Set the reply wait time for each RADIUS server

[Syntax]

radius-server timeout *time*
no radius-server timeout

[Parameter]

time : <1-1000>

Standby time for replying to requests (seconds)

[Initial value]

radius-server timeout 5

[Input mode]

global configuration mode

[Description]

Sets the reply wait time for each RADIUS server.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

If a server-specific wait time for replying to requests has been set using the **radius-server host** command, the **radius-server host** command settings are used.

The setting needs to be adjusted so that the value of (Setting of **radius-server timeout** command) x (Setting of **radius-server retransmit** command + 1) x (Number of RADIUS servers) falls within the number set in the auth timeout server-timeout command.

[Example]

Set the reply wait time for each RADIUS server to 10 seconds.

```
SWX3220(config)#radius-server timeout 10
```

5.3.22 Set number of times to resend requests to RADIUS server

[Syntax]

radius-server retransmit *count*
no radius-server retransmit

[Parameter]

count : <0-100>

Number of times to resend request

[Initial value]

radius-server retransmit 3

[Input mode]

global configuration mode

[Description]

Sets the number of times to resend requests to a RADIUS server.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

If a server-specific number of resends for requests has been set using the **radius-server host** command, the **radius-server host** command settings are used.

[Example]

Set the number of times to resend requests to a RADIUS server to 5.

```
SWX3220(config)#radius-server retransmit 5
```

5.3.23 Set RADIUS server shared password

[Syntax]

radius-server key *secret*
no radius-server key

[Parameter]

secret : Shared password

Single-byte alphanumeric characters, and single-byte symbols other than the characters '?' and spaces (128 characters or less)

[Initial value]

no radius-server key

[Input mode]

global configuration mode

[Description]

Sets the shared password used when communicating with a RADIUS server.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

If a server-specific shared password has been set using the **radius-server host** command, the **radius-server host** command settings are used.

[Example]

The shared password used with the RADIUS server is "abcde".

```
SWX3220(config)#radius-server key abcde
```

5.3.24 Set time of RADIUS server usage prevention

[Syntax]

radius-server deadtime *time*
no radius-server deadtime

[Parameter]

time : <0-1440>

RADIUS server usage prevention time (minutes)

[Initial value]

radius-server deadtime 0

[Input mode]

global configuration mode

[Description]

Sets the time during which the usage of the relevant server is prevented, when a request to the RADIUS server has timed out.

If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

This sets the usage prevention for the RADIUS server to 1 minute.

```
SWX3220(config)#radius-server deadtime 1
```

5.3.25 Set NAS-Identifier attribute sent to RADIUS server

[Syntax]

auth radius attribute nas-identifier *line*
no auth radius attribute nas-identifier

[Parameter]

line : Identifying text (253 characters or fewer)

The desired text string to be set as the NAS-Identifier attribute

[Initial value]

no auth radius attribute nas-identifier

[Input mode]

global configuration mode

[Description]

Specifies a desired text string that is sent as the NAS-Identifier attribute to the RADIUS server for port authentication.

If this setting is made, it is notified to RADIUS server as the NAS-Identifier attribute. If this setting is deleted, notification is stopped.

If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

Set "Nas-ID-001" as the NAS-Identifier attribute that is sent to the RADIUS server.

```
SWX3220(config)#auth radius attribute nas-identifier Nas-ID-001
```

5.3.26 Set RADIUS server authentication when no response

[Syntax]

auth no-response-authorized
no auth no-response-authorized

[Initial value]

no auth no-response-authorized

[Input mode]

global configuration mode

[Description]

When there is no response from the RADIUS server, operate as if authentication was successful.

If there is no response from the RADIUS server and a timeout occurred during IEEE802.1X authentication, MAC authentication and Web authentication, operate as if each of the authentication methods had succeeded.

To use this command, perform reauthentication settings with the **auth reauthentication** and **auth timeout reauth-period** commands.

By appropriately setting the reauthentication interval, you can put a limit on the temporarily authenticated and permitted state.

[Note]

Give careful consideration to your security policy when using this command, as this may create security-related problems.

The following actions are taken if this command is enabled and it is determined that there is no response from the RADIUS server.

- Permit authentication according to the authentication method used when the response from the RADIUS server timed out
- This may not operate correctly for IEEE802.1X authentication, depending on the specifications on the supplicant and so forth
- If multiple RADIUS servers are configured, consider authentication to have succeeded only when no response is received from any of the RADIUS servers
- Operate using the VLAN set for the port, even when using a dynamic VLAN
- As this authenticates and permits all supplicants, it does not work for guest VLANs
- If the RADIUS server host has not been set, authenticate will not succeed even when setting this command

[Example]

When there is no response from the RADIUS server, authentication is successful.

```
SWX3220(config)#auth no-response-authorized
```

5.3.27 Show port authentication information

[Syntax]

show auth status [interface *ifname*]

[Keyword]

interface	:	Show information for only a specified interface

[Parameter]

ifname	:	Interface name Interface to show

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the setting status for port authentication as well as the current authentication state.

[Example]

Show the port authentication information.

```
SWX3220#show auth status
[System information]
  802.1X Port-Based Authentication : Enabled
  MAC-Based Authentication         : Disabled
  WEB-Based Authentication         : Enabled

  Clear-state time : Not configured

  Redirect URL :
    Not configured

  Auth-web custom-file :
    There is no custom-file

  RADIUS server address :
    192.168.100.101 (port:1812)

[Interface information]
  Interface port1.1 (up)
    802.1X Authentication   : Auto (configured:auto)
    MAC Authentication      : Disabled (configured:disable)
    WEB Authentication      : Disabled (configured:disable)
    Host mode               : Single-host
    Dynamic VLAN creation   : Disabled
    Guest VLAN              : Disabled
    Reauthentication        : Disabled
    Reauthentication period : 60 sec
    MAX request             : 2 times
    Supplicant timeout      : 30 sec
    Quiet period            : 60 sec
    Controlled directions   : Both (configured:both)
    Protocol version        : 2
    Clear-state time        : Not configured
    Authentication status   : Authorized

  Interface port1.4 (down)
    802.1X Authentication   : Force Authorized (configured:-)
    MAC Authentication      : Disabled (configured:disable)
    WEB Authentication      : Enabled (configured:enable)
    Host mode               : Multi-supplicant
    Dynamic VLAN creation   : Disabled
    Guest VLAN              : Disabled
    Reauthentication        : Disabled
    Reauthentication period : 3600 sec
    MAX request             : 2 times
    Supplicant timeout      : 30 sec
    Server timeout          : 30 sec
    Quiet period            : 60 sec
    Controlled directions   : In (configured:both)
    Protocol version        : 2
    Clear-state time        : Not configured
```

5.3.28 Show supplicant information

[Syntax]

show auth supplicant [interface *ifname*]

[Keyword]

interface	:	Show information for only a specified interface

[Parameter]

ifname	:	Interface name Interface to show

[Input mode]

privileged EXEC mode

[Description]

Shows the supplicant information for port authentication.

[Example]

Show supplicant information for LAN port #1.

```
SWX3220#show auth supplicant interface port1.1
Port     MAC address       User name         Status          VLAN Method
-------- ----------------- ----------------- --------------- ---- ------
port1.1  0011.2233.4455    user              Authorized         1 802.1X
```

5.3.29 Show statistical information

[Syntax]

show auth statistics [interface *ifname*]

[Keyword]

interface	:	Shows statistical information for only the specified interface

[Parameter]

ifname	:	Interface name Interface to show

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows statistical information for packets during port authentication.

[Example]

Show statistical information for LAN port #1.

```
SWX3220#show auth statistics interface port1.1
Interface port1.1
  EAPOL frames:
    Received frames      : 11
      EAPOL Start        : 1
      EAPOL Logoff       : 0
      EAP Response ID    : 1
      EAP Response       : 9
      Invalid EAPOL      : 0
      EAP Length error   : 0
      Last EAPOL version : 1
      Last EAPOL source  : 0011.2233.4455
    Transmitted frames   : 11
      EAP Request ID     : 1
      EAP Request        : 9
      EAP Success        : 1
      EAP Fail           : 0

  RADIUS packets:
```

```
    Received packets     : 10
      Access Request     : 0
      Access Challenge   : 9
      Access Accept      : 1
      Access Reject      : 0
    Transmitted packets  : 10
      Access Request     : 10
```

5.3.30 Clear statistical information

[Syntax]

clear auth statistics [interface *ifname*]

[Keyword]

interface	:	Clears statistical information for only the specified interface

[Parameter]

ifname	:	Interface name Interface to show

[Input mode]

privileged EXEC mode

[Description]

Clears the packet statistical information during port authentication.

[Example]

Clear the statistical information for LAN port #1.

```
SWX3220#clear auth statistics interface port1.1
```

5.3.31 Show RADIUS server setting information

[Syntax]

show radius-server

[Input mode]

privileged EXEC mode

[Description]

Shows setting information related to the RADIUS server.

Shows setting information (server host, UDP port number for authentication, shared password, wait time for replying to requests, number of times to resend requests, server usage prevention time) for RADIUS servers registered in the authentication server list.

[Example]

Show setting information related to the RADIUS server.

```
SWX3220#show radius-server
Server Host : 192.168.100.101
  Authentication Port : 1812
  Secret Key          : abcde
  Timeout             : 10 sec
  Retransmit Count    : 5
  Deadtime            : 0 min

Server Host : 192.168.100.102
  Authentication Port : 1645
  Secret Key          : fghij
  Timeout             : 5 sec
  Retransmit Count    : 3
  Deadtime            : 0 min
```

5.3.32 Settings for redirect destination URL following successful Web authentication

[Syntax]

auth-web redirect-url *url*
no auth-web redirect-url

[Parameter]

url	:	Single-byte alphanumeric characters and single-byte symbols (maximum 255 characters) Redirect destination URL

[Initial value]

no auth-web redirect-url

[Input mode]

global configuration mode

[Description]

Specifies the URL to redirect to after successful Web authentication.
If this is executed with the "no" syntax, disables the redirect function after authentication.

[Note]

URLs that include question marks ("?") cannot be specified.

[Example]

Specify the redirect destination after successful Web authentication as http://192.168.100.200.

```
SWX3220(config)#auth-web redirect-url http://192.168.100.200
```

5.3.33 Clear the authentication state

[Syntax]

clear auth state [all] [interface *ifname*] [supplicant *mac-addr*]

[Keyword]

all	:	Clears the authentication state for all supplicants
interface	:	Clears the authentication state for supplicants connected to specific interfaces
supplicant	:	Clear the authentication state for specific supplicant

[Parameter]

ifname	:	Interfacee name Interface to clear
mac-addr	:	hhhh.hhhh.hhhh (h is hexadecimal) Applicable MAC address

[Input mode]

privileged EXEC mode

[Description]

Clears the supplicant authentication state.

[Example]

Clear the authentication state for supplicants connected to LAN port #1.

```
SWX3220#clear auth state interface port1.1
```

5.3.34 Setting the time for clearing the authentication state (system)

[Syntax]

auth clear-state time *time*
no auth clear-state time

[Parameter]

time	:	<0-23> Time at which the authentication state is cleared

[Initial value]

no auth clear-state time

[Input mode]

global configuration mode

[Description]

Sets the time at which the authentication state for the supplicant is cleared for the entire system.

If this command is executed with the "no" syntax, deletes the time setting for clearing the authentication state.

[Note]

If a time has been set to clear the interface authentication state, this will clear the authentication state at the time specified in the interface.

[Example]

This sets the time at which the authentication state for the supplicant is cleared for the entire system to 12:00.

```
SWX3220(config)#auth clear-state time 12
```

5.3.35 Setting the time for clearing the authentication state (interface)

[Syntax]

auth clear-state time *time*
no auth clear-state time

[Parameter]

time	:	<0-23> Time at which the authentication state is cleared

[Initial value]

no auth clear-state time

[Input mode]

interface mode

[Description]

Sets the time at which the authentication state of the supplicant is cleared for the applicable interface.

If this command is executed with the "no" syntax, deletes the time setting for clearing the authentication state.

[Note]

This command can be specified only for both LAN/SFP port and logical interface.

Even if a time has been set to clear the interface authentication state for the applicable interface system-wide, the authentication state will be cleared at the time specified by this command.

[Example]

This sets the time at which the authentication state of the supplicant connected to LAN port #1 is cleared to 12:00.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#auth clear-state time 12
```

5.3.36 Locate the file for customizing the Web authentication screen

[Syntax]

copy auth-web custom-file all *src_config_num dst_config_num*
copy auth-web custom-file *filename src_config_num dst_config_num*

[Keyword]

all	:	Copies the file for customizing all Web authentication screens

[Parameter]

filename	:	Single-byte alphanumeric characters and single-byte symbols Filename of the file for customizing the Web authentication screen
src_config_num	:	Copy source configuration number

Setting value	Description
0-1	Number of the start-up config
sd	SD card

dst_config_num : Copy destination configuration number

Setting value	Description
0−1	Number of the start-up config
sd	SD card

[Input mode]

privileged EXEC mode

[Description]

Copies the file for customizing all Web authentication screens.

[Note]

When copying the file for customizing the Web authentication screen from an SD card to the switch, put the respective files in the /[model name]/startup-config/web-auth/ folder on the SD card.

In a state in which the SD card is not mounted, executing this command on a config that is in the SD card produces an error.

[Example]

Copy all of the files for customizing the Web authentication screen from the SD card to startup configuration #0.

```
SWX3220#copy auth-web startup-config all sd 0
```

5.3.37 Delete the file for customizing the Web authentication screen

[Syntax]

erase auth-web custom-file all *config_num*
erase auth-web custom-file *filename config_num*

[Keyword]

all : Deletes the file for customizing all Web authentication screens

[Parameter]

filename : Single-byte alphanumeric characters and single-byte symbols

Filename of the file for customizing the Web authentication screen

config_num : Number of config

Setting value	Description
0-1	Number of the start-up config
sd	SD card

[Input mode]

privileged EXEC mode

[Description]

Deletes the file for customizing the Web authentication screen.

[Note]

In a state in which the SD card is not mounted, executing this command on a config that is in the SD card produces an error.

[Example]

Deletes logo.png from startup configuration #0.

```
SWX3220#erase auth-web startup-config logo.png 0
```

5.3.38 Set EAP pass through

[Syntax]

pass-through eap *switch*
no pass-through eap

[Parameter]

switch : Behavior EAP pass through

Setting value	Description
enable	Enable the EAP pass through
disable	Disable the EAP pass through

[Initial value]

pass-through eap enable

[Input mode]

global configuration mode

[Description]

Enables/disables EAP pass-through, specifying whether EAPOL frames are forwarded.

If "disable" is specified, EAP frames are discarded.

If this is executed with the "no" syntax, or if "enable" is specified, EAPOL frames are forwarded.

[Note]

For interfaces on which 802.1X authentication is enabled, authentication functionality is given priority, and EAP pass-through settings are not applied.

[Example]

Disable the EAP pass through.

```
SWX3220(config)#pass-through eap disable
```

5.4 Port security

5.4.1 Set port security function

[Syntax]

port-security enable
port-security disable
no port-security

[Keyword]

enable : Enables port security function

disable : Disables port security function

[Initial value]

port-security disable

[Input mode]

interface mode

[Description]

Enables the port security function for the applicable interface.

If this is executed with the "no" syntax, or disable is specified, port security will be disabled for the applicable interface.

[Note]

This command can be specified only for both LAN/SFP port and logical interface.

Any unregistered terminals will be discarded at the time when the port security function is enabled.

[Example]

Enable port security for LAN port #1.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#port-security enable
```

5.4.2 Register permitted MAC addresses

[Syntax]

port-security mac-address
no port-security mac-address

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Registers MAC addresses that are allowed to communicate on ports for which port security has been enabled.

If this command is executed with the "no" syntax, deletes the registered address.

[Example]

Register MAC address 00:A0:DE:00:00:01 as a permitted address for LAN port #1.

```
SWX3220(config)#port-security mac-address 00a0.de00.0001 forward port1.1 vlan 1
```

5.4.3 Set operations used for security violations

[Syntax]

port-security violation *action*
no port-security violation

[Parameter]

action : Operation used for port security violations

Operation mode	Description
discard	Discards packets
shutdown	Shuts down the port

[Initial value]

port-security violation discard

[Input mode]

interface mode

[Description]

Sets the action to be taken during a port security violation for the applicable interface.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

When restoring ports in shutdown mode that have been shut down, use the no shutdown command.

This command can be specified only for both LAN/SFP port and logical interface.

[Example]

Change the operation used for a violation on LAN port #1 to "port shutdown."

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#port-security violation shutdown
```

5.4.4 Show port security information

[Syntax]

show port-security status

[Input mode]

privileged EXEC mode

[Description]

Shows the port security information.

[Example]

Show the port security information.

```
SWX3220#show port-security status
 Port     Security  Action    Status    Last violation
 -------- --------- --------- --------- -----------------
 port1.1  Enabled   Discard   Blocking  00a0.de00.0003
 port1.2  Disabled  Discard   Normal
 port1.3  Disabled  Discard   Normal
 port1.4  Disabled  Discard   Normal
 port1.5  Disabled  Discard   Normal
 port1.6  Disabled  Discard   Normal
 port1.7  Disabled  Discard   Normal
 port1.8  Disabled  Discard   Normal
 port1.9  Disabled  Discard   Normal
 port1.10 Disabled  Discard   Normal
```

5.5 Error detection function

5.5.1 Set automatic recovery from errdisable state

[Syntax]

errdisable auto-recovery *function* [interval *interval*]
no errdisable auto-recovery *function*

[Keyword]

interval : Automatic recovery time setting

[Parameter]

function : Functions that can be the cause of errdisable

Setting value	Description
bpduguard	BPDU guard function
loop-detect	Loop detection function

interval : <10-1000000>

Time (seconds) until auto-recovery

[Initial value]

no errdisable auto-recovery bpduguard (BPDU guard function)

errdisable auto-recovery loop-detect interval 300 (Loop detection function)

[Input mode]

global configuration mode

[Description]

Enables the function that automatically recovers after the error detection function causes the errdisable state, and specifies the time until automatic recovery.

If interval is omitted, 300 seconds is specified.

this is executed with the "no" syntax, the automatic recovery function is disabled.

[Note]

For a LAN/SFP port that was put in the errdisable state by the BPDU guard function before this command was executed, the change in the setting is applied the next time BPDU is detected.

[Example]

Enable automatic recovery after BPDU guard has caused the errdisable state, and set the recovery time to 600 seconds.

```
SWX3220(config)#errdisable auto-recovery bpduguard interval 600
```

Disable automatic recovery after loop detection has caused the errdisable state.

```
SWX3220(config)#no errdisable auto-recovery loop-detect
```

5.5.2 Show error detection function information

[Syntax]

show errdisable

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows information for the error detection function.

The following items are shown.

- Whether automatic recovery from the errdisable state is enabled or disabled
- The interface that is in the errdisable state, and the function that detected the error

[Example]

Show information for the error detection function.

```
SWX3220>show errdisable

function        auto recovery          interval
----------------------------------------------
BPDU guard      disable
Loop detect     enable                      300
Port-security   disable

port            reason
----------------------------
port1.1         BPDU guard
port1.7         Loop detect
sa1             Loop detect
```

Chapter 6

Layer 2 functions

6.1 FDB (Forwarding Data Base)

6.1.1 Set MAC address acquisition function

[Syntax]

mac-address-table learning enable
mac-address-table learning disable
no mac-address-table learning

[Keyword]

enable	:	Enables MAC address learning function
disable	:	Disables MAC address learning function

[Initial value]

mac-address-table learning enable

[Input mode]

global configuration mode

[Description]

Enables/disables the MAC address learning function.

If this is executed with the "no"syntax, the MAC address acquisition function is enabled.

[Note]

If the MAC address acquisition function is disabled, a dynamic entry is not registered in the MAC address table even if a frame is received.

[Example]

Enable the MAC address acquisition function.

```
SWX3220(config)#mac-address-table learning enable
```

6.1.2 Set dynamic entry ageing time

[Syntax]

mac-address-table ageing-time *time*
no mac-address-table ageing-time

[Parameter]

time	:	<10-400>
		Ageing time (seconds)

[Initial value]

mac-address-table ageing-time 300

[Input mode]

global configuration mode

[Description]

Sets the dynamic entry ageing time.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

In some cases, there might be a discrepancy between the time specified by this command and the time until the dynamic entry is actually deleted from the MAC address table.

[Example]

Set the dynamic entry ageing time to 400 seconds.

```
SWX3220(config)#mac-address-table ageing-time 400
```

6.1.3 Clear dynamic entry

[Syntax]

clear mac-address-table dynamic
clear mac-address-table dynamic address *mac-addr*
clear mac-address-table dynamic vlan *vlan-id*
clear mac-address-table dynamic interface *ifname* [instance *inst*]

[Keyword]

address	:	Specifies the MAC address
vlan	:	Specifies the VLAN ID
interface	:	Specifies the interface
instance	:	Specifies the MST instance

[Parameter]

mac-addr	:	hhhh.hhhh.hhhh (h is hexadecimal) Applicable MAC address
ifname	:	Name of LAN/SFP port or logical interface Applicable interface
vlan-id	:	<1-4094> Applicable VLAN ID
inst	:	<1-63> Applicable MST instance ID

[Input mode]

privileged EXEC mode

[Description]

Deletes a dynamic entry from the MAC address table.

If a keyword is specified, only the entries that match the applicable conditions are deleted.

If no keyword is specified, all dynamic entries are deleted.

[Example]

Delete the dynamic entry whose MAC address is 00a0.de11.2233.

```
SWX3220#clear mac-address-table dynamic address 00a0.de11.2233
```

6.1.4 Set static entry

[Syntax]

mac-address-table static *mac-addr action ifname* [vlan *vlan-id*]
no mac-address-table static *mac-addr action ifname* [vlan *vlan-id*]

[Keyword]

vlan	:	Specifies the VLAN ID

[Parameter]

mac-addr	:	hhhh.hhhh.hhhh (h is hexadecimal) Applicable MAC address
action	:	Action applied to frames addressed to mac-addr

Setting value	Description
forward	Forward
discard	Discard

ifname : Name of LAN/SFP port or logical interface

Applicable interface

vlan-id : <1-4094>

Applicable VLAN ID

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Registers a static entry in the MAC address table.

If

action is specified as "forward," received frames that match the specified MAC address and VLAN ID are forwarded to the specified interface.
If *action* is specified as "discard," received frames that match the specified MAC address and VLAN ID are discarded.

If this command is executed with the "no" syntax, the static entry is deleted from the MAC address table.

If "vlan" is omitted, VLAN #1 is specified.

[Note]

If *action* is specified as "discard," a multicast MAC address cannot be specified as *mac-addr*.

The following MAC addresses cannot be specified as *mac-addr*.

- 0000.0000.0000
- 0100.5e00.0000 - 0100.5eff.ffff
- 0180.c200.0000 - 0180.c200.000f
- 0180.c200.0020 - 0180.c200.002f
- ffff.ffff.ffff

[Example]

Specify that frames addressed to 00a0.de11.2233 are forwarded to LAN port #2.

```
SWX3220(config)#mac-address-table static 00a0.de11.2233 forward port1.2
```

6.1.5 Show MAC address table

[Syntax]

show mac-address-table

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the MAC address table.

The following items are shown.

- VLAN ID
- Interface name
- MAC address
- Action applied to frames
- Entry type
- Ageing time

[Example]

Show the MAC address table.

```
SWX3220>show mac-address-table
VLAN  port      mac             fwd      type     timeout
   1  port1.1   00a0.de11.2233  forward  static        0
   1  sa1       1803.731e.8c2b  forward  dynamic     300
   1  sa2       782b.cbcb.218d  forward  dynamic     300
```

6.1.6 Show number of MAC addresses

[Syntax]

show mac-address-table count
show mac-address-table count interface *ifname*
show mac-address-table count vlan *vlan-id*

[Keyword]

interface	:	Show the number of MAC addresses for only a specified interface
vlan	:	Show the number of MAC addresses for only a specific VLAN

[Parameter]

ifname	:	Name of interface to show Only LAN/SFP port or logical interface can be specified
vlan-id	:	<1-4094> VLAN ID to show

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the number of MAC addresses that are registered in the FDB entries.

The number of dynamic addresses registered by automatic learning and of manually registered static addresses are shown.

[Example]

Show the number of MAC addresses that are registered in the FDB entries.

```
SWX3220>show mac-address-table count
 MAC Entries for all vlans
  Dynamic Address   : 20
  Static Address    : 10
  Total MAC Address : 30
```

6.2 VLAN

6.2.1 Move to VLAN mode

[Syntax]

vlan database

[Input mode]

global configuration mode

[Description]

Moves to VLAN mode in order to make VLAN interface settings.

[Note]

To return from VLAN mode to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

[Example]

Move to VLAN mode.

```
SWX3220(config)#vlan database
SWX3220(config-vlan)#
```

6.2.2 Set VLAN interface

[Syntax]

vlan *vlan-id* [name *name*] [state *state*]
no vlan *vlan-id*

[Keyword]

name	:	Specifies the name of the VLAN
state	:	Specifies the state of the VLAN

[Parameter]

vlan-id : <2-4094>

VLAN ID

name : Single-byte alphanumeric characters and single-byte symbols(32characters or less)

Name of the VLAN

state : Whether frame forwarding is enabled or disabled

Setting value	Description
enable	Frames are forwarded
disable	Frames are not forwarded

[Initial value]

none

[Input mode]

VLAN mode

[Description]

Sets the VLAN interface.

If this command is executed with the "no" syntax, the VLAN interface is deleted.

If "name" is omitted, the VLAN name "VLANxxxx" (xxxx is the four-digit VLAN ID) is automatically specified. Note that names that are automatically specified do not show up in the configuration.

If "state" is omitted, "enable" is specified.

If "disable" is specified, all settings of the VLAN interface are deleted.

[Note]

If this command is executed with "name" omitted for a VLAN ID for which *name* is already specified, the already-specified *name* is not changed.

Multiple VLAN IDs can be specified for *vlan-id*. Use "-" or "," as shown below.

- To select from VLAN #2 through VLAN #4 : 2-4
- To select VLAN #2 and VLAN #4 : 2,4

The way that *name* is handled when multiple VLAN IDs are specified is as follows.

- When a name is specified, the same name is set for all multiple VLANs.
- When a name is not specified, the VLAN name with the name omitted is set for all multiple VLANs.

[Example]

Set VLAN #1000 with the name "Sales".

```
SWX3220(config-vlan)#vlan 1000 name Sales
```

6.2.3 Set private VLAN

[Syntax]

private-vlan *vlan-id type*
no private-vlan *vlan-id type*

[Parameter]

vlan-id : <2-4094>

VLAN ID set by the **vlan** command

type : Type of private VLAN

Setting value	Description
primary	Primary VLAN
community	Secondary VLAN (community VLAN)
isolated	Secondary VLAN (isolated VLAN)

[Initial value]

none

[Input mode]

VLAN mode

[Description]

Uses *vlan-id* as a private VLAN.

If this command is executed with the "no" syntax, the private VLAN setting is deleted, and it is used as a conventional VLAN.

[Note]

If this is set as a community VLAN, it can communicate with the promiscuous port of the primary VLAN and with another interface that is associated with the same community VLAN, but cannot communicate with a different community VLAN or with an interface that is associated with an isolated VLAN.

If this is set as an isolated VLAN, it can communicate with the promiscuous port of the primary VLAN, but cannot communicate with the community VLAN or with another interface that is associated with an isolated VLAN.

[Example]

Set the following private VLANs.

- VLAN #100 : Primary VLAN
- VLAN #101 : Secondary VLAN (community VLAN)
- VLAN #102 : Secondary VLAN (community VLAN)
- VLAN #103 : Secondary VLAN (isolated VLAN)

```
SWX3220(config-vlan)#vlan 100
SWX3220(config-vlan)#vlan 101
SWX3220(config-vlan)#vlan 102
SWX3220(config-vlan)#vlan 103
SWX3220(config-vlan)#private-vlan 100 primary
SWX3220(config-vlan)#private-vlan 101 community
SWX3220(config-vlan)#private-vlan 102 community
SWX3220(config-vlan)#private-vlan 103 isolated
```

6.2.4 Set secondary VLAN for primary VLAN

[Syntax]

private-vlan *vlan-id* **association** add *2nd-vlan-ids*
private-vlan *vlan-id* **association** remove *2nd-vlan-ids*
no private-vlan *vlan-id* **association**

[Keyword]

add : Associate the specified VLAN

remove : Remove the association of the specified VLAN

[Parameter]

vlan-id : <2-4094>

VLAN ID specified for the primary VLAN

2nd-vlan-ids : <2-4094>

VLAN ID specified for the secondary VLAN

To specify multiple items, use "-" or "," as shown below

- To select from VLAN #2 through VLAN #4: 2-4
- To select VLAN #2 and VLAN #4: 2,4

[Initial value]

none

[Input mode]

VLAN mode

[Description]

Specify the association of the secondary VLAN (isolated VLAN, community VLAN) with the primary VLAN of the private VLAN.

By specifying "add," specify the association of the *vlan-id* with the *2nd-vlan-ids*.

By specifying "remove," remove the association of the *vlan-id* and the *2nd-vlan-ids*.

If this command is executed with the "no" syntax, all associations to the primary VLAN are deleted.

[Example]

After specifying the following private VLAN, associate the secondary VLANs to the primary VLAN.

- VLAN #100 : Primary VLAN
- VLAN #101 : Secondary VLAN (community VLAN)
- VLAN #102 : Secondary VLAN (community VLAN)
- VLAN #103 : Secondary VLAN (isolated VLAN)

```
SWX3220(config-vlan)#vlan 100
SWX3220(config-vlan)#vlan 101
SWX3220(config-vlan)#vlan 102
SWX3220(config-vlan)#vlan 103
SWX3220(config-vlan)#private-vlan 100 primary
SWX3220(config-vlan)#private-vlan 101 community
SWX3220(config-vlan)#private-vlan 102 community
SWX3220(config-vlan)#private-vlan 103 isolated
SWX3220(config-vlan)#private-vlan 100 association add 101
SWX3220(config-vlan)#private-vlan 100 association add 102
SWX3220(config-vlan)#private-vlan 100 association add 103
```

6.2.5 Set access port (untagged port)

[Syntax]

switchport mode access

[Initial value]

switchport mode access

[Input mode]

interface mode

[Description]

Specifies the port type of the applicable interface as an access port.

[Note]

This command can be specified only for LAN/SFP port and logical interface.

If this command is applied to a logical interface, the settings of every LAN/SFP port associated with that interface are changed.

If the port type is changed from a trunk port to an access port, the setting of the **switchport trunk allowed vlan** command and the **switchport trunk native vlan** command return to their default settings.

To specify the VLAN that is associated as an access port, use the **switchport access vlan** command.

[Example]

Set LAN port #1 as an access port.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#switchport mode access
```

6.2.6 Set associated VLAN of an access port (untagged port)

[Syntax]

switchport access vlan *vlan-id*
no switchport access vlan

[Parameter]

vlan-id : <1-4094>
Associated VLAN ID

[Initial value]

switchport access vlan 1

[Input mode]

interface mode

[Description]

Sets the VLAN ID that is associated as an access port with the applicable interface.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be set only for a LAN/SFP port or logical interface for which the **switchport mode access** command is set.

If this command is applied to a logical interface, the settings of every LAN/SFP port associated with that interface are changed.

If the port type is changed to a trunk port, the setting of this command returns to the default setting.

[Example]

Set VLAN #10 as the VLAN to which LAN port #1 is associated as the access port.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#switchport access vlan 10
```

6.2.7 Set trunk port (tagged port)

[Syntax]

switchport mode trunk [ingress-filter *action*]

[Keyword]

ingress-filter : Specifies the behavior of the ingress filter

[Parameter]

action : Behavior of the ingress filter

Setting value	Description
enable	Enable the ingress filter
disable	Disable the ingress filter

[Initial value]

none

[Input mode]

interface mode

[Description]

Specifies the port type of the applicable interface as an trunk port.

If "ingress-filter" is omitted, "enable" is specified.

If ingress filtering is enabled, frames are forwarded only if the VLAN ID of the received frame matches the VLAN associated with the interface.

If ingress filtering is disabled, all frames are forwarded.

[Note]

This command can be specified only for LAN/SFP port and logical interface.

If this command is applied to a logical interface, the settings of every LAN/SFP port associated with that interface are changed.

If the port type is changed from an access port to a trunk port, the setting of the **switchport access vlan** command returns to the default setting.

To specify the VLAN ID that is associated as a trunk port, use the **switchport trunk allowed vlan** command. To specify the native VLAN, use the **switchport trunk native vlan** command.

[Example]

Set LAN port #1 as a trunk port.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#switchport mode trunk
```

6.2.8 Set associated VLAN for trunk port (tagged port)

[Syntax]

switchport trunk allowed vlan all
switchport trunk allowed vlan none
switchport trunk allowed vlan add *vlan-ids*
switchport trunk allowed vlan except *vlan-ids*
switchport trunk allowed vlan remove *vlan-ids*
no switchport trunk

[Keyword]

all	:	vlanAssociate to all VLANs that are set by the vlan command
none	:	Dissociate from all VLANs
add	:	Associate to the specified VLAN
except	:	Associate to all VLANs that are set by the vlan command except for the specified
remove	:	Dissociate from the specified VLAN

[Parameter]

vlan-ids : <1-4094>

VLAN ID set by the **vlan** command

To specify multiple items, use "-" or "," as shown below

- To select from VLAN #2 through VLAN #4: 2-4
- To select VLAN #2 and VLAN #4: 2,4

[Initial value]

none

[Input mode]

interface mode

[Description]

Sets the VLAN ID that is associated as a trunk port with the applicable interface.

If this is executed with the "no" syntax, all associated VLAN IDs are deleted and the port type is changed to access port.

[Note]

This command can be set only for a LAN/SFP port or logical interface for which the **switchport mode trunk** command is set.

If this command is applied to a logical interface, the settings of every LAN/SFP port associated with that interface are changed.

If the port type is changed to access port, the setting of this command returns to the default setting.

If this is set with "all" or "except" specified, the content of a subsequently changed **vlan** command is always applied.

If this is set with "all" or "except" specified, making the following settings will change the remaining affiliated VLAN IDs to the settings that were specified by "add."

- If you specify "remove" to delete a VLAN ID that is associated
- If you use the **switchport trunk native vlan** command to specify an associated VLAN ID

If you make this setting with "except" specified, and then associate the VLAN ID that had been excluded by specifying "add", the associated VLAN ID is changed to the setting specified by "add".

If you specify "remove" and then specify an unassociated VLAN ID, an error occurs.

For the setting of this command and the **switchport trunk native vlan** command, the last-specified command takes priority.

- If you use the **switchport trunk native vlan** command to specify a VLAN ID that was associated by this command, it is removed from the specified VLAN ID.
- If you specify and associate a VLAN ID that was set by the **switchport trunk native vlan** command, **switchport trunk native vlan none** is set.

If you specify the **switchport trunk allowed vlan add** command with a combination of "-" or "," in the *vlan-ids*, the command setting will fail if you revert to an older version (Rev.2.00.08 or earlier). As a result, normal communication might become impossible. (Example setting: switchport trunk allowed vlan add 101,103-105)

[Example]

Set LAN port #1 as the trunk port, and associate it to VLAN #2.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#switchport mode trunk
SWX3220(config-if)#switchport trunk allowed vlan add 2
```

6.2.9 Set native VLAN for trunk port (tagged port)

[Syntax]

switchport trunk native vlan *vlan-id*
switchport trunk native vlan none
no switchport trunk native vlan

[Keyword]

none	:	Disables the native VLAN

[Parameter]

vlan-id	:	<1-4094> VLAN ID set by the **vlan** command

[Initial value]

switchport trunk native vlan 1

[Input mode]

interface mode

[Description]

Sets the native VLAN for the applicable interface.

If "none" is specified, the native VLAN is disabled. This means that untagged frames received by the applicable interface are discarded.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be set only for a LAN/SFP port or logical interface for which the **switchport mode trunk** command is set.

If this command is applied to a logical interface, the settings of every LAN/SFP port associated with that interface are changed.

If the port type is changed to access port, the setting of this command returns to the default setting.

For the setting of this command and the setting of the **switchport trunk allowed vlan** command, the last-specified command takes priority.

- If you use the **switchport trunk allowed vlan** command to specify the associated VLAN ID, and then specify this command, it is removed from the specified VLAN ID.
- If the VLAN ID specified by this command is associated using the **switchport trunk allowed vlan** command, **switchport trunk native vlan none** is specified.

[Example]

Set LAN port #1 as the trunk port, and specify VLAN #2 as the native VLAN.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#switchport mode trunk
SWX3220(config-if)#switchport trunk native vlan 2
```

6.2.10 Set private VLAN port type

[Syntax]

switchport mode private-vlan *port-type*
no switchport mode private-vlan *port-type*

[Parameter]

port-type : Port mode

Setting value	Description
promiscuous	Promiscuous port
host	Host port

[Initial value]

none

[Input mode]

interface mode

[Description]

Specifies the private VLAN port type for the applicable interface.

If this is executed with the "no" syntax, the setting of the private VLAN specified for the applicable interface is deleted.

[Note]

This command can be set only for a LAN/SFP port for which the **switchport mode access** command is set.

In addition, promiscuous can be specified for the following interfaces.

- Interface that is operating as a trunk port
- logical interface

[Example]

Set LAN port #1 as a promiscuous port, and LAN port #2 as a host port.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#switchport mode private-vlan promiscuous
SWX3220(config-if)#exit
SWX3220(config)#interface port1.2
SWX3220(config-if)#switchport mode private-vlan host
```

6.2.11 Set private VLAN host port

[Syntax]

switchport private-vlan host-association *pri-vlan-id* add *2nd-vlan-id*
no switchport private-vlan host-association

[Keyword]

add : Sets the secondary VLAN for the primary VLAN

[Parameter]

pri-vlan-id : <2-4094>

VLAN ID specified as the primary VLAN

2nd-vlan-id : <2-4094>

VLAN ID specified as the secondary VLAN

[Initial value]

none

[Input mode]

interface mode

[Description]

Specifies the primary VLAN that is associated as the host port of the private VLAN for the applicable interface, and associates the secondary VLAN.

If this is executed with the "no" syntax, the setting of the primary VLAN associated as the host port of the applicable interface, and the association of the secondary VLAN, are deleted.

[Note]

This command can be set only for a LAN/SFP port that has been set as the host port by the **switchport mode private-vlan** command.

pri-vlan-id and *2nd-vlan-id* must be associated by the **private-vlan association** command.

If the **switchport mode private-vlan** command is used to set the port type to something other than host port, the setting of this command is deleted.

[Example]

Specify the following private VLAN for each interface.

- LAN port #1 : Primary VLAN #100, Secondary VLAN #101
- LAN port #2 : Primary VLAN #100, Secondary VLAN #102
- LAN port #3 : Primary VLAN #100, Secondary VLAN #103

```
SWX3220(config)# interface port1.1
SWX3220(config-if)# switchport mode private-vlan host
SWX3220(config-if)# switchport private-vlan host-association 100 add 101
SWX3220(config-if)# interface port1.2
SWX3220(config-if)# switchport mode private-vlan host
SWX3220(config-if)# switchport private-vlan host-association 100 add 102
SWX3220(config-if)# interface port1.3
SWX3220(config-if)# switchport mode private-vlan host
SWX3220(config-if)# switchport private-vlan host-association 100 add 103
```

6.2.12 Set promiscuous port for private VLAN

[Syntax]

switchport private-vlan mapping *pri-vlan-id* add *2nd-vlan-ids*
switchport private-vlan mapping *pri-vlan-id* remove *2nd-vlan-ids*
no switchport private-vlan mapping

[Keyword]

add	:	Sets the secondary VLAN for the primary VLAN
remove	:	Deletes the secondary VLAN for the primary VLAN

[Parameter]

pri-vlan-id	:	<2-4094> VLAN ID specified as the primary VLAN
2nd-vlan-ids	:	<2-4094> VLAN ID specified as the secondary To specify multiple items, use "-" or "," as shown below • To select from VLAN #2 through VLAN #4: 2-4 • select VLAN #2 and VLAN #4: 2,4

[Initial value]

none

[Input mode]

interface mode

[Description]

Specifies the primary VLAN that is associated with the applicable interface as the promiscuous port, and associates the secondary VLAN.

If this is executed with the "no" syntax, the setting of the primary VLAN that is associated with the applicable interface as the promiscuous port, and the association of the secondary VLAN, are deleted.

[Note]

This command can be set only for a LAN/SFP port that has been set as a promiscuous port by the **switchport mode private-vlan** command.

In addition, it can also be set for the following interfaces that are specified as promiscuous ports.

- Interface that is operating as a trunk port
- logical interface

pri-vlan-id and *2nd-vlan-ids* must be associated by the **private-vlan association** command.

If this command is applied to a logical interface, the settings of every LAN/SFP port associated with that interface are changed.

If the **switchport mode private-vlan** command is used to set the port type to something other than promiscuous port, the setting of this command is deleted.

A community VLAN can be associated with multiple promiscuous ports.

Multiple promiscuous ports can be specified for one primary VLAN.

Since an interface in an isolated VLAN can communicate only with one promiscuous port, only one promiscuous port can be associated with one isolated VLAN.

[Example]

Make LAN port #1 operate as a promiscuous port, specify primary VLAN #100, and associate the secondary VLANs #101, #102, and #103.

```
SWX3220(config)# interface port1.1
SWX3220(config-if)# switchport mode private-vlan promiscuous
SWX3220(config-if)# switchport private-vlan mapping 100 add 101
SWX3220(config-if)# switchport private-vlan mapping 100 add 102
SWX3220(config-if)# switchport private-vlan mapping 100 add 103
```

6.2.13 Set voice VLAN

[Syntax]

switchport voice vlan *type*
no switchport voice vlan

[Parameter]

type : Type

Setting value	Description
<1-4094>	VLAN ID
dot1p	Use priority tagged frames
untagged	Use untagged frames

[Initial value]

none

[Input mode]

interface mode

[Description]

Sets voice VLAN. This can be specified only for a physical interface that is specified as an access port.

If a VLAN ID is specified, frames with an 802.1p tag of the specified VLAN are used as voice traffic.

If dot1p is specified, priority tag frames (VLAN ID of 0, and CoS value of the specified 802.1p tag) are used as voice traffic.

If untagged is specified, untagged frames are used as voice traffic.

[Example]

Assign LAN port #1 as voice VLAN to VLAN #100.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#switchport voice vlan 100
```

6.2.14 Set CoS value for voice VLAN

[Syntax]

switchport voice cos *value*
no switchport voice cos

[Parameter]

value : <0-7>

CoS value to specify for connected device

[Initial value]

switchport voice cos 5

[Input mode]

interface mode

[Description]

Specify the CoS value to use for voice traffic by the connected device.

The connected device is notified of the setting via LLDP-MED in the following cases.

- Voice VLAN is specified for the corresponding port.
- LLDP-MED transmission and reception is possible for the corresponding port.

[Example]

Set the CoS value to 6 for using LAN port #1 as voice VLAN.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#switchport voice cos 6
```

6.2.15 Set DSCP value for voice VLAN

[Syntax]

switchport voice dscp *value*
no switchport voice dscp

[Parameter]

value : <0-63>

DSCP value to specify for connected device

[Initial value]

switchport voice dscp 0

[Input mode]

interface mode

[Description]

Specify the DSCP value to use for voice traffic by the connected device.

The connected device is notified of the setting via LLDP-MED in the following cases.

- Voice VLAN is specified for the corresponding port.
- LLDP-MED transmission and reception is possible for the corresponding port.

[Example]

Set the DSCP value to 63 for using LAN port #1 as voice VLAN.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#switchport voice dscp 63
```

6.2.16 Set multiple VALN group

[Syntax]

switchport multiple-vlan group *group-ids*
no switchport multiple-vlan group

[Parameter]

group-ids : <1-256>

Multiple VLAN group ID

To specify multiple items, use "-" or "," as shown below

- To select from group #2 through group #4: 2-4
- To select group #2 and group #4: 2,4

[Initial value]

none

[Input mode]

interface mode

[Description]

Specify the group of multiple VLAN.

If a group is specified for the interface, the corresponding interface can communicate only with interfaces of the same multiple VLAN group. Even if the VLAN is the same, communication is not possible if the multiple VLAN group differs.

This can be specified only for a physical interface or for a link aggregation logical interface.

By default, each interface is not associated with a multiple VLAN group.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This cannot be used in conjunction with the private VLAN.

Ports that are associated with a link aggregation logical interface must be set to the same multiple VLAN group.

The multiple VLAN group is applied only to forwarding between ports. Self-originating packets are not affected by multiple VLAN group settings.

Even if multiple VLAN is specified, correct communication might not be possible due to the following.

- Spanning tree block status
- IGMP snooping or MLD snooping status
- Loop detection block status

[Example]

Assign LAN port #1 to multiple VLAN group #10.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#switchport multiple-vlan group 10
SWX3220(config-if)#exit
```

6.2.17 Set name of multiple VLAN group

[Syntax]

multiple-vlan group *group-id* **name** *name*
no multiple-vlan group *group-id*

[Parameter]

group-id : <1-256>

Multiple VLAN group ID

name : Single-byte alphanumeric characters and single-byte symbols(32characters or less)

Name of mulitiple VLAN group

[Initial value]

multiple-vlan group *group-id* name GROUPxxxx (xxxx is the four-digit group ID)

[Input mode]

global configuration mode

[Description]

Sets the name of multiple VLAN group.

If this command is executed with the "no" syntax, the setting returns to the default.

The name that was set is shown with the **show vlan multiple-vlan** command.

[Example]

Set multiple VLAN group #10 with the name "Network1".

```
SWX3220(config)#multiple-vlan group 10 name Network1
```

6.2.18 Configuring the YMPI frame transmission when multiple VLANs are configured

[Syntax]

multiple-vlan transfer ympi *switch*
no multiple-vlan transfer ympi

[Parameter]

switch : Behavior of the YMPI frame transmission when multiple VLANs are configured

Setting value	Description
enable	Enable transmission
disable	Disable transmission

[Initial value]

multiple-vlan transfer ympi enable

[Input mode]

global configuration mode

[Description]

Sets whether YMPI frames, the management frames for Yamaha wireless access points, are transmitted when multiple VLANs are configured.

This must be enabled if you want to use cluster management or wireless LAN controller functionality with multiple Yamaha wireless access points belonging to different multiple VLAN groups.

If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

Disable YMPI frame transmission when multiple VLANs are configured.

```
SWX3220(config)#multiple-vlan transfer ympi disable
```

6.2.19 Show VLAN information

[Syntax]

show vlan *vlan-id*
show vlan brief

[Keyword]

brief : Show all VLAN information

[Parameter]

vlan-id : <1-4094>

VLAN ID to show

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows information for the specified VLAN ID.

The following items are shown.

Item	Description
VLAN ID	VLAN ID

Item	Description
Name	Name of the VLAN
State	VLAN status (whether frames are forwarded) • ACTIVE : forwarded • SUSPEND : not forwarded
Member ports	Interfaces associated with the VLAN ID • (u) : Access port (untagged port) • (t) : Trunk port (tagged port)

[Example]

Show all VLAN information.

```
SWX3220>show vlan brief
(u)-Untagged, (t)-Tagged

VLAN ID  Name                            State   Member ports
======= ================================ ======= =======================
1       default                          ACTIVE  port1.1(u) port1.2(u)
                                                 port1.3(u) port1.4(u)
                                                 port1.5(u) port1.6(u)
                                                 port1.7(u) port1.8(u)
```

6.2.20 Show private VLAN information

[Syntax]

show vlan private-vlan

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows private VLAN information.

The following items are shown.

Item	Description
PRIMARY	VLAN ID of primary VLAN
SECONDARY	VLAN ID of secondary VLAN
TYPE	Type of secondary VLAN • isolated : Isolated VLAN • community : Community VLAN
INTERFACES	Interfaces that are associated as a host port

[Example]

Show private VLAN information.

```
SWX3220>show vlan private-vlan
PRIMARY       SECONDARY          TYPE         INTERFACES
-------        ---------       ----------      ----------
      2              21         isolated
      2              22         community
```

6.2.21 Show multiple VLAN group setting information

[Syntax]

show vlan multiple-vlan [**group** *group-id*]

[Keyword]

group : Show information for specific multiple VLAN groups

[Parameter]

group-id : <1-256>

Multiple VLAN group ID

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the setting status for multiple VLAN groups.

If the "group" specification is omitted, all groups that are actually assigned to the interface are shown.

The setting state of the YMPI frame transmission function is also displayed.

[Example]

Shows the setting status for multiple VLAN groups.

```
SWX3220>show vlan multiple-vlan
GROUP ID  Name                              Member ports
======== ================================ =======================
1        GROUP0001                         port1.1 port1.2
                                           port1.5

YMPI transfer: Enable
```

6.3 STP (Spanning Tree Protocol)

6.3.1 Set spanning tree for the system

[Syntax]

spanning-tree shutdown
no spanning-tree shutdown

[Initial value]

no spanning-tree shutdown

[Input mode]

global configuration mode

[Description]

Disables spanning tree for the entire system.

If this command is executed with the "no" syntax, spanning tree is enabled for the entire system.

[Note]

In order to enable spanning tree, spanning tree must be enabled on the interface in addition to this command.

[Example]

Disable spanning tree for the entire system.

```
SWX3220(config)#spanning-tree shutdown
```

6.3.2 Set forward delay time

[Syntax]

spanning-tree forward-time *time*
no spanning-tree forward-time

[Parameter]

time : <4-30>

Forward delay time (seconds)

[Initial value]

spanning-tree forward-time 15

[Input mode]

global configuration mode

[Description]

Sets the forward delay time.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

The setting of this command must satisfy the following conditions.
2 x (hello time + 1) <= maximum aging time <= 2 x (forward delay time - 1)

The maximum aging time can be set by the **spanning-tree max-age** command.

The hello time is always 2 seconds, and cannot be changed.

[Example]

Set the forward delay time to 10 seconds.

```
SWX3220(config)#spanning-tree forward-time 10
```

6.3.3 Set maximum aging time

[Syntax]

spanning-tree max-age *time*
no spanning-tree max-age

[Parameter]

time	:	<6-40>
		Maximum aging time (seconds)

[Initial value]

spanning-tree max-age 20

[Input mode]

global configuration mode

[Description]

Sets the maximum aging time.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

The maximum aging time is the time that the L2 switch waits without receiving a spanning tree configuration message, and after which time it attempts to reconfigure.

The setting of this command must satisfy the following conditions.
2 x (hello time + 1) <= maximum aging time <= 2 x (forward delay time - 1)

The forward delay time can be set by the **spanning-tree forward-time** command.

The hello time is always 2 seconds, and cannot be changed.

[Example]

Set the maximum aging time to 25 seconds.

```
SWX3220(config)#spanning-tree max-age 25
```

6.3.4 Set bridge priority

[Syntax]

spanning-tree priority *priority*
no spanning-tree priority

[Parameter]

priority	:	<0-61440> (multiple of 4096)
		Priority value

[Initial value]

spanning-tree priority 32768

[Input mode]

global configuration mode

[Description]

Sets the bridge priority. Lower numbers have higher priority.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

In the case of MSTP, this is the setting for CIST (instance #0).

[Example]

Set the bridge priority to 4096.

```
SWX3220(config)#spanning-tree priority 4096
```

6.3.5 Set spanning tree for an interface

[Syntax]

spanning-tree *switch*

[Parameter]

switch : Spanning tree operation

Setting value	Description
enable	Enable spanning tree
disable	Disable spanning tree

[Initial value]

spanning-tree enable

[Input mode]

interface mode

[Description]

Sets spanning tree operation for the applicable interface.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be specified only for LAN/SFP port and logical interface.

It is not possible to specify this command for a LAN/SFP port that is associated to a logical interface.

[Example]

Disable spanning tree for LAN port #1.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#spanning-tree disable
```

6.3.6 Set spanning tree link type

[Syntax]

spanning-tree link-type *type*
no spanning-tree link-type

[Parameter]

type : Link type

Setting value	Description
point-to-point	Point-to-point link
shared	Shared link

[Initial value]

spanning-tree link-type point-to-point

[Input mode]

interface mode

[Description]

Sets the link type for the applicable interface.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be specified only for LAN/SFP port and logical interface.

It is not possible to specify this command for a LAN/SFP port that is associated to a logical interface.

If a LAN/SFP port is associated with a logical interface, the setting of this command for the corresponding LAN/SFP port returns to the default.

[Example]

Set the LAN port #1 link type to "shared."

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#spanning-tree link-type shared
```

6.3.7 Set interface BPDU filtering

[Syntax]

spanning-tree bpdu-filter *filter*
no spanning-tree bpdu-filter

[Parameter]

filter : BPDU filtering operation

Setting value	Description
enable	Enables BPDU filtering
disable	Disables BPDU filtering

[Initial value]

spanning-tree bpdu-filter disable

[Input mode]

interface mode

[Description]

Sets BPDU filtering for the applicable interface.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be specified only for LAN/SFP port and logical interface.

It is not possible to specify this command for a LAN/SFP port that is associated to a logical interface.

If a LAN/SFP port is associated with a logical interface, the setting of this command for the corresponding LAN/SFP port returns to the default.

[Example]

Enable BPDU filtering for LAN port #1.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#spanning-tree bpdu-filter enable
```

6.3.8 Set interface BPDU guard

[Syntax]

spanning-tree bpdu-guard *guard*
no spanning-tree bpdu-guard

[Parameter]

guard : BPDU guard operation

Setting value	Description
enable	Enables BPDU guard
disable	Disables BPDU guard

[Initial value]

spanning-tree bpdu-guard disable

[Input mode]

interface mode

[Description]

Sets BPDU guard for the applicable interface.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be specified only for LAN/SFP port and logical interface.

It is not possible to specify this command for a LAN/SFP port that is associated to a logical interface.

If a LAN/SFP port is associated with a logical interface, the setting of this command for the corresponding LAN/SFP port returns to the default.

If a LAN/SFP port is **shutdown** by BPDU guard, it can be brought back by executing the **no shutdown** command for that interface.

If a logical interface is **shutdown** by BPDU guard, it can be brought back by executing the **shutdown** command for that interface and then executing the **no shutdown** command.

[Example]

Enable BPDU guard for LAN port #1.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#spanning-tree bpdu-guard enable
```

6.3.9 Set interface path cost

[Syntax]

spanning-tree path-cost *path-cost*
no spanning-tree path-cost

[Parameter]

path-cost : <1-200000000>

Path cost value

[Initial value]

Use the following values according to the link speed of the interface.

Link speed	Path cost value
1000Mbps	20000
100Mbps	200000
10Mbps	2000000

For a logical interface, the path cost value is calculated based on totaling the link speed of each associated LAN/SFP port.

[Input mode]

interface mode

[Description]

Sets the path cost of the applicable interface.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

In the case of MSTP, this is the setting for CIST (instance #0).

This command can be specified only for LAN/SFP port and logical interface.

It is not possible to specify this command for a LAN/SFP port that is associated to a logical interface.

If a LAN/SFP port is associated with a logical interface, the setting of this command for the corresponding LAN/SFP port returns to the default.

[Example]

Set the path cost of LAN port #1 to 100000.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#spanning-tree path-cost 100000
```

6.3.10 Set interface priority

[Syntax]

spanning-tree priority *priority*
no spanning-tree priority

[Parameter]

priority	:	<0-240> (multiple of 16) Priority value

[Initial value]

spanning-tree priority 128

[Input mode]

interface mode

[Description]

Sets the priority of the applicable interface.

If this command is executed with the "no" syntax, the setting returns to the default.

Lower numeric values indicate a higher priority, increasing the probability that the other interface will become the root port.

[Note]

In the case of MSTP, this is the setting for CIST (instance #0).

This command can be specified only for LAN/SFP port and logical interface.

It is not possible to specify this command for a LAN/SFP port that is associated to a logical interface.

If a LAN/SFP port is associated with a logical interface, the setting of this command for the corresponding LAN/SFP port returns to the default.

[Example]

Set the LAN port #1 priority to 64.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#spanning-tree priority 64
```

6.3.11 Set edge port for interface

[Syntax]

spanning-tree edgeport
no spanning-tree edgeport

[Initial value]

no spanning-tree edgeport

[Input mode]

interface mode

[Description]

Sets the edge port of the applicable interface.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be specified only for LAN/SFP port and logical interface.

It is not possible to specify this command for a LAN/SFP port that is associated to a logical interface.

If a LAN/SFP port is associated with a logical interface, the setting of this command for the corresponding LAN/SFP port returns to the default.

[Example]

Set LAN port #1 as the edge port.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#spanning-tree edgeport
```

6.3.12 Show spanning tree status

[Syntax]

show spanning-tree [interface *ifname*]

[Keyword]

interface : Specifies the interface to show

[Parameter]

ifname : Name of LAN/SFP port or logical interface

Interface to show

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the spanning tree status.

If "interface" is omitted, the status of all interfaces is shown.

In the case of MSTP, shows CIST (instance #0) information.

The following items are shown.

Item	Description
Bridge up	Spanning tree protocol enabled/disabled
Root Path Cost	Path cost of the root bridge
Root Port	Interface index number of the root port. Shows 0 if it is the root bridge. In the case of a logical interface, this is shown as the interface index number of the logical interface.
Bridge Priority	Bridge priority
Forward Delay	Root bridge forwarding delay time setting
Hello Time	Hello time setting of the root bridge
Max Age	Maximum ageing time setting of the root bridge
Root Id	Root bridge identifier. This consists of the root bridge priority (the first four hexadecimal digits) and MAC address
Bridge Id	Bridge identifier. This consists of the bridge priority (the first four hexadecimal digits) and MAC address
topology change(s)	Number of times that a topology change has occurred (to be precise, this indicates the number of BPDU that have the TC flag)
last topology change	Date and time at which the last topology change occurred
Ifindex	Interface index number
Port Id	Interface's port ID
Role	Role of the interface. This is either Disabled, Designated, Rootport, or Alternate
State	State of the interface. This is either Listening, Learning, Forwarding, or Discarding
Designated Path Cost	Path cost

Item	Description
Configured Path Cost	Path cost setting of the interface
Add type Explicit ref count	Number of STP domains associated with the interface
Designated Port Id	ID of the designated port
Priority	Priority of the interface
Root	Root bridge identifier. This consists of the root bridge priority (the first four hexadecimal digits) and MAC address
Designated Bridge	Bridge identifier. This consists of the bridge priority (the first four hexadecimal digits) and MAC address
Message Age	Elapsed time of message
Hello Time	Hello time setting value
Forward Delay	Forward delay time setting value
Forward Timer	Actual forward delay timer
Msg Age Timer	Timer at which the interface destroys BPDU information. With the default setting, count down from 20 seconds for STP, or count down Hello Time x 3 for RSTP/MSTP.
Hello Timer	Timer used to send hello. Hello packet is sent when 0 is reached
topo change timer	Topology change timer
forward-transitions	Number of times that the interface has entered Forward State
Version	Spanning tree protocol operating mode (version)
Received	Type of BPDU that was received
Send	Type of BPDU to transmit
portfast configured	Edge port setting value and current status. This will be either portfast off, portfast on, or edgeport on
bpdu-guard	Setting and current status of the interface's BPDU guard function
bpdu-filter	Setting and current status of the interface's BPDU filtering function
root guard configured	Setting and current status of the root guard function
Configured Link Type	Setting and current status of the interface's link type. Either point-to-point or shared
auto-edge configured	Auto-edge setting and current status

[Example]

Show the spanning tree status for LAN port #1.

```
SWX3220>show spanning-tree interface port1.1
% Default: Bridge up - Spanning Tree Enabled  - topology change detected
% Default: CIST Root Path Cost 0 - CIST Root Port 0 -  CIST Bridge Priority 32768
% Default: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 -
Max-hops 20
% Default: CIST Root Id 8000ac44f2300110
% Default: CIST Reg Root Id 8000ac44f2300110
% Default: CIST Bridge Id 8000ac44f2300110
% Default: 6 topology change(s)  - last topology change Tue Feb 27 19:52:52 2018

%   port1.1: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - Role Designated -
State Forwarding
%   port1.1: Designated External Path Cost 0 -Internal Path Cost 0
%   port1.1: Configured Path Cost 20000  - Add type Explicit ref count 1
%   port1.1: Designated Port Id 0x8389 - CIST Priority 128  -
%   port1.1: CIST Root 8000ac44f2300110
%   port1.1: Regional Root 8000ac44f2300110
```

```
%   port1.1: Designated Bridge 8000ac44f2300110
%   port1.1: Message Age 0 - Max Age 20
%   port1.1: CIST Hello Time 2 - Forward Delay 15
%   port1.1: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change
timer 0
%   port1.1: forward-transitions 1
%   port1.1: Version Multiple Spanning Tree Protocol - Received MSTP - Send MSTP
%   port1.1: No portfast configured - Current  portfast off
%   port1.1: bpdu-guard  disabled  - Current bpdu-guard off
%   port1.1: bpdu-filter disabled  - Current bpdu-filter off
%   port1.1: no root guard configured     - Current root guard off
%   port1.1: Configured Link Type point-to-point - Current point-to-point
%   port1.1: No auto-edge configured - Current port Auto Edge off
```

6.3.13 Show spanning tree BPDU statistics

[Syntax]

show spanning-tree statistics [interface *ifname*]

[Keyword]

interface	:	Specifies the interface to show

[Parameter]

ifname	:	Name of LAN/SFP port or logical interface Interface to show

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows spanning tree BPDU statistics.

If "interface" is omitted, the status of all interfaces is shown.

[Example]

Show the BPDU statistics for LAN port #1.

```
SWX3220>show spanning-tree statistics interface port1.1
                 Port number = 905 Interface = port1.1
                 ================================
% BPDU Related Parameters
% ------------------------
% Port Spanning Tree                 : Enable
% Spanning Tree Type                 : Multiple Spanning Tree Protocol
% Current Port State                 : Forwarding
% Port ID                            : 8389
% Port Number                        : 389
% Path Cost                          : 20000
% Message Age                        : 0
% Designated Root                    : ac:44:f2:30:01:10
% Designated Cost                    : 0
% Designated Bridge                  : ac:44:f2:30:01:10
% Designated Port Id                 : 0x8389
% Top Change Ack                     : FALSE
% Config Pending                     : FALSE

% PORT Based Information & Statistics
% -----------------------------------
% Config Bpdu's xmitted              : 3
% Config Bpdu's received             : 0
% TCN Bpdu's xmitted                 : 2
% TCN Bpdu's received                : 3
% Forward Trans Count                : 1

% STATUS of Port Timers
% ---------------------
% Hello Time Configured              : 2
% Hello timer                        : ACTIVE
% Hello Time Value                   : 0
% Forward Delay Timer                : INACTIVE
% Forward Delay Timer Value          : 0
```

```
% Message Age Timer                  : INACTIVE
% Message Age Timer Value            : 0
% Topology Change Timer              : INACTIVE
% Topology Change Timer Value        : 0
% Hold Timer                         : INACTIVE
% Hold Timer Value                   : 0

% Other Port-Specific Info
  ------------------------
% Max Age Transitions                : 1
% Msg Age Expiry                     : 0
% Similar BPDUS Rcvd                 : 0
% Src Mac Count                      : 0
% Total Src Mac Rcvd                 : 3
% Next State                         : Discard/Blocking
% Topology Change Time               : 0

% Other Bridge information & Statistics
  -------------------------------------
% STP Multicast Address              : 01:80:c2:00:00:00
% Bridge Priority                    : 32768
% Bridge Mac Address                 : ac:44:f2:30:01:10
% Bridge Hello Time                  : 2
% Bridge Forward Delay               : 15
% Topology Change Initiator          : 5001
% Last Topology Change Occured       : Tue Feb 27 19:52:52 2018
% Topology Change                    : FALSE
% Topology Change Detected           : TRUE
% Topology Change Count              : 6
% Topology Change Last Recvd from    : 00:a0:de:ae:b8:79
```

6.3.14 Clear protocol compatibility mode

[Syntax]

clear spanning-tree detected protocols [interface *ifname*]

[Keyword]

interface	:	Specifies the interface to clear

[Parameter]

ifname	:	Name of LAN/SFP port or logical interface Interface to clear

[Input mode]

privileged EXEC mode

[Description]

Returns an interface that had been operating in STP compatibility mode to normal mode.

If "interface" is omitted, the status of all interfaces is cleared.

[Note]

If a STP BPDU is received, the interface that received it will operate in STP compatibility mode. However even if STP BPDU is no longer received subsequently, the corresponding interface continues to operate in STP compatibility mode. In such cases, you can execute this command to make the interface return from STP compatibility mode to normal mode.

[Example]

Return LAN port #1 from STP compatibility to normal mode.

```
SWX3220#clear spanning-tree detected protocols interface port1.1
```

6.3.15 Move to MST mode

[Syntax]

spanning-tree mst configuration

[Input mode]

global configuration mode

[Description]

Moves to MST mode in order to make MST instance and MST region settings.

[Note]

To return from MST mode to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

[Example]

Move to MST mode.

```
SWX3220(config)#spanning-tree mst configuration
SWX3220(config-mst)#
```

6.3.16 Generate MST instance

[Syntax]

instance *instance-id*
no instance

[Parameter]

instance-id	:	<1-15> Instance ID

[Initial value]

none

[Input mode]

MST mode

[Description]

Generates an MST instance.

If this command is executed with the "no" syntax, the MST instance is deleted.

[Note]

MST instance generation and association with a VLAN is specified by the **instance vlan** command.

[Example]

Generate MST instance #1.

```
SWX3220(config)#spanning-tree mst configuration
SWX3220(config-mst)#instance 1
```

6.3.17 Set VLAN for MST instance

[Syntax]

instance *instance-id* **vlan** *vlan-id*
no instance *instance-id* **vlan** *vlan-id*

[Parameter]

instance-id	:	<1-15> Instance ID
vlan-id	:	<2-4094> VLAN ID set by the **vlan** command

[Initial value]

none

[Input mode]

MST mode

[Description]

Associates a VLAN with an MST instance.

If this command is executed with the "no" syntax, the VLAN association for the MST instance is deleted. If as a result of this deletion, not even one VLAN is associated with the MST instance, the MST instance is deleted.

If you specify an MST instance that has not been generated, the MST instance will also be generated.

[Note]

You cannot specify a VLAN ID that is associated with another MST instance.

The number of VLANs that are associated with an MST instance can be a maximum of 256 for the system overall.

[Example]

Associate VLAN #2 with MST instance #1.

```
SWX3220(config)#spanning-tree mst configuration
SWX3220(config-mst)#instance 1 vlan 2
```

6.3.18 Set priority of MST instance

[Syntax]

instance *instance-id* **priority** *priority*
no instance *instance-id* **priority**

[Parameter]

instance-id	:	<1-15> Instance ID
priority	:	<0-61440> (multiple of 4096) Priority value

[Initial value]

instance *instance-id* priority 32768

[Input mode]

MST mode

[Description]

Sets the priority of the MST instance.

Lower numeric values indicate a higher priority, increasing the probability that this MST instance will become the root bridge.

If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

Set MST instance #2 to a priority of 4096.

```
SWX3220(config)#spanning-tree mst configuration
SWX3220(config-mst)#instance 2
SWX3220(config-mst)#instance 2 priority 4096
```

6.3.19 Set MST region name

[Syntax]

region *region-name*
no region

[Parameter]

region-name	:	Single-byte alphanumeric characters and single-byte symbols(32characters or less) Region name

[Initial value]

region Default

[Input mode]

MST mode

[Description]

Sets the MST region name.

If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

Set the MST region name to "Test1".

```
SWX3220(config)#spanning-tree mst configuration
SWX3220(config-mst)#region Test1
```

6.3.20 Set revision number of MST region

[Syntax]

revision *revision*

[Parameter]

revision	:	<0-65535> Revision number

[Initial value]

revision 0

[Input mode]

MST mode

[Description]

Sets the revision number of the MST region.

If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

Set the revision number as 2 for the MST region.

```
SWX3220(config)#spanning-tree mst configuration
SWX3220(config-mst)#revision 2
```

6.3.21 Set MST instance for interface

[Syntax]

spanning-tree instance *instance-id*
no spanning-tree instance

[Parameter]

instance-id	:	<1-15> ID of generated MST interface

[Initial value]

none

[Input mode]

interface mode

[Description]

Sets MST instance for the applicable interface.

If this command is executed with the "no" syntax, the MST instance setting is deleted.

[Note]

This command can be specified only for LAN/SFP port and logical interface.

It is not possible to specify this command for a LAN/SFP port that is associated to a logical interface.

If a LAN/SFP port is associated with a logical interface, the setting of this command for the corresponding LAN/SFP port returns to the default.

[Example]

Set MST instance #2 for LAN port #1.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#spanning-tree instance 2
```

6.3.22 Set interface priority for MST instance

[Syntax]

spanning-tree instance *instance-id* **priority** *priority*
no spanning-tree instance *instance-id* **priority**

[Parameter]

instance-id : <1-15>

ID of MST instance specified for the applicable interface

priority : <0-240> (multiple of 16)

Priority value

[Initial value]

spanning-tree instance *instance-id* priority 128

[Input mode]

interface mode

[Description]

Sets the priority for the applicable interface in the MST instance.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be specified only for LAN/SFP port and logical interface.

It is not possible to specify this command for a LAN/SFP port that is associated to a logical interface.

If a LAN/SFP port is associated with a logical interface, the setting of this command for the corresponding LAN/SFP port returns to the default.

[Example]

Set LAN port #1 MST instance #2 to a priority of 16.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#spanning-tree instance 2
SWX3220(config-if)#spanning-tree instance 2 priority 16
```

6.3.23 Set interface path cost for MST instance

[Syntax]

spanning-tree instance *instance-id* **path-cost** *path-cost*
no spanning-tree instance *instance-id* **path-cost**

[Parameter]

instance-id : <1-15>

ID of MST instance specified for the applicable interface

path-cost : <1-200000000>

Path cost value

[Initial value]

Use the following values according to the link speed of the interface.

Link speed	Path cost value
1000Mbps	20000
100Mbps	200000
10Mbps	2000000

For a logical interface, the path cost value is calculated based on totaling the link speed of each associated LAN/SFP port.

[Input mode]

interface mode

[Description]

Sets the path cost of the applicable interface on an MST instance.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be specified only for LAN/SFP port and logical interface.

It is not possible to specify this command for a LAN/SFP port that is associated to a logical interface.

If a LAN/SFP port is associated with a logical interface, the setting of this command for the corresponding LAN/SFP port returns to the default.

[Example]

Set LAN port #1 MST instance #2 to a path cost of 100000.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#spanning-tree instance 2
SWX3220(config-if)#spanning-tree instance 2 path-cost 100000
```

6.3.24 Show MST region information

[Syntax]

show spanning-tree mst config

[Input mode]

unprivileged EXEC mode, privileged EXEC mode, interface mode

[Description]

Shows distinguishing information for the MST region.

[Example]

Show distinguishing information for the MST region.

```
SWX3220>show spanning-tree mst config
%
%  MSTP Configuration Information for bridge Default :
%-----------------------------------------------------
%  Format Id      : 0
%  Name           : Default
%  Revision Level : 0
%  Digest         : 0xAC36177F50283CD4B83821D8AB26DE62
%-----------------------------------------------------
```

6.3.25 Show MSTP information

[Syntax]

show spanning-tree mst [detail] [interface *ifname*]

[Keyword]

detail	:	Shows detailed information
interface	:	Specifies the interface to show

[Parameter]

ifname	:	Name of LAN/SFP port or logical interface Interface to show

[Input mode]

unprivileged EXEC mode, privileged EXEC mode, interface mode

[Description]

Shows MSTP information.

Normally, this shows association information for the MST instance and VLAN and interface.

If "detail" is specified, this shows detailed information for the interface and MST instance.

If "interface" is omitted, information for all interfaces is shown.

[Note]

A LAN/SFP port that is associated with a logical interface cannot be specified as *ifname*.

[Example]

Show MSTP information.

```
SWX3220>show spanning-tree mst
% Default: Bridge up - Spanning Tree Enabled  - topology change detected
% Default: CIST Root Path Cost 0 - CIST Root Port 0 -  CIST Bridge Priority 32768
% Default: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 -
Max-hops 20
% Default: CIST Root Id 8000ac44f2300110
% Default: CIST Reg Root Id 8000ac44f2300110
% Default: CIST Bridge Id 8000ac44f2300110
% Default: 9 topology change(s)  - last topology change Tue Feb 27 20:14:35 2018

%
%   Instance        VLAN
%   0:              1
%   1:              100 (port1.8)
```

Show detailed MSTP information for LAN port #8.

```
SWX3220>show spanning-tree mst detail interface port1.8
% Default: Bridge up - Spanning Tree Enabled  - topology change detected
% Default: CIST Root Path Cost 0 - CIST Root Port 0 -  CIST Bridge Priority 32768
% Default: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 -
Max-hops 20
% Default: CIST Root Id 8000ac44f2300110
% Default: CIST Reg Root Id 8000ac44f2300110
% Default: CIST Bridge Id 8000ac44f2300110
% Default: 9 topology change(s)  - last topology change Tue Feb 27 20:14:35 2018

%   port1.8: Port Number 912 - Ifindex 5008 - Port Id 0x8390 - Role Designated -
State Forwarding
%   port1.8: Designated External Path Cost 0 -Internal Path Cost 0
%   port1.8: Configured Path Cost 20000  - Add type Explicit ref count 2
%   port1.8: Designated Port Id 0x8390 - CIST Priority 128  -
%   port1.8: CIST Root 8000ac44f2300110
%   port1.8: Regional Root 8000ac44f2300110
%   port1.8: Designated Bridge 8000ac44f2300110
%   port1.8: Message Age 0 - Max Age 20
%   port1.8: CIST Hello Time 2 - Forward Delay 15
%   port1.8: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change
timer 0
%   port1.8: forward-transitions 1
%   port1.8: Version Multiple Spanning Tree Protocol - Received MSTP - Send MSTP
%   port1.8: No portfast configured - Current  portfast off
%   port1.8: bpdu-guard  disabled  - Current bpdu-guard off
%   port1.8: bpdu-filter disabled  - Current bpdu-filter off
%   port1.8: no root guard configured     - Current root guard off
%   port1.8: Configured Link Type point-to-point - Current point-to-point
%   port1.8: No auto-edge configured - Current port Auto Edge off
%

% Instance  1:  Vlans: 100
% Default: MSTI Root Path Cost 0 -MSTI Root Port 0 - MSTI Bridge Priority 32768
% Default: MSTI Root Id 8001ac44f2300110
% Default: MSTI Bridge Id 8001ac44f2300110
%   port1.8: Port Number 912 - Ifindex 5008 - Port Id 0x8390 - Role Designated -
State Forwarding
%   port1.8: Designated Internal Path Cost 0  - Designated Port Id 0x8390
%   port1.8: Configured Internal Path Cost 20000
%   port1.8: Configured CST External Path cost 20000
%   port1.8: CST Priority 128  - MSTI Priority 128
%   port1.8: Designated Root 8001ac44f2300110
%   port1.8: Designated Bridge 8001ac44f2300110
%   port1.8: Message Age 0
%   port1.8: Hello Time 2 - Forward Delay 15
%   port1.8: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
```

6.3.26 Show MST instance information

[Syntax]

show spanning-tree mst instance *instance-id* [interface *ifname*]

[Keyword]

interface	:	Specifies the interface to show

[Parameter]

instance-id	:	<1-15> ID of generated MST interface
ifname	:	Name of LAN/SFP port or logical interface Interface to show

[Input mode]

unprivileged EXEC mode, privileged EXEC mode, interface mode

[Description]

Shows information for the specified MST instance.

If "interface" is omitted, information is shown for all interfaces that are assigned the specified MST instance.

[Note]

A LAN/SFP port that is associated with a logical interface cannot be specified as *ifname*.

[Example]

Show information for MST instance #1.

```
SWX3220>show spanning-tree mst instance 1
% Default: MSTI Root Path Cost 0 - MSTI Root Port 0 - MSTI Bridge Priority 32768
% Default: MSTI Root Id 8001ac44f2300110
% Default: MSTI Bridge Id 8001ac44f2300110
%   port1.8: Port Number 912 - Ifindex 5008 - Port Id 0x8390 - Role Designated -
State Forwarding
%   port1.8: Designated Internal Path Cost 0  - Designated Port Id 0x8390
%   port1.8: Configured Internal Path Cost 20000
%   port1.8: Configured CST External Path cost 20000
%   port1.8: CST Priority 128  - MSTI Priority 128
%   port1.8: Designated Root 8001ac44f2300110
%   port1.8: Designated Bridge 8001ac44f2300110
%   port1.8: Message Age 0
%   port1.8: Hello Time 2 - Forward Delay 15
%   port1.8: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%
```

6.4 Loop detection

6.4.1 Set loop detection function (system)

[Syntax]

loop-detect *switch*
no loop-detect

[Parameter]

switch : Set system-wide loop detection function

Setting value	Description
enable	Enables system-wide loop detection function
disable	Disables system-wide loop detection function

[Initial value]

loop-detect disable

[Input mode]

global configuration mode

[Description]

Enables or disables the system-wide loop detection function.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

The spanning tree function and the loop detection function can be used together on the entire system.

In order to enable the loop detection function, the loop detection function must be enabled on the interface in addition to this command.

Even if the loop detection function is enabled, the loop detection function does not operate on the following interfaces.

- LAN/SFP port and logical interface on which the spanning tree function is operating However, because a Forwarding port transmits and receives LDF, the loop detection will operate if misconnection or another issue causes a loop to occur.
- LAN/SFP port that is operating as a mirror port for the mirroring function

[Example]

Enable the loop detection function for the entire system.

```
SWX3220(config)#loop-detect enable
```

Disable the loop detection function for the entire system.

```
SWX3220(config)#loop-detect disable
```

6.4.2 Set loop detection function (interface)

[Syntax]

loop-detect *switch*
no loop-detect

[Parameter]

switch : Set loop detection function for the applicable interface

Setting value	Description
enable	Enables loop detection function for the applicable interface
disable	Disables loop detection function for the applicable interface

[Initial value]

loop-detect enable

[Input mode]

interface mode

[Description]

Enables or disables loop detection function for the applicable interface.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

In order to enable the loop detection function, the loop detection function must be enabled on the entire system in addition to this command.

An LAN/SFP port whose settings of this command differ cannot be aggregated as a logical interface. However, in the case of settings for an LAN/SFP port that is associated with an logical interface in the startup config, the setting for the lowest-numbered port is applied to the logical interface.

This command cannot be executed for LAN/SFP port that belong to logical interface.

Even if the loop detection function is enabled, the loop detection function does not operate on the following interfaces.

- LAN/SFP port and logical interface on which the spanning tree function is operating However, because a forwarding port transmits and receives LDF, the loop detection will operate if misconnection or another issue causes a loop to occur.
- LAN/SFP port that is operating as a mirror port for the mirroring function

The following table shows which function is enabled depending on the settings of the spanning tree function (STP) and the loop detection function (LPD).

			Interface			
			LPD disabled		LPD enabled	
			STP disabled	STP enabled	STP disabled	STP enaabled
System	LPD disabled	STP disabled	-	-	-	-
		STP enabled	-	STP	-	STP
	LPD enabled	STP disabled	-	-	LPD	LPD
		STP enabled	-	STP	LPD	STP

[Example]

Enable the loop detection function of LAN port #1.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#loop-detect enable
```

Enables the loop detection function of static logical interface #1.

```
SWX3220(config)#interface sa1
SWX3220(config-if)#loop-detect enable
```

Enables the loop detection function of LACP logical interface #1.

```
SWX3220(config)#interface po1
SWX3220(config-if)#loop-detect enable
```

Disable the loop detection function of LAN port #1.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#loop-detect disable
```

6.4.3 Set port blocking for loop detection

[Syntax]

loop-detect blocking *switch*
no loop-detect blocking

[Parameter]

switch : Set port blocking for the applicable interface

Setting value	Description
enable	Enables port blocking for the applicable interface
disable	Disables port blocking for the applicable interface

[Initial value]

loop-detect blocking enable

[Input mode]

interface mode

[Description]

Enables or disables blocking when a loop is detected for the applicable interface.

If this is executed with the "no" syntax, the setting returns to the default.

[Note]

An LAN/SFP port whose settings of this command differ cannot be aggregated as a logical interface. However, in the case of settings for an LAN/SFP port that is associated with an logical interface in the startup config, the setting for the lowest-numbered port is applied to the logical interface.

This command cannot be executed for LAN/SFP port that belong to logical interface.

[Example]

Block if a loop is detected on LAN port #1.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#loop-detect blocking enable
```

This executes blocking if a loop is detected on static logical interface #1.

```
SWX3220(config)#interface sa1
SWX3220(config-if)#loop-detect blocking enable
```

This executes blocking if a loop is detected on LACP logical interface #1.

```
SWX3220(config)#interface po1
SWX3220(config-if)#loop-detect blocking enable
```

Do not block if a loop is detected on LAN port #1.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#loop-detect blocking disable
```

6.4.4 Detects Port Blocking loop clearing at regular intervals

[Syntax]

loop-detect blocking interval *interval*
no loop-detect blocking interval

[Parameter]

interval	:	<10-3600>
		Time between loop clearing detection (seconds)

[Initial value]

None

[Input mode]

global configuration mode

[Description]

Normally, Blocking is released immediately when the loop is cleared.

When this command is configured, it detects if the loop is cleared at regular intervals.

If the loop is cleared, Blocking is released, but if the loop is not cleared, Blocking continues until that time passes again.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

If a port in the Port Blocking state goes link down, the Port Blocking is removed immediately.

[Example]

Set the Port Blocking loop clearing detection interval to 300 seconds.

```
SWX3220(config)#loop-detect blocking interval 300
```

6.4.5 Reset loop detection status

[Syntax]

loop-detect reset

[Input mode]

privileged EXEC mode

[Description]

Resets the loop detection status of all interfaces.

[Note]

This command can be executed only if the system-wide loop detection function is enabled.

[Example]

Reset the loop detection status.

```
SWX3220#loop-detect reset
```

6.4.6 Show loop detection function status

[Syntax]

show loop-detect

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the settings and status of the loop detection function.

The following items are shown.

- Setting of the system-wide loop detection function
- Port Blocking loop clearing detection interval ("auto" or "N seconds")
- Loop detection status for each LAN/SFP port and logical interface
  - Interface name (port, sa, po)
  - Setting of the loop detection function (loop-detect) for LAN/SFP port and logical interface. If the loop detection function is operating, (*) is added
  - Status of the Port Blocking setting (port-blocking)
  - Loop detection status (status)

[Note]

This is not shown for LAN/SFP port that belong to a logical interface.

[Example]

Show the loop detection status.

```
SWX3220>show loop-detect
loop-detect: Enable
port-blocking interval: 300 seconds

port      loop-detect    port-blocking           status
-------------------------------------------------------
port1.1        enable(*)        enable         Detected
port1.2        enable(*)        enable         Blocking
port1.3        enable(*)        enable           Normal
port1.4        enable(*)       disable           Normal
port1.5        enable(*)        enable           Normal
port1.6        enable(*)        enable         Shutdown
port1.7       disable           enable           ------
   :             :                :                :
sa1            enable(*)        enable         Blocking
   :             :                :                :
po1            enable(*)        enable           Normal
   :             :                :                :
-------------------------------------------------------
(*): Indicates that the feature is enabled.
```

6.5 DHCP snooping

6.5.1 Enable/disable setting for DHCP snooping (system)

[Syntax]

ip dhcp snooping *switch*
no ip dhcp snooping

[Parameter]

switch : System-wide DHCP snooping function setting

Setting value	Description
enable	Enables settings of the DHCP snooping function for the entire system
disable	Disables settings of the DHCP snooping function for the entire system

[Initial value]

ip dhcp snooping disable

[Input mode]

global configuration mode

[Description]

Enables or disables settings of the system-wide DHCP snooping function.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

To enable the DHCP snooping function, you must enable the DHCP snooping function for the VLAN interface in addition to using this command.

Also, you must use the **ip dhcp snooping trust** command to set the port that is connected to the DHCP server.

If the DHCP server function or the relay agent function for the entire system is enabled, you cannot enable this function.

Further, when this function is enabled, you cannot enable the DHCP server function or the DHCP relay agent function for the entire system.

[Example]

This enables the DHCP snooping function for the entire system.

```
SWX3220(config)#ip dhcp snooping enable
```

This disables the DHCP snooping function for the entire system.

```
SWX3220(config)#ip dhcp snooping disable
```

6.5.2 Enable/disable DHCP snooping (VLAN) setting

[Syntax]

ip dhcp snooping *switch*
no ip dhcp snooping

[Parameter]

switch : Setting for the DHCP snooping function of the applicable interface

Setting value	Description
enable	Enables the DHCP snooping detection function setting for the applicable interface
disable	Disables the DHCP snooping detection function setting for the applicable interface

[Initial value]

ip dhcp snooping disable

[Input mode]

interface mode

[Description]

Enables or disables the DHCP snooping function settings for the applicable interface.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be specified only for VLAN interfaces.

To enable the DHCP snooping function, you must enable the DHCP snooping function for the entire system in addition to using this command.

Also, you must use the **ip dhcp snooping trust** command to set the port that is connected to the DHCP server.

[Example]

This enables the DHCP snooping function for VLAN1.

```
SWX3220(config)#interface vlan1
SWX3220(config-if)#ip dhcp snooping enable
```

This disables the DHCP snooping function for VLAN1.

```
SWX3220(config)#interface vlan1
SWX3220(config-if)#ip dhcp snooping disable
```

6.5.3 DHCP snooping port type setting

[Syntax]

ip dhcp snooping trust
no ip dhcp snooping trust

[Initial value]

None

[Input mode]

interface mode

[Description]

Sets the applicable interface as a trusted port for DHCP snooping.

If this command is executed with the "no" syntax, the setting returns to the default.

All ports are set as untrusted ports by default.

[Note]

This command can be specified only for the LAN/SFP ports and for logical interfaces.

This cannot be set for LAN/SFP ports that belong to a logical interface.

DHCP packet filtering is not performed with trusted ports, and trusted ports are set as ports to which trusted DHCP servers are connected.

DHCP packet filtering is processed for untrusted ports as follows.

- DHCP packets transmitted from the DHCP server are discarded.
- Discard IP address release requests (DHCP RELEASE) and IP address duplicate detection notifications (DHCP DECLINE) received from an interface whose MAC address is registered in the binding database and which is also different from the registered interface.
- When MAC address verification is enabled, the MAC address for the DHCP packet transmission source is compared with the client hardware database (chaddr). If the two do not match, the relevant DHCP packet is discarded.
- When Option 82 is enabled and the Option 82 information is already added to the DHCP packet received from the DHCP client, the relevant DHCP packet is discarded.

[Example]

This specifies port1.5 as a trusted port.

```
SWX3220(config)#interface port1.5
SWX3220(config-if)#ip dhcp snooping trust
```

6.5.4 Enable/disable setting for MAC address verification

[Syntax]

ip dhcp snooping verify mac-address *switch*
no ip dhcp snooping verify mac-address

[Parameter]

switch : MAC address verification setting

Setting value	Description
enable	Enables MAC address verification setting
disable	Disables MAC address verification setting

[Initial value]

ip dhcp snooping verify mac-address enable

[Input mode]

global configuration mode

[Description]

The MAC address for the transmission source of the DHCP packet received from an untrusted port is compared with the client hardware database (chaddr). If the two do not match, the relevant DHCP packet is discarded.

If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

Disables MAC address verification setting.

```
SWX3220(config)#ip dhcp snooping verify mac-address disable
```

6.5.5 Enable/disable Option 82 setting

[Syntax]

ip dhcp snooping information option *switch*
no ip dhcp snooping information option

[Parameter]

switch : Option 82 setting

Setting value	Description
enable	Enable setting for Option 82
disable	Disable setting for Option 82

[Initial value]

ip dhcp snooping information option enable

[Input mode]

global configuration mode

[Description]

Enables/disables the settings for adding, inspecting and deleting Option 82 information in DHCP packets.

If this command is executed with the "no" syntax, the setting returns to the default.

When Option 82 is enabled, the Option 82 information is added to DHCP packets received from the DHCP client on the untrusted port,

and the return packets are forwarded to the DHCP client from the DHCP server with the Option 82 information deleted.

The Option 82 information is as follows.

- Remote-ID
  - The MAC address of this device is added by default.
  - You can use the **ip dhcp snooping information option format remote-id** command to add a desired text string (single-byte alphanumeric characters and single-byte symbols) to the Remote-ID.
- Circuit-ID
  - The VLAN ID that received the DHCP packet from the DHCP client as well as the interface number are added by default.
  - Use the **ip dhcp snooping vlan vlan-id information option format-type circuit-id** command to change the Circuit-ID information to the VLAN ID that received the DHCP packet from the DHCP client as well as the port number.
- Subscriber-ID
  - Not added by default.
  - You can use the **ip dhcp snooping subscriber-id** command to set the desired text string for the Subscriber-ID of the applicable port.

When a DHCP packet to which Option 82 information has already been added is received, that DHCP packet is discarded.

You can use the **ip dhcp snooping information option allow-untrusted** command to permit forwarding of DHCP packets that include Option 82 information at the untrusted port.

[Example]

This disables Option 82 settings.

```
SWX3220(config)#ip dhcp snooping information option disable
```

6.5.6 Settings for permitting receipt of packets on an untrusted port, including Option 82 information

[Syntax]

ip dhcp snooping information option allow-untrusted
no ip dhcp snooping information option allow-untrusted

[Initial value]

None

[Input mode]

global configuration mode

[Description]

Enables forwarding of DHCP packets to which Option 82 information has been added at an untrusted port.

If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

This enables forwarding of DHCP packets to which Option 82 information has been added at an untrusted port.

```
SWX3220(config)#ip dhcp snooping information option allow-untrusted
```

6.5.7 Option 82 Remote-ID settings

[Syntax]

ip dhcp snooping information option format remote-id string *remoteid*
ip dhcp snooping information option format remote-id hostname
no ip dhcp snooping information option format remote-id

[Keyword]

string	:	Specifies the REMOTEID text string
hostname	:	Sets the REMOTEID host name

[Parameter]

remoteid	:	Desired text string (single-byte alphanumeric characters and single-byte symbols, 63 characters or less)

[Initial value]

None

[Input mode]

interface mode

[Description]

Lets you add a desired text string to an Option 82 Remote-ID.

Note that "?" cannot be included in the desired text string.

If this command is executed with the "no" syntax, this unit’s MAC address is added to the Remote-ID.

[Note]

This command can be specified only for VLAN interfaces.

[Example]

This lets you add desired characters to a Remote-ID.

```
SWX3220(config)#interface vlan1
SWX3220(config-if)#ip dhcp snooping information option format remote-id pc1
```

6.5.8 Option 82 Circuit-ID settings

[Syntax]

ip dhcp snooping information option format-type circuit-id vlan-port
ip dhcp snooping information option format-type circuit-id string *string*
ip dhcp snooping information option format-type circuit-id vlan-ifindex

no ip dhcp snooping information option format-type circuit-id

[Keyword]

vlan-port	:	Use Circuit-ID type 0 VLAN ID, Module (stack ID), port number
string	:	Use Circuit-ID type 1 desired text string
vlan-ifindex	:	Use Circuit-ID type 2 VLAN ID, ifindex

[Parameter]

string	:	Desired text string (single-byte alphanumeric characters and single-byte symbols, 63 characters or less)

[Initial value]

ip dhcp snooping information option format-type circuit-id vlan-ifindex

[Input mode]

interface mode

[Description]

Specifies the information used for Option 82 Circuit-ID.

When "vlan-port" is specified, this adds the VLAN ID that received the DHCP packet from the DHCP client, as well as the stack number and port number.

When "string" is specified, a desired text string is added. Note that "?" cannot be included in the desired text string.

When "vlan-ifindex" is specified, this adds the VLAN ID that received the DHCP packet from the DHCP client, as well as the interface number.

If this command is executed with the "no" syntax, the setting is returned to the default.

[Note]

This command can be specified only for VLAN interfaces.

[Example]

Adds the VLAN ID that received the DHCP packet from the DHCP client to the Circuit ID, as well as the port number.

```
SWX3220(config)#interface vlan1
SWX3220(config-if)#ip dhcp snooping information option format-type circuit-id vlan-
port
```

6.5.9 Option 82 Subscriber-ID settings

[Syntax]

ip dhcp snooping subscriber-id *subid*
no ip dhcp snooping subscriber-id

[Parameter]

subid	:	Desired text string (single-byte alphanumeric characters and single-byte symbols, 50 characters or less)

[Initial value]

None

[Input mode]

interface mode

[Description]

Sets the desired text string (1–50 characters) for the Subscriber-ID of the applicable port. Note that "?" cannot be included in the text string.

If this command is executed with the "no" syntax, the Subscriber-ID is not added to the Option 82 information.

[Note]

This command can be specified only for the LAN/SFP ports and for logical interfaces.

This cannot be set for LAN/SFP ports that belong to a logical interface.

[Example]

This sets the Subscriber-ID for port1.1.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#ip dhcp snooping subscriber-id a_room
```

6.5.10 DHCP packet reception rate limitation setting

[Syntax]

ip dhcp snooping limit rate *limit*
no ip dhcp snooping limit rate

[Parameter]

limit : 10 - 125

Number of DHCP packets that can be received per second (pps)

[Initial value]

None

[Input mode]

global configuration mode

[Description]

Sets the number of DHCP packets that can be received per second (pps) for the entire system.

If this exceeds the reception rate limitation, the received DHCP packets that exceed the rate are discarded.

If this command is executed with the "no" syntax, the DHCP packet reception rate is not limited.

[Example]

This sets the DHCP packet reception rate to 100 pps for the entire system.

```
SWX3220(config)#ip dhcp snooping limit rate 100
```

6.5.11 Setting to enable/disable SYSLOG output when DHCP packets are discarded

[Syntax]

ip dhcp snooping logging *switch*
no ip dhcp snooping logging

[Parameter]

switch : SYSLOG output setting when DHCP packets are discarded

Setting value	Description
enable	Outputs to SYSLOG when DHCP packets are discarded
disable	Does not output to SYSLOG when DHCP packets are discarded

[Initial value]

ip dhcp snooping logging enable

[Input mode]

global configuration mode

[Description]

Outputs the reason why DHCP packets were discarded to SYSLOG.

If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

This outputs to SYSLOG when DHCP packets are discarded.

```
SWX3220(config)#ip dhcp snooping logging enable
```

6.5.12 Show DHCP snooping system setting information

[Syntax]

show ip dhcp snooping

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

Shows DHCP snooping system setting information.

[Example]

This shows the DHCP snooping system setting information.

```
SWX3220>show ip dhcp snooping
DHCP Snooping Information for system:
  DHCP Snooping service ............. Enabled
  Option 82 insertion ............... Enabled
  Option 82 on untrusted ports ...... Disabled
  Verify MAC address ................ Enabled
  Rate limit ........................ 100 pps
  Logging ........................... Enabled
```

6.5.13 Show interface setting information for DHCP snooping

[Syntax]

show ip dhcp snooping interface

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

Shows the interface setting information for DHCP snooping.

[Example]

This shows the interface setting information for DHCP snooping.

```
SWX3220>show ip dhcp snooping interface
DHCP Snooping information for vlan1:
  DHCP snooping ... Enabled
  Remote-ID ....... 00a0.de00.0001
  Circuit-ID ...... vlan-ifindex
  Interface   Type        Subscriber-ID
  ----------  ----------  ----------------
  port1.1     Trusted
  port1.2     Untrusted   a_room
  port1.10    Untrusted   b_room

DHCP Snooping information for vlan2:
  DHCP snooping ... Enabled
  Remote-ID ....... yamaha
  Circuit-ID ...... vlan-port
  Interface   Type        Subscriber-ID
  ----------  ----------  ----------------
  port1.3     Trusted
  port1.4     Untrusted   c_room
  port1.5     Untrusted   d_room

DHCP Snooping information for vlan3:
  DHCP snooping ... Disabled

DHCP Snooping information for vlan4:
  DHCP snooping ... Enabled
  Remote-ID ....... yamaha
  Circuit-ID ...... torakusu
  Interface   Type        Subscriber-ID
  ----------  ----------  ----------------
  port1.8     Untrusted   e_room
  port1.9     Trusted
```

6.5.14 View the binding database

[Syntax]

show ip dhcp snooping binding

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

Shows information for the entries that are registered in the binding database.

The entry information is as follows.

- VLAN ID that received a DHCP message from a DHCP client
- Information on the interface that received a DHCP message from a DHCP client
- MAC addresses of DHCP clients
- IP addresses of DHCP clients
- Lease time

[Example]

Shows the contents of the binding database.

```
SWX3220>show ip dhcp snooping binding
DHCP Snooping Bindings:
Total number of bindings in database: 4

VLAN  Interface  MAC address     IP address       Expires(sec)
----  ---------  --------------  ---------------  ------------
   1  port1.1    0000.1111.2222  192.168.100.2          259170
   1  port1.2    0000.3333.4444  192.168.100.3          112000
   2  sa1        0000.5555.6666  192.168.200.2          100000
   2  port1.10   0000.7777.8888  192.168.200.3        infinite
```

6.5.15 Show DHCP snooping statistics

[Syntax]

show ip dhcp snooping statistics

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

Shows DHCP snooping statistics.

Shows the number of received and discarded DHCP packets for each interface.

[Note]

The packets that are discarded as a result of DHCP packet reception rate limitation settings are not counted.

[Example]

Shows DHCP snooping statistics.

```
SWX3220>show ip dhcp snooping statistics
DHCP Snooping Statistics:

VLAN  Interface  IN-Packets  IN-Discards
----  ---------  ----------  -----------
   1  port1.1           200          100
   1  port1.2           300            0
   1  port1.5             0            0
   2  port1.3             0            0
   2  port1.4             0            0
   2  sa1                50            2
```

6.5.16 Clear the binding database

[Syntax]

clear ip dhcp snooping binding

[Input mode]

privileged EXEC mode

[Description]

Clears the binding database.

[Example]

This clears the binding database.

```
SWX3220#clear ip dhcp snooping binding
```

6.5.17 Clear the DHCP snooping statistics

[Syntax]

clear ip dhcp snooping statistics

[Input mode]

privileged EXEC mode

[Description]

Clears the DHCP snooping statistics.

[Example]

This clears the DHCP snooping statistics.

```
SWX3220#clear ip dhcp snooping statistics
```

Chapter 7

Layer 3 functions

7.1 IPv4 address management

7.1.1 Set IPv4 address

[Syntax]

ip address *ip_address*/*mask* [secondary] [label *textline*]
ip address *ip_address netmask* [secondary] [label *textline*]
no ip address *ip_address*/*mask* [secondary]
no ip address *ip_address netmask* [secondary]
no ip address

[Keyword]

label	:	Set label as IPv4 address
secondary	:	Set as the secondary address

[Parameter]

ip_address	:	A.B.C.D IPv4 address
mask	:	<1-31> Number of mask bits
netmask	:	A.B.C.D Netmask in IPv4 address format
textline	:	Label (maximum 64 characters)

[Initial value]

None

[Input mode]

interface mode

[Description]

Specifies the IPv4 address and net mask for the VLAN interface.

For IPv4 addresses, one primary address and four secondary addresses can be set in one VLAN interface.

Up to 256 IPv4 addresses can be configured for the system overall.

A primary address must be set before configuring a secondary address.

If this command is executed with the "no" syntax, the specified IPv4 address is deleted. If no IPv4 address is specified, all IPv4 addresses are deleted.

You cannot delete a primary address while a secondary address is set.

If a label is specified, it is shown in the "IPv4 address" field by the **show interface** command.

[Note]

It is not possible to assign an IPv4 address of the same subnet to multiple interfaces.

[Example]

Specify 192.168.1.100 as the IP address for VLAN #1.

```
SWX3220(config)#interface vlan1
SWX3220(config-if)#ip address 192.168.1.100/24
```

7.1.2 Show IPv4 address

[Syntax]

show ip interface [*interface*] **brief**

[Parameter]

interface	:	VLAN interface name

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the IPv4 address for each interface.

The following content is shown.

- IPv4 address
  - For secondary addresses, “(secondary)” is appended to the end of IPv4 addresses.
  - If an IPv4 address has been specified by the **ip address dhcp** command, an "*" is shown added before the displayed IPv4 address.
  - If the IPv4 address is not specified after setting the **ip address dhcp** command (such as while searching for the server), then "searching" is shown.
  - If the **ip address** command has not been set, the indication "unassigned" is shown.
- Physical layer status
- Data link layer status

If an interface is specified, information for that interface is shown. If the interface is omitted, information is shown for all interfaces for which an IPv4 address can be specified.

[Note]

An error occurs if the specified interface is one to which an IP address cannot be assigned.

[Example]

Show the IP address of every VLAN interface.

```
SWX3220>show ip interface brief
Interface      IP-Address                      Admin-Status          Link-Status
vlan1          192.168.1.100/24
               192.168.101.100/24 (secondary)  up                    up
vlan2          192.168.2.100/24                up                    down
vlan3          unassigned                      up                    down
```

7.1.3 Automatically set IPv4 address by DHCP client

[Syntax]

ip address dhcp [hostname *hostname*]
no ip address

[Keyword]

hostname	:	Set host name of DHCP server

[Parameter]

hostname	:	Host name or IPv4 address (A.B.C.D)

[Initial value]

none

[Input mode]

interface mode

[Description]

Using the DHCP client, assigns the IPv4 address granted by the DHCP server to the VLAN interface.

If the DHCP server is specified, the HostName option (option code 12) can be added to the Discover/Request message.

If an IPv4 address has been obtained, you can execute the **no ip address** command to send a release message for the obtained IP address to the DHCP server.

A secondary address cannot be set for interfaces that are set as DHCP clients.

If this command is executed with the "no" syntax, the DHCP client setting is deleted.

[Note]

The lease time requested from the DHCP server is fixed at 72 hours. However, the actual lease time will depend on the setting of the DHCP server.

Even if this command is used to obtain the default gateway, DNS server, and default domain name from the DHCP server, the settings of the **ip route, dns-client name-server, dns-client domain-name** commands take priority.

If an IPv4 address cannot be obtained from the DHCP server even by using this command, then an IPv4 link local address (169.254.xxx.xxx/16) is automatically assigned only to VLAN interfaces for which the Auto IP function is enabled.

This command cannot be used if the stack function is enabled and the stack port is using the Auto IP function.

[Example]

Use the DHCP client to assign an IPv4 address to VLAN #100.

```
SWX3220(config)#interface vlan100
SWX3220(config-if)#ip address dhcp
```

7.1.4 Show DHCP client status

[Syntax]

show dhcp lease

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the DHCP client status. The following items are shown.

- Interface that is operating as a DHCP client
- Assigned IPv4 address
- Lease expiration time
- Lease renewal request time
- Lease rebinding time
- DHCP server name
- Information obtained as DHCP options
  - Net mask
  - Default gateway
  - Lease time
  - DNS server
  - DHCP server ID
  - Domain name

[Note]

This command cannot be used if the stack function is enabled.

[Example]

Show the current DHCP client status.

```
SWX3220>show dhcp lease
Interface vlan1
-------------------------------------------------------------------------------
IP Address:                     192.168.100.2
Expires:                        2018/01/01 00:00:00
Renew:                          2018/01/01 00:00:00
Rebind:                         2018/01/01 00:00:00
Server:
Options:
  subnet-mask                   255.255.255.0
  default-gateway               192.168.100.1
  dhcp-lease-time               259200
  domain-name-servers           192.168.100.1
  dhcp-server-identifier        192.168.100.1
  domain-name                   example.com
```

7.1.5 Set auto IP function

[Syntax]

auto-ip *switch*
no auto-ip

[Parameter]

switch : Behavior of the auto IP function

Setting value	Description
enable	Enable the auto IP function
disable	Disable the auto IP function

[Initial value]

auto-ip disable

[Input mode]

interface mode

[Description]

For the VLAN interface, enables the Auto IP function which automatically generates the IPv4 link local address (169.254.xxx.xxx/16).

The Auto IP function works only if an IPv4 address cannot be obtained from the DHCP server after the **ip address dhcp** command is specified.

The Auto IP function can be enabled for only one VLAN interface.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

If an IPv4 address could be obtained from the DHCP server after the IPv4 link local address was determined, the IPv4 link local address is discarded, and the IPv4 address obtained from the DHCP server is used.

This command cannot be used if the stack function is enabled and the stack port is using the Auto IP function.

[Example]

Enable the Auto IP function for VLAN #2.

```
SWX3220(config)#interface vlan2
SWX3220(config-if)#auto-ip enable
```

7.2 IPv4 route control

7.2.1 Set static IPv4 route

[Syntax]

ip route *ip_address*/*mask gateway* [*number*]
ip route *ip_address*/*mask* null [*number*]
ip route *ip_address netmask gateway* [*number*]
ip route *ip_address netmask* null [*number*]
no ip route *ip_address*/*mask* [*gateway* [*number*]]
no ip route *ip_address*/*mask* [null [*number*]]
no ip route *ip_address netmask* [*gateway* [*number*]]
no ip route *ip_address netmask* [null [*number*]]

[Keyword]

null : Discard packet without forwarding it

[Parameter]

ip_address : A.B.C.D

IPv4 address

Set this to 0.0.0.0 if specifying the default gateway

mask : <1-31>

Number of mask bits

Set this to 0 if specifying the default gateway

netmask : A.B.C.D

Netmask in address format

Set this to 0.0.0.0 if specifying the default gateway

gateway : A.B.C.D

IPv4 address of gateway

number : <1-255>

Administrative distance (priority order when selecting route) (if omitted: 1)

Lower numbers have higher priority.

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Adds a static route for IPv4.

If this command is executed with the "no" syntax, the specified route is deleted.

[Example]

Set the default gateway to 192.168.1.1.

```
SWX3220(config)#ip route 0.0.0.0/0 192.168.1.1
```

For the destination 172.16.0.0/16, set the gateway to 192.168.2.1.

```
SWX3220(config)#ip route 172.16.0.0 255.255.0.0 192.168.2.1
```

7.2.2 Set number of equal-cost multi-path registrations

[Syntax]

maximum-paths *num*
no maximum-paths [*num*]

[Parameter]

num : <1-8>

Number of equal-cost multi-path registrations

[Initial value]

4

[Input mode]

global configuration mode

[Description]

Sets the number of equal-cost multi-path registrations.

The setting value of this command is the number of equal-cost multi-path routes that can be registered in the IPv4 and IPv6 routing tables and forwarding tables.

[Example]

Set the number of equal-cost multi-path registrations as 8.

```
SWX3220(config)#maximum-paths 8
```

7.2.3 Show IPv4 Forwarding Information Base

[Syntax]

show ip route [*ip_address*[/*mask*]]

[Parameter]

ip_address	:	A.B.C.D IPv4 address
mask	:	<0-32> Number of mask bits (if omitted: 32)

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the IPv4 Forwarding Information Base (FIB).

If the IPv4 address is omitted, the entire content of the FIB is shown.

If the IPv4 address or network address is specified, detailed information for the routing entry that matches the destination is shown.

[Example]

Show the entire IPv4 forwarding information base.

```
SWX3220>show ip route
Codes: C - connected, S - static
       * - candidate default

Gateway of last resort is 192.168.100.1 to network 0.0.0.0

S*      0.0.0.0/0 [1/0] via 192.168.100.1, vlan1
S       172.16.0.0/16 [1/0] via 192.168.200.240, vlan100
S       192.168.1.1/32 [1/0] is directly connected, vlan100
C       192.168.100.0/24 is directly connected, vlan1
C       192.168.200.0/24 is directly connected, vlan100
```

Show the route used for sending packets that are addressed to 192.168.100.10.

```
SWX3220>show ip route 192.168.100.10
Routing entry for 192.168.100.0/24
  Known via "connected", distance 0, metric 0, best
  * is directly connected, vlan1
```

7.2.4 Show IPv4 Routing Information Base

[Syntax]

show ip route database

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the IPv4 Routing Information Base (RIB).

[Example]

Show the IPv4 routing information base.

```
SWX3220>show ip route database
Codes: C - connected, S - static
       > - selected route, * - FIB route

S    *> 0.0.0.0/0 [1/0] via 192.168.100.1, vlan1
S    *> 172.16.0.0/16 [1/0] via 192.168.200.240, vlan100
S    *> 192.168.1.1/32 [1/0] is directly connected, vlan100
C    *> 192.168.100.0/24 is directly connected, vlan1
C    *> 192.168.200.0/24 is directly connected, vlan100

Gateway of last resort is not set
```

7.2.5 Show summary of the route entries registered in the IPv4 Routing Information Base

[Syntax]

show ip route summary

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows a summary of the route entries that are registered in the IPv4 Routing Information Base (RIB).

[Example]

Show a summary of the route entries that are registered in the IPv4 Routing Information Base.

```
SWX3220>show ip route summary
IP routing table name is Default-IP-Routing-Table(0)
IP routing table maximum-paths is 1
Route Source    Networks
connected       2
static          3
Total           5
```

7.2.6 Clear IPv4 route

[Syntax]

clear ip route *
clear ip route *ip_address*/*mask*

[Parameter]

ip_address	:	A.B.C.D IPv4 address
mask	:	<0-32> Number of mask bits

[Input mode]

privileged EXEC mode

[Description]

Clear the RIP and OSPFv2 route of the IPv4 forwarding table.

The first syntax clears all RIP and OSPFv2 routes.

The second syntax clears only the route within the network that was specified within the RIP and OSPFv2 routes.

[Example]

Clear all RIP and OSPFv2 routes of the IPv4 forwarding table.

```
SWX3220#clear ip route *
```

Of the RIP and OSPFv2 routes in the IPv4 forwarding table, clear only those that are included in 10.0.0.0/8.

```
SWX3220#clear ip route 10.0.0.0/8
```

7.3 ARP

7.3.1 Show ARP table

[Syntax]

show arp

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the ARP cache.

[Example]

Show the ARP cache.

```
SWX3220>show arp
 IP Address      MAC Address   Interface  Type
192.168.100.10  00a0.de00.0000 vlan1    dynamic
192.168.100.100 00a0.de00.0001 vlan1    static
```

7.3.2 Clear ARP table

[Syntax]

clear arp-cache

[Input mode]

privileged EXEC mode

[Description]

Clears the ARP cache.

[Example]

Clear the ARP cache.

```
SWX3220#clear arp-cache
```

7.3.3 Set static ARP entry

[Syntax]

arp *ip_address mac_address interface*
no arp *ip_address*

[Parameter]

ip_address	:	A.B.C.D IP address
mac_address	:	HHHH.HHHH.HHHH MAC address
interface	:	portN.M Physical interface name

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Creates a static group ARP entry.

If this command is executed with the "no" syntax, the specified entry is deleted.

[Example]

Create a static ARP entry of IP address 192.168.100.100 and MAC address 00a0.de00.0000 connected to port1.1.

```
SWX3220(config)#arp 192.168.100.100 00a0.de00.0000 port1.1
```

7.3.4 Set ARP timeout

[Syntax]

arp-ageing-timeout *time*
no arp-ageing-timeout [*time*]

[Parameter]

time	:	<1-3000> ARP entry ageing timeout (seconds)

[Initial value]

arp-ageing-timeout 300

[Input mode]

interface mode

[Description]

Changes the length of time that ARP entries are maintained in the applicable VLAN interface. ARP entries that are not received within this length of time are deleted.

If this command is executed with the "no" syntax, the ARP entry timeout is set to 300 seconds.

[Example]

Change the ARP entry ageing timeout for VLAN #1 to ten minutes.

```
SWX3220(config)#interface vlan1
SWX3220(config)#arp-aging-timeout 600
```

7.3.5 ARP request transmission method settings during ARP timeout

[Syntax]

arp-ageing-timeout request *mode*
no arp-ageing-timeout request

[Parameter]

mode : ARP request transmission method

Setting value	Description
unicast	Transmits ARP request that is transmitted during ARP timeout, via unicast
broadcast	Transmits ARP request that is transmitted during ARP timeout via broadcast

[Initial value]

arp-ageing-timeout request unicast

[Input mode]

interface mode

[Description]

Sets the ARP request method that is transmitted when the ARP entry timeout has expired for the target VLAN interface.

If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

Transmits the ARP request that is transmitted when ARP entry timeout for VLAN #1 has expired, via broadcast.

```
SWX3220(config)#interface vlan1
SWX3220(config)#arp-aging-timeout request broadcast
```

7.4 IPv4 forwarding control

7.4.1 IPv4 forwarding settings (system)

[Syntax]

ip forwarding *switch*
no ip forwarding [*switch*]

[Parameter]

switch : IPv4 packet forwarding settings

Setting value	Description
enable	Enable forwarding of IPv4 packets
disable	Disable forwarding of IPv4 packets

[Initial value]

ip forwarding enable

[Input mode]

global configuration mode

[Description]

Enables or disables forwarding of IPv4 packets.

If this is executed with the "no" syntax, the setting returns to the default.

7.4.2 IPv4 forwarding settings (interface)

[Syntax]

ip forwarding *switch*
no ip forwarding [*switch*]

[Parameter]

switch : IPv4 packet forwarding settings

Setting value	Description
enable	Enable forwarding of IPv4 packets
disable	Disable forwarding of IPv4 packets

[Initial value]

ip forwarding enable

[Input mode]

interface mode

[Description]

Enables or disables forwarding of IPv4 packets.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be specified only for VLAN interfaces.

If IPv4 packet forwarding is enabled on a system level and IPv4 packet forwarding is enabled for the VLAN interface via this command, IPv4 packet forwarding is carried out on that VLAN interface.

7.4.3 Show IPv4 forwarding settings

[Syntax]

show ip forwarding

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the IPv4 packet forwarding settings.

[Example]

Shows the IPv4 packet forwarding settings.

```
SWX3220>show ip forwarding
IP forwarding is on
```

7.4.4 IPv4 directed broadcast forwarding settings

[Syntax]

ip directed-broadcast *switch*
no ip directed-broadcast

[Parameter]

switch : IPv4 directed broadcast forwarding settings

Setting value	Description
enable	Enables IPv4 directed broadcast forwarding settings
disable	Disables IPv4 directed broadcast forwarding settings

[Initial value]

ip directed-broadcast disable

[Input mode]

interface mode

[Description]

This configures the forwarding of directed broadcasts for the VLAN interface from other VLAN interfaces.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be specified only for VLAN interfaces. This only works if an IP address is assigned to the VLAN interface.

Use caution, as this may be exploited by Smurf attacks and similar attacks when directed broadcast forwarding is enabled.

[Example]

This enables directed broadcast forwarding for VLAN #2.

```
SWX3220(config)#interface vlan2
SWX3220(config-if)#ip directed-broadcast enable
```

7.4.5 MTU setting

[Syntax]

mtu *mtu*
no mtu

[Parameter]

mtu : <68-9216>

Maximum packet size that can be transmitted

[Initial value]

mtu 1500

[Input mode]

interface mode

[Description]

Sets the maximum value (MTU) for the size of packets that can be transmitted from the VLAN interface.

Eligible packets are those which are transmitted from this product, as well as those which are L3 forwarded (routing). Ethernet frames that are L2 forwarded by this product are not eligible.

When L3 forwarding packets for which the total length of the IPv4 header exceeds the MTU value, the packets are IP fragmented and then transmitted.

When L3 forwarding packets for which the payload length of the IPv6 header exceeds the MTU value, an ICMPv6 error is sent back and the packets are discarded.

Since packets that fit into the Ethernet frame length set by the mru command are eligible for routing, you must use the mru command to adjust the length of Ethernet frames that can be received when routing jumbo frames.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be specified only for VLAN interface.

You can specify up to seven different values for the MTU besides the default value.

On VLAN interfaces for which ipv6 enable has been specified, the MTU can be set within a range of <1280-9216>.

You cannot specify the ipv6 enable command for a VLAN interface that is set to an MTU value less than 1280.

[Example]

This allows jumbo frames of up to 10240 bytes between the LAN port #1 belonging to VLAN interface #1 and the LAN port #2 belonging to VLAN interface #2, and sets the MTU to 2000 bytes.

```
SWX3220(config)#interface port1.1-2
SWX3220(config-if)#mru 10240
SWX3220(config-if)#interface vlan1-2
SWX3220(config-if)#mtu 2000
```

7.5 IPv4 ping

7.5.1 IPv4 ping

[Syntax]

ping *host* [repeat *count*] [size *datalen*] [timeout *timeout*] [source *ip_address*]

[Keyword]

repeat	:	Specifies the number of times to execute
size	:	Specifies the length of the ICMP payload (byte units)
timeout	:	Specifies the time to wait for a reply after transmitting the specified number of Echo requests
source	:	Sets the source address for ICMP packets

[Parameter]

host : Target to which ICMP Echo is sent

Host name, or target IP address (A.B.C.D)

count : Number of times to execute (if omitted: 5)

Setting value	Description
<1-2147483647>	Execute the specified number of times
continuous	Execute repeatedly until Ctrl+C is entered

datalen : <36-18024>

Length of the ICMP payload (if omitted: 56)

timeout : <1-65535>

Time to wait for a reply (if omitted: 2)

This is ignored if the number of times to execute is specified as "continuous"

ip_address : A.B.C.D

IPv4 address

[Input mode]

privileged EXEC mode

[Description]

Send ICMP Echo to the specified host, and wait for ICMP Echo Reply.

If there is a reply, show it. Show statistical information when the command ends.

[Example]

Ping the IP address 192.168.100.254 three times with a data size of 120 bytes.

```
SWX3220#ping 192.168.100.254 repeat 3 size 120
PING 192.168.100.254 (192.168.100.254): 120 data bytes
128 bytes from 192.168.100.254: seq=0 ttl=255 time=8.368 ms
128 bytes from 192.168.100.254: seq=1 ttl=255 time=9.946 ms
128 bytes from 192.168.100.254: seq=2 ttl=255 time=10.069 ms

--- 192.168.100.254 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 8.368/9.461/10.069 ms
```

7.5.2 Check IPv4 route

[Syntax]

traceroute *host*

[Parameter]

host : Destination for which to check the route

Host name, or target IP address (A.B.C.D)

[Input mode]

privileged EXEC mode

[Description]

Shows information for the route to the specified host.

[Example]

Check the route to 192.168.100.1.

```
SWX3220#traceroute 192.168.100.1
traceroute to 192.168.100.1 (192.168.100.1), 30 hops max
 1  192.168.10.1 (192.168.10.1)  0.563 ms  0.412 ms  0.428 ms
 2  192.168.20.1 (192.168.20.1)  0.561 ms  0.485 ms  0.476 ms
 3  192.168.30.1 (192.168.30.1)  0.864 ms  0.693 ms  21.104 ms
 4  192.168.40.1 (192.168.40.1)  0.751 ms  0.783 ms  0.673 ms
 5  192.168.50.1 (192.168.50.1)  7.689 ms  7.527 ms  7.168 ms
 6  192.168.100.1 (192.168.100.1)  33.948 ms  10.413 ms  7.681 ms
```

7.6 IPv6 address management

7.6.1 Set IPv6

[Syntax]

ipv6 *switch*
no ipv6

[Parameter]

switch : Behavior of the IPv6

Setting value	Description
enable	Enable the IPv6
disable	Disable the IPv6

[Initial value]

ipv6 disable

[Input mode]

interface mode

[Description]

Enables IPv6 for the VLAN interface and automatically sets the link local address.

IPv6 addresses can be assigned to a maximum of 256 VLAN interfaces.

If IPv6 is disabled, related settings are also simultaneously deleted.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

The automatically-specified link local address can be viewed by using the **show ipv6 interface brief** command.

This command cannot be used if the stack function is enabled.

[Example]

Enable IPv6 for VLAN #1.

```
SWX3220(config)#interface vlan1
SWX3220(config-if)#ipv6 enable
```

7.6.2 Set IPv6 address

[Syntax]

ipv6 address *ipv6_address*/*prefix_len*
no ipv6 address *ipv6_address*/*prefix_len*
no ipv6 address

[Parameter]

ipv6_address	:	X:X::X:X IPv6 address
prefix_len	:	<0-127> IPv6 prefix length

[Input mode]

interface mode

[Description]

Specifies the IPv6 address and prefix length for the VLAN interface.

An IPv6 address can be set for a VLAN interface for which the **ipv6 enable** command has been set.

This command can be used with the **ipv6 address autoconfig**, **ipv6 address dhcp** and **ipv6 address pd** commands.

For IPv6 addresses, up to five global addresses (including RA settings, DHCPv6 clients and the settings for IPv6 addresses that use DHCPv6-PD) and one link local address can be set in one VLAN interface.

Up to 256 IPv6 addresses can be configured for the system overall (excepting link local addresses that are automatically assigned).

If this command is executed with the "no" syntax, the specified IPv6 address is deleted. If no IPv6 address is specified, all IPv6 addresses (including RA settings, DHCPv6 clients and the settings for IPv6 addresses that use DHCPv6-PD) are deleted.

[Note]

It is not possible to assign an IPv6 address of the same subnet to multiple interfaces.

This command cannot be used if the stack function is enabled.

[Example]

Specify 2001:db8:1::2 as the IPv6 address for VLAN #1.

```
SWX3220(config)#interface vlan1
SWX3220(config-if)#ipv6 address 2001:db8:1::2/64
```

7.6.3 Set RA for IPv6 address

[Syntax]

ipv6 address autoconfig [stateless]
no ipv6 address autoconfig

[Keyword]

stateless	:	Operates a stateless DHCPv6.

[Initial value]

none

[Input mode]

interface mode

[Description]

Uses RA to specify an IPv6 address for the VLAN interface.

RA can be specified only for the VLAN interface for which the **ipv6 enable** command has been specified.

This command can be used with the **ipv6 address** and **ipv6 address pd** commands.

This cannot be set for VLAN interface that has already been set using the **ipv6 address dhcp** or **dhcpv6-server** commands (only for models that support a DHCPv6 server).

If an RA with a valid router lifetime is received after enabling this command, the address of the device that transmitted the RA is added to the default gateway.

Also, if an RA with a router lifetime of "0" is received, the address of the device that transmitted the RA is deleted from the default gateway.

However, if the **ipv6 nd accept-ra-default-routes disable** command has been set, nothing is added to the default gateway based on the RA.

If "stateless" is specified, a DHCPv6 "Information-request" is sent and the unit operates in DHCPv6 stateless mode.

If "stateless" is specified, this cannot be set for a VLAN interface for which the **ipv6 dhcp client pd** command has already been set.

Only one DHCPv6 stateless can be set for one VLAN interface.

This command for which "stateless" has been specified can be set for a maximum of 8 VLAN interface.

If you overwrite the **ipv6 address autoconfig stateless** command after setting it with the **ipv6 address autoconfig** command, the DHCPv6 stateless mode is stopped.

If this command is executed with the "no" syntax, the RA setting is deleted.

[Note]

If "stateless" is specified regardless of whether the received RA "O" flag is on or off, DHCPv6 stateless operations are enabled.

This requests "OPTION_DNS_SERVERS" (option code 23) and "OPTION_DOMAIN_LIST" (option code 24) to the DHCPv6 server during stateless operations.

When multiple options are returned from the DHCPv6 server, up to three can be obtained for a DNS server and up to six can be obtained for a domain list.

You can use the **show ipv6 dhcp interface** to confirm the DNS servers or domain lists obtained due to requests made when operating in stateless mode.

If there is no period (dot) at the end of the domain name of a domain list that was obtained, "." is appended.

Even when this command is used to obtain the DNS server or query domain list from the DHCPv6 server, the settings of the **dns-client name-server** and **dns-client domain-list** commands take priority.

You can use the **show dns-client** command to confirm the DNS servers or domain lists configured in the system.

This command cannot be used if the stack function is enabled.

[Example]

Use RA to set the IPv6 address for VLAN #1.

```
SWX3220(config)#interface vlan1
SWX3220(config-if)#ipv6 address autoconfig
```

7.6.4 Set dynamic IPv6 addresses with a DHCPv6 client

[Syntax]

ipv6 address dhcp
no ipv6 address dhcp

[Initial value]

None

[Input mode]

interface mode

[Description]

Using the DHCPv6 client, this sets the IPv6 address granted by the DHCPv6 server for the VLAN interface.

This command can be set for a VLAN interface for which the **ipv6 enable** command has been set.

Only one address can be set with this command for one VLAN interface.

This command can be used with the **ipv6 address** and **ipv6 address pd** commands.

This command can be specified for a maximum of eight VLAN interface.

This cannot be set for VLAN interface that has already been set using the **ipv6 dhcp client pd**, **ipv6 address autoconfig** or **dhcpv6-server** commands (only for models that support a DHCPv6 server).

If an IPv6 address has been obtained, you can execute the **no ipv6 address dhcp** command to send a release message for the obtained IPv6 address to the DHCPv6 server.

If this command is executed with the "no" syntax, the DHCPv6 client setting is deleted.

If the **ipv6** command is set to "disable", this command is also deleted.

[Note]

If the IPv6 address is automatically set using this command, the prefix length is set to "/128".

If this command is set regardless of whether the received RA "M" flag is on or off, DHCPv6 stateful operations (IA_NA) are enabled.

The DHCPv6 client requests "OPTION_DNS_SERVERS" (option code 23) and "OPTION_DOMAIN_LIST" (option code 24) to the DHCPv6 server.

When multiple options are returned from the DHCPv6 server, up to three can be obtained for a DNS server and up to six can be obtained for a domain list.

You can use the **show ipv6 dhcp interface** command to confirm the DNS servers or domain lists obtained due to requests made by the DHCPv6 client.

If there is no period (dot) at the end of the domain name of a domain list that was obtained, "." is appended.

Even when this command is used to obtain the DNS server or query domain list from the DHCPv6 server, the settings of the **dns-client name-server** and **dns-client domain-list** commands take priority.

You can use the **show dns-client** command to confirm the DNS servers or domain lists configured in the system.

If an RA with a valid router lifetime is received after enabling this command, the address of the device that transmitted the RA is added to the default gateway.

Also, if an RA with a router lifetime of "0" is received, the address of the device that transmitted the RA is deleted from the default gateway.

However, if the **ipv6 nd accept-ra-default-routes disable** command has been set, nothing is added to the default gateway based on the RA.

This command cannot be used if the stack function is enabled.

[Example]

This assigns an IPv6 address to VLAN #100 via the DHCPv6 client.

```
SWX3220(config)#interface vlan100
SWX3220(config-if)#ipv6 address dhcp
```

7.6.5 Set an IPv6 address using DHCPv6-PD

[Syntax]

ipv6 address pd *pd_prefixname pd_ipv6_address/prefix_len*
no ipv6 address pd *pd_prefixname pd_ipv6_address/prefix_len*

[Parameter]

pd_prefixname	:	Prefix name set on the DHCPv6-PD client (ipv6 dhcp client pd command) Up to 32 single-byte alphanumeric characters, including dots, hyphens and underscores
pd_ipv6_address	:	X:X::X:X IPv6 address based on prefix obtained from DHCPv6-PD client Sets the lower level (remaining) portion for the prefix obtained from a DHCPv6-PD client "0" must be specified for the prefix obtained from DHCPv6-PD client
prefix_len	:	<0-127> IPv6 prefix length

[Initial value]

None

[Input mode]

interface mode

[Description]

Specifies the IPv6 address and prefix length for the VLAN interface.

An IPv6 address can be set for a VLAN interface for which the **ipv6 enable** command has been set.

This generates an IPv6 address based on the prefix obtained using the DHCPv6-PD client function.

The generated IPv6 address can be checked by using the **show ipv6 interface** command.

This command can be used with the **ipv6 address**, **ipv6 address autoconfig** and **ipv6 address dhcp** commands.

For IPv6 addresses, up to five global addresses (including RA settings and DHCPv6 client) and one link local address can be set in one VLAN interface.

Up to 256 IPv6 addresses can be configured for the system overall (excepting link local addresses that are automatically assigned).

If this command is executed with the "no" syntax, the specified IPv6 address is deleted.

[Note]

If prefix information cannot be obtained via the DHCPv6-PD client function, the IPv6 address is not generated.

The IPv6 address is not generated if the combination of the prefix information and lower (host) part of the address is incorrect, or if the subnet is duplicated across interfaces.

This command cannot be used if the stack function is enabled.

[Example]

This obtains the IPv6 prefix for VLAN #100 via the DHCPv6-PD client.

The prefix name "PD_VLAN100" that was obtained is used to set the IPv6 address for VLAN #200.

In this example, we assume that "2001:db8:1:aaf0::/60" is obtained with "PD_VLAN100".

The following settings are used to set "2001:db8:1:aaf2::1/64" for VLAN #200.

```
SWX3220(config)#interface vlan100
SWX3220(config-if)#ipv6 dhcp client pd PD_VLAN100
SWX3220(config)#interface vlan200
SWX3220(config-if)#ipv6 address pd PD_VLAN100 ::2:0:0:0:1/64
```

7.6.6 Set DHCPv6-PD client

[Syntax]

ipv6 dhcp client pd *prefixname*
no ipv6 dhcp client pd

[Parameter]

prefixname	:	Internal name attached to assigned prefix Up to 32 single-byte alphanumeric characters, including dots, hyphens and underscores

[Initial value]

None

[Input mode]

interface mode

[Description]

Enables the DHCPv6-PD client function on the applicable interface, and configures the client to request prefix assignments.

This command can be set for a VLAN interface for which the **ipv6 enable** command has been set.

The prefix obtained using the *prefixname* of this command can be used as shown below.

- Use the prefix obtained with the **ipv6 address pd** command to set a IPv6 address.
- Use the prefix obtained with the **range** command in DHCPv6 mode to set an IPv6 address range for dynamic assignment on a DHCPv6 server. (Only for models that support a DHCPv6 server.)
- Use the prefix obtained with the **prefix-delegation** command in DHCPv6 mode to reassign a prefix on a DHCPv6 server. (Only for models that support a DHCPv6 server.)

Only one address can be set with this command for one VLAN interface.

This command can be specified for a maximum of eight VLAN interface.

This cannot be set for a VLAN interface that has already been set using the **ipv6 address dhcp**, **ipv6 address autoconfig stateless** or **dhcpv6-server** commands (only for models that support a DHCPv6 server).

If an IPv6 prefix has been obtained, you can execute the **no ipv6 dhcp client pd** command to send a release message for the obtained prefix to the DHCPv6 server.

If this command is executed with the "no" syntax, the DHCPv6-PD client setting is deleted.

If the **ipv6** command is set to "disable", this command is also deleted.

[Note]

If this command is set regardless of whether the received RA "M" flag is on or off, DHCPv6-PD stateful operations (IA_PD) are enabled.

The DHCPv6-PD client requests "OPTION_DNS_SERVERS" (option code 23) and "OPTION_DOMAIN_LIST" (option code 24) to the DHCPv6 server.

When multiple options are returned from the DHCPv6 server, up to three can be obtained for a DNS server and up to six can be obtained for a domain list.

You can use the **dns-server** and **domain-name** commands in DHCPv6 mode for DNS servers and domain lists obtained by a DHCPv6-PD client. (Only for models that support a DHCPv6 server.)

You can use the **show ipv6 dhcp interface** command to confirm the DNS servers or domain lists obtained due to requests made by the DHCPv6-PD client.

If there is no period (dot) at the end of the domain name of a domain list that was obtained, "." is appended.

Even when this command is used to obtain a DNS server or query domain list from the DHCPv6-PD server, the settings of the **dns-client name-server** and **dns-client domain-list** commands take priority.

You can use the **show dns-client** command to confirm the DNS servers or domain lists configured in the system.

If an RA with a valid router lifetime is received after enabling this command, the address of the device that transmitted the RA is added to the default gateway.

Also, if an RA with a router lifetime of "0" is received, the address of the device that transmitted the RA is deleted from the default gateway.

However, if the **ipv6 nd accept-ra-default-routes disable** command has been set, nothing is added to the default gateway based on the RA.

This command cannot be used if the stack function is enabled.

[Example]

This obtains the IPv6 prefix for VLAN #100 via the DHCPv6-PD client.

The prefix name "PD_VLAN100" that was obtained is used to set the IPv6 address for VLAN #200.

In this example, we assume that "2001:db8:1:aaf0::/60" is obtained with "PD_VLAN100".

The following settings are used to set "2001:db8:1:aaf2::1/64" for VLAN #200.

```
SWX3220(config)#interface vlan100
SWX3220(config-if)#ipv6 dhcp client pd PD_VLAN100
SWX3220(config)#interface vlan200
SWX3220(config-if)#ipv6 address pd PD_VLAN100 ::2:0:0:0:1/64
```

7.6.7 Set automatic registration of default gateway using RA

[Syntax]

ipv6 nd accept-ra-default-routes *switch*
no ipv6 nd accept-ra-default-routes

[Parameter]

switch : Settings for automatic registration of default gateway using RA

Setting value	Description
enable	Enable setting of automatic registration for the default gateway using RA
disable	Disable setting of automatic registration for the default gateway using RA

[Initial value]

ipv6 nd accept-ra-default-routes enable

[Input mode]

interface mode

[Description]

Enables/disables the setting of automatic registration of a IPv6 default gateway, based on the starting address of the router advertisement (RA) received by the applicable interface.

This command can be set for a VLAN interface for which the **ipv6 enable** command has been set.

If this command is executed with the "no" syntax, the setting returns to the default value.

If the **ipv6** command is set to "disable", this command is also deleted.

[Note]

If an RA was received when the **ipv6 address dhcp**, **ipv6 dhcp client pd** or **ipv6 address autoconfig** command was set, the setting for this command takes priority.

If these commands have not been set, default gateways are not automatically registered, even if this command is set to "enable".

This command cannot be used if the stack function is enabled.

[Example]

Disables setting of automatic registration for the default gateway using RA on VLAN #100.

```
SWX3220(config)#interface vlan100
SWX3220(config-if)#ipv6 nd accept-ra-default-routes disable
```

7.6.8 Show IPv6 address

[Syntax]

show ipv6 interface [*interface*] **brief**

[Parameter]

interface	:	VLAN interface name Interface to show

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the IPv6 address for each interface.

- IPv6 address
  - If an IPv6 address has been dynamically specified by the **ipv6 address dhcp** command, an asterisk is shown added before the displayed IPv6 address.
  - If the IPv6 address is not specified after setting the **ipv6 address dhcp** command (such as while searching for the server), "searching" is shown.
  - If the address uses *pd_prefixname* as set by the **ipv6 address pd** command, an asterisk is shown added before the displayed IPv6 address.
  - If an IPv6 address has not been set, this will be "unassigned."
- Physical layer status
- Data link layer status

If an interface is specified, information for that interface is shown. If the interface is omitted, information is shown for all interfaces for which an IPv6 address is specified.

[Note]

An error occurs if the specified interface is one to which an IPv6 address cannot be assigned.

This command cannot be used if the stack function is enabled.

[Example]

Show the IPv6 address for all VLAN interface.

```
SWX3220>show ipv6 interface brief
Interface        IPv6-Address                                Admin-Status
Link-Status
vlan1            2001:db8:1::2/64
                 2001:db8:2::2/64
                 fe80::2a0:deff:fe:2/64                      up                    up
vlan2            2001:db8:2::2/64
                 fe80::2a0:deff:fe:2/64                      up
down
vlan3            unassigned                                  up
down
```

7.6.9 Show DHCPv6 client status

[Syntax]

show ipv6 dhcp interface [*ifname*]

[Parameter]

ifname : VLAN interface name

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

Shows the DHCPv6 client status.

If *ifname* is not specified, this shows information for all VLAN interface.

[Note]

This command cannot be used if the stack function is enabled.

[Example]

Shows the DHCPv6 client status for all VLAN interface.

```
SWX3220#show ipv6 dhcp interface
Interface vlan1
  Client Type        : IA_NA
  Address            : 2001:db8:1:aa10::dd2d
  IAID               : 0f28924a
  DUID               : 000100010000000000a0de000000
  preferred lifetime : 604800
  valid lifetime     : 2592000
  expires            : 2023/4/19 07:25:48

Interface vlan2
  Client Type        : Stateless
  DUID               : 000100012ce737dbac44f284efdd
  DNS Server         : 2001:db8:1:bb10::100
  DNS Server         : 2001:db8:1:bb10::200
  Domain Name        : example.com.

Interface vlan100
  Client Type        : IA_PD
  Prefix name        : PD_VLAN100
  prefix             : 2001:db8:1:aaf0::/60
  IAID               : 0f28924a
  DUID               : 000100010000000000a0de000000
  preferred lifetime : 604800
  valid lifetime     : 2592000
  expires            : 2023/4/19 08:08:04
  DNS Server         : 2001:db8:2::100
  DNS Server         : 2001:db8:2::200
  Domain Name        : example.com.
```

7.6.10 Reset DHCPv6 client

[Syntax]

clear ipv6 dhcp client *ifname*

[Parameter]

ifname : VLAN interface name

[Input mode]

privileged EXEC mode

[Description]

Clears the DHCPv6 client that's operating on the applicable interface.

When you execute this command, the DHCPv6 information that was acquired on the applicable interface is erased.

At this time, release messages acquired for the IPv6 address are sent to the DHCPv6 server.

After this, the request to the DHCPv6 server is transmitted again, to make the settings again for the DHCPv6 client.

When using a DHCPv6-PD client, if the prefix acquired via the **ipv6 address pd** command is used,the interface address that was set is configured again.

When the information acquired via the DHCPv6 mode **range** command, **prefix-delegation** command, **dns-server** command or **domain-name** command by means of the DHCPv6 server function is used, the DHCPv6 server function is also reconfigured. (Only for models that support a DHCPv6 server.)

[Note]

This command cannot be used if the stack function is enabled.

[Example]

Clears the DHCPv6 client for VLAN #100.

```
SWX3220#clear ipv6 dhcp client vlan100
```

7.6.11 Set ND prefix received when configuring a DHCPv6 client

[Syntax]

ipv6 dhcp client nd-prefix *prefix_len*
no ipv6 dhcp client nd-prefix

[Parameter]

prefix_len	:	<1-127> Length of ND prefix received

[Initial value]

None

[Input mode]

interface mode

[Description]

For a VLAN interface on which an IPv6 address (prefix /128) is automatically set via the **ipv6 address dhcp** command, all ND (Neighbor Discovery) packets are received regardless of the IPv6 address from which they are transmitted.

When this command is set, both addresses listed below are compared within the set prefix range when the ND packets are received. For identical segments, the ND packet is received. For differing segments, the ND packet is discarded.

- IPv6 addresses automatically configured via the **ipv6 address dhcp** command
- Source IPv6 addresses for ND packets received

This command can be set for a VLAN interface for which the **ipv6 enable** command has been set.

The ND packets targeted by this command are limited to NS (Neighbor Solicitation) and NA (Neighbor Advertisement).

If this command is executed with the "no" syntax, the ND prefix received when the DHCPv6 client is set is deleted.

[Note]

This only works for a VLAN interface on which an IPv6 address (prefix /128) is automatically set via the **ipv6 address dhcp** command.

This command cannot be used if the stack function is enabled.

[Example]

This allows the receipt of only ND packets from subnet /64, on VLAN #1 for which an IPv6 address has been set automatically via the **ipv6 address dhcp** command.

```
SWX3220(config)#interface vlan1
SWX3220(config-if)#ipv6 dhcp client nd-prefix 64
```

7.7 IPv6 route control

7.7.1 Set IPv6 static route

[Syntax]

ipv6 route *ipv6_address*/*prefix_len gateway* [*number*]
ipv6 route *ipv6_address*/*prefix_len* null [*number*]
no ipv6 route *ipv6_address*/*prefix_len* [*gateway* [*number*]]
no ipv6 route *ipv6_address*/*prefix_len* [null [*number*]]

[Keyword]

null	:	Discard packet without forwarding it

[Parameter]

ipv6_address	:	X:X::X:X IPv6 address Set this to :: (abbreviated 0:0:0:0:0:0:0:0) if specifying the default gateway
prefix_len	:	<1-127> IPv6 prefix Set this to 0 if specifying the default gateway
gateway	:	X:X::X:X IPv6 address of gateway If you specify an IPv6 link local address, you must also specify the output interface (fe80::X%vlanN format)
number	:	<1-255> Management route (priority order when selecting route) (if omitted: 1) Lower numbers have higher priority.

[Input mode]

global configuration mode

[Description]

Adds a static route for IPv6.

If this command is executed with the "no" syntax, the specified route is deleted.

[Note]

For the default gateway setting, the static route setting takes priority over the RA setting.

This command cannot be used if the stack function is enabled.

[Example]

For the destination 2001:db8:2::/64, set the gateway to 2001:db8:1::1.

```
SWX3220(config)#ipv6 route 2001:db8:2::/64 2001:db8:1::1
```

Set the default gateway to fe80::2a0:deff:fe:1 on VLAN #1.

```
SWX3220(config)#ipv6 route ::/0 fe80::2a0:deff:fe:1%vlan1
```

7.7.2 Show IPv6 Forwarding Information Base

[Syntax]

show ipv6 route [*ipv6_address*[/*prefix_len*]]

[Parameter]

ipv6_address	:	X:X::X:X IPv6 address
mask	:	<0-128> IPv6 prefix length (if omitted: 128)

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the IPv6 Forwarding Information Base (FIB).

If the IPv6 address is omitted, the entire content of the FIB is shown.

If the IPv6 address or network address is specified, detailed information for the routing entry that matches the destination is shown.

[Note]

This command cannot be used if the stack function is enabled.

[Example]

Show the entire IPv6 forwarding information base.

```
SWX3220>show ipv6 route
Codes: C - connected, S - static
Timers: Uptime

S      ::/0 [1/0] via fe80::2a0:deff:fe:1, vlan1, 00:03:08
C      2001:db8:1::/64 via ::, vlan1, 00:01:10
S      2001:db8:2::/64 [1/0] via 2001:db8:1::1, vlan1, 00:01:52
C      fe80::/64 via ::, vlan1, 00:03:08
```

Show the route used for sending packets that are addressed to 2001:db8:1::2.

```
SWX3220>show ipv6 route 2001:db8:1::2
Routing entry for 2001:db8:1::/64
  Known via "connected", distance 0, metric 0, best
  Last update 00:18:27 ago
  * directly connected, vlan1
```

7.7.3 Show IPv6 Routing Information Base

[Syntax]

show ipv6 route database

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the IPv6 Routing Information Base (RIB).

[Note]

This command cannot be used if the stack function is enabled.

[Example]

Show the IPv6 routing information base.

```
SWX3220>show ipv6 route database
Codes: C - connected, S - static
       > - selected route, * - FIB route
Timers: Uptime

S   *> ::/0 [1/0] via fe80::2a0:deff:fe:1, vlan1, 00:21:39
C   *> 2001:db8:1::/64 via ::, vlan1, 00:19:41
S   *> 2001:db8:2::/64 [1/0] via 2001:db8:1::1, vlan1, 00:20:23
C   *> fe80::/64 via ::, vlan1, 00:21:39
```

7.7.4 Show summary of the route entries registered in the IPv6 Routing Information Base

[Syntax]

show ipv6 route summary

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows a summary of the route entries that are registered in the IPv6 Routing Information Base (RIB).

[Note]

This command cannot be used if the stack function is enabled.

[Example]

Show a summary of the IPv6 Routing Information Base.

```
SWX3220>show ipv6 route summary
IPv6 routing table name is Default-IPv6-Routing-Table(0)
IPv6 routing table maximum-paths is 1
Route Source    Networks
connected       2
```

```
static           2
Total            4
```

7.7.5 Clear IPv6 route

[Syntax]

clear ipv6 route *
clear ipv6 route *ipv6_address/prefix_len*

[Parameter]

ipv6_address	:	X:X::X:X IPv6 address
mask	:	<0-128> IPv6 prefix length

[Input mode]

privileged EXEC mode

[Description]

Clear the RIPng and OSPFv3 route of the IPv4 forwarding table.

The first syntax clears all RIPng and OSPFv3 routes.

The second syntax clears only the route within the network that was specified within the RIPng and OSPFv3 routes.

[Note]

This command cannot be used if the stack function is enabled.

[Example]

Clear all RIPng and OSPFv3 routes of the IPv4 forwarding table.

```
SWX3220#clear ipv6 route *
```

Of the RIPng and OSPFv3 routes in the IPv4 forwarding table, clear only those that are included in 2001:db8:1::/64.

```
SWX3220#clear ipv6 route 2001:db8:1::/64
```

7.8 Neighbor cache

7.8.1 Set static neighbor cache entry

[Syntax]

ipv6 neighbor *ipv6_address interface mac_address interface*
no ipv6 neighbor *ipv6_address interface*

[Parameter]

ipv6_address	:	X:X::X:X IPv6 address
interface	:	vlanN VLAN interface name
mac_address	:	HHHH.HHHH.HHHH MAC address
interface	:	portN.M Physical interface name

[Input mode]

global configuration mode

[Description]

Adds a static entry to the neighbor cache.

If this command is executed with the "no" syntax, the specified static entry is deleted.

[Note]

This command cannot be used if the stack function is enabled.

[Example]

Set the MAC address of IPv6 2001:db8:cafe::1 located at port1.1 of VLAN #1, in the Neighbor cache.

```
SWX3220(config)#ipv6 neighbor 2001:db8:cafe::1 vlan1 00a0.de80.cafe port1.1
```

7.8.2 Show neighbor cache table

[Syntax]

show ipv6 neighbors

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the neighbor cache table.

[Note]

This command cannot be used if the stack function is enabled.

[Example]

Show the neighbor cache table.

```
SWX3220>show ipv neighbors
 IPv6 Address                              MAC Address     Interface  Type
2001:db8:1:0:3538:5dc7:6bc4:1a23          0011.2233.4455   vlan1      dynamic
2001:db8:cafe::1                          00a0.de80.cafe   vlan1      static
fe80::0211:22ff:fe33:4455                 0011.2233.4455   vlan1      dynamic
fe80::6477:88ff:fe99:aabb                 6677.8899.aabb   vlan1      dynamic
```

7.8.3 Clear neighbor cache table

[Syntax]

clear ipv6 neighbors

[Input mode]

privileged EXEC mode

[Description]

Clears the neighbor cache.

[Note]

This command cannot be used if the stack function is enabled.

[Example]

Clear the neighbor cache.

```
SWX3220#clear ipv6 neighbors
```

7.9 IPv6 RA

7.9.1 Set IPv6 RA transmission

[Syntax]

ipv6 nd send-ra
no ipv6 nd send-ra

[Initial value]

None

[Input mode]

interface mode

[Description]

Sets the IPv6 RA for transmission.

If this command is executed with the "no" syntax, the setting returns to the default.

This command can be set for a VLAN interface for which the **ipv6** command is set to "enable".

If the **ipv6** command is set to "disable", this command is also deleted.

[Note]

This command cannot be used if the stack function is enabled.

[Example]

This sets IPv6 RA for transmission.

```
SWX3220(config-if)#ipv6 nd send-ra
```

7.9.2 Set prefix information advertised by RA

[Syntax]

ipv6 nd prefix *ipv6_address*/*prefix_len* [*valid preferred*] [off-link] [no-autoconfig]
no ipv6 prefix *ipv6_address*/*prefix_len*

[Keyword]

off-link	:	Advertises off-link. The Prefix Information option L flag is not set. When abbreviated, the L flag is set.
no-autoconfig	:	Automatically generate IPv6 addresses with no notification (advertisement). The Prefix Information option A flag is not set. When abbreviated, the A flag is set.

[Parameter]

ipv6_address	:	X:X::X:X IPv6 address
prefix_len	:	<0-128> IPv6 prefix length
valid	:	<0-4294967295> (seconds) The value set for the Valid Lifetime field of the Prefix Information option. The default value is 2592000.
preferred	:	<0-4294967295> (seconds) The value set for the Preferred Lifetime field of the Prefix Information option. This must be set to a value equal to or less than *valid*. The default value is 604800.

[Initial value]

None

[Input mode]

interface mode

[Description]

Sets prefix information advertised by RA.

The prefix information advertised by RA is as shown below.

- When this command is set, only the set prefix is targeted for advertisement.
- When this command is not set, all IPv6 global address prefixes set for the interface are targeted for advertisement.
  - In this case, the default values for *valid*, *preferred*, off-link and no-autoconfig are used.

With this command, the following maximum number can be set for one VLAN interface.

- The number of IPv6 global addresses that can be set for one VLAN interface.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

When both *valid* and *preferred* are equal to the default value, *valid* and *preferred* are not shown when config is shown.

If either *valid* or *preferred* are not equal to the default value, both *valid* and *preferred* are shown in the config.

The DHCPv6-PD remaining time is used for Valid Lifetime and Preferred Lifetime under the following conditions.

- When this command is not set.
- When the IPv6 global address prefixes set for the interface are using the DHCPv6-PD client prefix.
- When the Valid Lifetime and Preferred Lifetime obtained by the DHCPv6-PD are smaller than the Valid Lifetime (2592000) and Preferred Lifetime (604800) for the prefix targeting the above address.

This command cannot be used if the stack function is enabled.

[Example]

This sets the prefix advertised by RA to "2001:db8:1::/64".

```
SWX3220(config-if)#ipv6 nd prefix 2001:db8:1::/64
```

7.9.3 Set maximum RA periodic transmission interval

[Syntax]

ipv6 nd ra-interval *time*
no ipv6 nd ra-interval

[Parameter]

time	:	<4-65535> (seconds)

[Initial value]

ipv6 nd ra-interval 600

[Input mode]

interface mode

[Description]

Sets the maximum value for the RA periodic transmission interval.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

When this command is set and one of the conditions below is met, the command results in an error.

- When the **ipv6 nd minimum-ra-interval** command has been set.
  - When the value specified by this command multiplied by 0.75 is less than the value set in the **ipv6 nd minimum-ra-interval** command.
- When a value except for "0" is set for the **ipv6 nd ra-lifetime** command.
  - When the value specified by this command is greater than the value set for the **ipv6 nd ra-lifetime** command.

This command cannot be used if the stack function is enabled.

[Example]

This sets the maximum value for the RA periodic transmission interval to 1200 seconds.

```
SWX3220(config-if)#ipv6 nd ra-interval 1200
```

7.9.4 Set minimum RA periodic transmission interval

[Syntax]

ipv6 nd minimum-ra-interval *time*
no ipv6 nd minimum-ra-interval

[Parameter]

time	:	<3-49151> (seconds)

[Initial value]

None

[Input mode]

interface mode

[Description]

Sets the minimum value for the RA periodic transmission interval.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

When specifying a value that's 0.75 times greater than the setting in **ipv6 nd ra-interval** command, this command results in an error.

If this command has not been set, the following minimum value is used for the RA periodic transmission interval.

Use the **show ipv6 nd ra** command to confirm the value actually used.

- When the setting in **ipv6 nd ra-interval** command value is 9 seconds or more.
  - The value is 0.33 times that of the **ipv6 nd ra-interval** command.
    - The value is set 3 seconds when it is less than 3 seconds as a result of being multiplied by 0.33.
- When the value of **ipv6 nd ra-interval** is less than 9 seconds.
  - The value is 0.75 times that of the **ipv6 nd ra-interval** command.

This command cannot be used if the stack function is enabled.

[Example]

This sets the minimum value for the RA periodic transmission interval to 300 seconds.

```
SWX3220(config-if)#ipv6 nd minimum-ra-interval 300
```

7.9.5 Set the Cur Hop Limit field for RA

[Syntax]

ipv6 nd current-hoplimit *hoplimit*
no ipv6 nd current-hoplimit

[Parameter]

hoplimit : <0-255>

[Initial value]

ipv6 nd current-hoplimit 64

[Input mode]

interface mode

[Description]

Sets the Cur Hop Limit field for the RA.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command cannot be used if the stack function is enabled.

[Example]

Sets the value of the Cur Hop Limit field for RA to 128.

```
SWX3220(config-if)#ipv6 nd current-hoplimit 128
```

7.9.6 Set the RA M flag

[Syntax]

ipv6 nd managed-config-flag
no ipv6 nd managed-config-flag

[Initial value]

None

[Input mode]

interface mode

[Description]

Sets the RA M flag.

Use this command to set the RA M flag.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command cannot be used if the stack function is enabled.

[Example]

Sets the RA M flag.

```
SWX3220(config-if)#ipv6 nd managed-config-flag
```

7.9.7 Set the RA O flag

[Syntax]

ipv6 nd other-config-flag
no ipv6 nd other-config-flag

[Initial value]

None

[Input mode]

interface mode

[Description]

Sets the RA O flag.

Use this command to set the RA O flag.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command cannot be used if the stack function is enabled.

[Example]

This sets the RA O flag.

```
SWX3220(config-if)#ipv6 nd other-config-flag
```

7.9.8 Set RA Router Lifetime

[Syntax]

ipv6 nd ra-lifetime *time*
no ipv6 nd ra-lifetime

[Parameter]

time	:	<0-65535> (seconds)

[Initial value]

None

[Input mode]

interface mode

[Description]

Sets the Router Lifetime field for RA.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

When both conditions below are met, this command results in an error.

- When this command is set to a value other than "0".
- When a value of less than that specified by the **ipv6 nd ra-interval** command is specified.

If this command has not been set, the following value is used for the RA Router Lifetime.

Use the **show ipv6 nd ra** command to confirm the value actually used.

- The value is 3 times that of the **ipv6 nd ra-interval** command.

- If the value multiplied by 3 exceeds 65535, the value is set to 65535.

This command cannot be used if the stack function is enabled.

[Example]

This sets the Router Lifetime field for RA to 3600.

```
SWX3220(config-if)#ipv6 nd ra-lifetimet 3600
```

7.9.9 Set RA Reachable Time

[Syntax]

ipv6 nd reachable-time *time*
no ipv6 nd reachable-time

[Parameter]

time : <0-3600000> (milliseconds)

[Initial value]

ipv6 nd reachable-time 0

[Input mode]

interface mode

[Description]

Sets the value for the RA Reachable Time field.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command cannot be used if the stack function is enabled.

[Example]

This sets the RA Reachable Time field to 3600.

```
SWX3220(config-if)#ipv6 nd reachable-time 3600
```

7.9.10 Set RA Retrans Timer

[Syntax]

ipv6 nd retransmission-time *time*
no ipv6 nd retransmission-time

[Parameter]

time : <0-4294967295> (milliseconds)

[Initial value]

ipv6 nd retransmission-time 0

[Input mode]

interface mode

[Description]

Sets the RA Retrans Timer field value.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command cannot be used if the stack function is enabled.

[Example]

This sets the RA Retrans Timer field to 3600.

```
SWX3220(config-if)#ipv6 nd retransmission-time 3600
```

7.9.11 Set MTU option for RA

[Syntax]

ipv6 nd link-mtu *mtu*
no ipv6 nd link-mtu

[Parameter]

mtu : <1280-65535>

[Initial value]

None

[Input mode]

interface mode

[Description]

Sets the MTU option value.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

If this command is not set, the MTU option for RA is not added.

This command cannot be used if the stack function is enabled.

[Example]

Sets MTU option value for RA to 1500.

```
SWX3220(config-if)#ipv6 nd link-mtu 1500
```

7.9.12 Show RA information

[Syntax]

show ipv6 nd ra [*ifname*]

[Parameter]

ifname : VLAN interface name

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

Shows the IPv6 router advertisement information.

If *ifname* is not specified, this shows information for all VLAN interface.

[Note]

This command cannot be used if the stack function is enabled.

[Example]

Shows the IPv6 router advertisement-related information for all VLAN interface.

```
SWX3220#show ipv6 nd ra
Interface vlan1 RA information
  RA send enable
    Next RA due in 454 seconds
  Router Lifetime is 1800 seconds
  Reachable Time is 0 milliseconds
  Retrans timer is 0 milliseconds
  Hop limit is 64
  Maximum-ra-interval is 600
  Minimum-ra-interval is 198
  M flag disable
  O flag disable
  Link mtu option disable
  Prefix information setting none

Interface vlan2 RA information
```

```
  RA send disable
  Router Lifetime is 1800 seconds
  Reachable Time is 0 milliseconds
  Retrans timer is 0 milliseconds
  Hop limit is 64
  Maximum-ra-interval is 600
  Minimum-ra-interval is 198
  M flag disable
  O flag disable
  Link mtu option disable
  Prefix information setting none

SWX3220#
```

7.10 IPv6 forwarding control

7.10.1 IPv6 forwarding settings

[Syntax]

ipv6 forwarding *switch*
no ipv6 forwarding [*switch*]

[Parameter]

switch : IPv6 packet forwarding settings

Setting value	Description
enable	Enable forwarding of IPv6 packets
disable	Disable forwarding of IPv6 packets

[Initial value]

ipv6 forwarding enable

[Input mode]

global configuration mode

[Description]

Enables or disables forwarding of IPv6 packets.

If this is executed with the "no" syntax, the setting returns to the default.

7.10.2 Show IPv6 forwarding settings

[Syntax]

show ipv6 forwarding

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the IPv6 packet forwarding settings.

[Example]

Shows the IPv6 packet forwarding settings.

```
SWX3220>show ipv6 forwarding
IPv6 forwarding is on
```

7.11 IPv6 ping

7.11.1 IPv6 ping

[Syntax]

ping6 *host* [repeat *count*] [size *datalen*] [timeout *timeout*] [source *ipv6_address*]

[Keyword]

repeat	:	Specifies the number of times to execute
size	:	Specifies the length of the ICMPv6 payload (byte units)
timeout	:	Specifies the time to wait for a reply after transmitting the specified number of Echo requests
source	:	Sets the source address for ICMPv6 packets

[Parameter]

host : Host name, or target IPv6 address (X:X::X:X)

Target to which ICMPv6 Echo is sent

If you specify an IPv6 link local address, you must also specify the output interface (fe80::X%vlanN format)

count : Number of times to execute (if omitted: 5)

Setting value	Description
<1-2147483647>	Execute the specified number of times
continuous	Execute repeatedly until Ctrl+C is entered

datalen : <36-18024>

Length of ICMP payload (if omitted: 56)

timeout : <1-65535>

Time to wait for a reply (if omitted: 2)

Ignored if count is specified as "continuous"

ipv6_address : X:X::X:X

IPv6 address

[Input mode]

privileged EXEC mode

[Description]

Send ICMPv6 Echo to the specified host, and wait for ICMPv6 Echo Reply.

When it is received, indicate this. Show simple statistical information when the command ends.

[Note]

This command cannot be used if the stack function is enabled.

[Example]

Ping fe80::2a0:deff:fe11:2233.

```
SWX3220#ping6 fe80::2a0:deff:fe11:2233%vlan1
PING fe80::2a0:deff:fe11:2233%vlan1 (fe80::2a0:deff:fe11:2233%vlan1): 56 data bytes
64 bytes from fe80::2a0:deff:fe11:2233: seq=0 ttl=64 time=2.681 ms
64 bytes from fe80::2a0:deff:fe11:2233: seq=1 ttl=64 time=4.760 ms
64 bytes from fe80::2a0:deff:fe11:2233: seq=2 ttl=64 time=10.045 ms
64 bytes from fe80::2a0:deff:fe11:2233: seq=3 ttl=64 time=10.078 ms
64 bytes from fe80::2a0:deff:fe11:2233: seq=4 ttl=64 time=10.210 ms

--- fe80::2a0:deff:fe11:2233%vlan1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 2.681/7.554/10.210 ms
```

7.11.2 Check IPv6 route

[Syntax]

traceroute6 *host*

[Parameter]

host : Destination for which to check the route

Host name, or target IPv6 address (X:X::X:X)

[Input mode]

privileged EXEC mode

[Description]

Shows information for the route to the specified host.

[Note]

This command cannot be used if the stack function is enabled.

[Example]

Check the route to 2001:db8:1::2.

```
SWX3220#traceroute6 2001:db8:1::2
traceroute to 2001:db8:1::2 (2001:db8:1::2), 30 hops max
 1  2001:db8:10::1 (2001:db8:10::1)  0.563 ms  0.412 ms  0.428 ms
 2  2001:db8:20::1 (2001:db8:20::1)  0.561 ms  0.485 ms  0.476 ms
 3  2001:db8:30::1 (2001:db8:30::1)  0.864 ms  0.693 ms  21.104 ms
 4  2001:db8:40::1 (2001:db8:40::1)  0.751 ms  0.783 ms  0.673 ms
 5  2001:db8:50::1 (2001:db8:50::1)  7.689 ms  7.527 ms  7.168 ms
 6  2001:db8:1::2 (2001:db8:1::2)  33.948 ms  10.413 ms  7.681 ms
```

7.12 DNS client

7.12.1 Set DNS lookup function

[Syntax]

dns-client *switch*
no dns-client

[Parameter]

switch : Behavior of the DNS client

Setting value	Description
enable	Enable the DNS client
disable	Disable the DNS client

[Initial value]

dns-client disable

[Input mode]

global configuration mode

[Description]

Enables or disables the DNS lookup function.

If this command is executed with the "no" syntax, the function is disabled.

[Example]

Enable the DNS lookup function.

```
SWX3220(config)#dns-client enable
```

7.12.2 Set DNS server list

[Syntax]

dns-client name-server *server*
no dns-client name-server *server*

[Parameter]

server : A.B.C.D

IPv4 addtess of the DNS server

: X:X::X:X

IPv6 address of the DNS server

If you specify an IPv6 link local address, you must also specify the output interface (fe80::X%vlanN format)

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Adds a server to the DNS server list.

Up to three servers can be specified.

If this command is executed with the "no" syntax, the specified server is deleted from the DNS server list.

[Note]

If the **ip address dhcp**, **ipv6 address dhcp**, **ipv6 dhcp client pd** or **ipv6 address autoconfig stateless** command was used to obtain the DNS server list from the DHCP server, the settings of this command take priority.

However if fewer than three items were registered to the DNS server list by this command, up to a total of three items of the DNS server list obtained from the DHCP server are added to the end of this list.

[Example]

Add the IP addresses 192.168.100.1, 2001:db8::1234, and fe80::2a0:deff:fe11:2233 to the DNS server list.

```
SWX3220(config)#dns-client name-server 192.168.100.1
SWX3220(config)#dns-client name-server 2001:db8::1234
SWX3220(config)#dns-client name-server fe80::2a0:deff:fe11:2233%vlan1
```

7.12.3 Set default domain name

[Syntax]

dns-client domain-name *name*
no dns-client domain-name *name*

[Parameter]

name	:	Domain name (maximum 255 characters)

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Specifies the default domain name used for DNS queries.

If this command is executed with the "no" syntax, the default domain name is deleted.

[Note]

The setting of this command takes priority if the default domain name (option code 15) was obtained from the DHCP server by the **ip address dhcp** command.

If a search domain list is specified by the **dns-client domain-list** command, the default domain name specified by this command and the default domain name automatically specified by the **ip address dhcp** command are not used.

[Example]

Set the default domain name to "example.com".

```
SWX3220(config)#dns-client domain-name example.com
```

7.12.4 Set search domain list

[Syntax]

dns-client domain-list *name*
no dns-client domain-list *name*

[Parameter]

name : Domain name (maximum 255 characters)

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Adds a domain name to the list of domain names used for DNS queries.

Up to six domains can be registered in the search domain list.

If this command is executed with the "no" syntax, the specified domain name is deleted from the search domain list.

[Note]

If a search domain list is specified by this command, the default domain name specified by the **dns-client domain-name** command and the default domain name automatically specified by the **ip address dhcp** command are not used.

If the **ipv6 address dhcp**, **ipv6 dhcp client pd** or **ipv6 address autoconfig stateless** command was used to obtain the query domain list from the DHCP server, the setting for this command takes priority.

However if fewer than six items were registered by this command in the query domain list, up to six items from the query domain list obtained by the DHCP server are added to the end of this list.

[Example]

Add the domain names "example1.com" and "example2.com" to the search domain list.

```
SWX3220(config)#dns-client domain-list example1.com
SWX3220(config)#dns-client domain-list example2.com
```

7.12.5 Show DNS client information

[Syntax]

show dns-client

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the DNS client information.

The following content is shown.

Item	Description
DNS Client is enabled	Enable the DNS client
DNS Client is disabled	Disable the DNS client
Default domain	Default domain name
Domain list	Search domain list
Name Servers	DNS server list (IP address)

[Example]

Show the DNS client information.

```
SWX3220>show dns-client

DNS client is enabled
 Default domain  : example.com
 Domain list     : example1.com example2.com
 Name Servers    : 192.168.100.1 2001:db8::1234 fe80::2a0:deff:fe11:2233%vlan1

 * - Values assigned by DHCP or DHCPv6 Client.
```

7.13 BGP

7.13.1 Set function enable and AS number

[Syntax]

router bgp *AS_NUM*
no router bgp *AS_NUM*

[Parameter]

AS_NUM : <1-4294967295>
AS number

[Initial value]

None

[Input mode]

global configuration mode

[Description]

This specifies an AS number and switches to BGP configuration mode.

[Example]

This specifies an AS number of 20000 and switches to BGP configuration mode.

```
SWX3220#configure terminal
SWX3220(config)#router bgp 20000
SWX3220(config-router)#
```

7.13.2 Switch to BGP IPv6 address family mode

[Syntax]

address-family ipv6

[Initial value]

None

[Input mode]

BGP mode

[Description]

Switches to the BGP IPv6 address family mode.

When returning to BGP mode, the "exit-address-family" command is used.

This cannot be executed if the stack is enabled.

[Example]

This switches from BGP configuration mode to IPv6 address family mode.

```
SWX3220(config-router)#address-family ipv6
SWX3220(config-router-af)#
```

7.13.3 Leave BGP IPv6 address family mode

[Syntax]

exit-address-family

[Initial value]

None

[Input mode]

BGP IPv6 address-family mode

[Description]

This switches to BGP mode from BGP IPv6 address family mode.

[Example]

This switches to BGP mode.

```
SWX3220(config-router-af)#exit-address-family
SWX3220(config-router)#
```

7.13.4 Set router ID

[Syntax]

bgp router-id *ip_address*
no bgp router-id [*ip_address*]

[Parameter]

ip_address : A.B.C.D

IP address

[Initial value]

None

[Input mode]

BGP mode

[Description]

Sets the BGP router ID.

If this command is not used to specify the router ID, the greatest IPv4 address amongst the IP addresses of this device is used as the router ID.

[Example]

This specifies 192.168.100.240 the BGP router ID.

```
SWX3220#configure terminal
SWX3220(config)#router bgp 20000
SWX3220(config-router)#bgp router-id 192.168.100.240
```

7.13.5 Set IPv4 unicast route exchange operations

[Syntax]

bgp default ipv4-unicast *SWITCH*
no bgp default ipv4-unicast [*SWITCH*]

[Parameter]

SWITCH : IPv4 unicast routing exchange operations

Setting value	Description
enable	Permit IPv4 unicast routing information
disable	Deny IPv4 unicast routing information

[Initial value]

bgp default ipv4-unicast enable

[Input mode]

BGP mode

[Description]

Start IPv4 unicast routing exchange right after the BGP peer is established.

When set to "disable", IPv4 unicast routing information exchange will not begin until the "neighbor activate" command is executed.

Regardless of this command’s setting, IPv6 unicast routing does not begin exchanging until the "neighbor activate" command in BGP IPv6 address family mode is executed.

[Example]

This permits IPv4 unicast routing information.

```
SWX3220(config-router)#bgp default ipv4-unicast enable
```

This denies IPv4 unicast routing information.

```
SWX3220(config-router)#bgp default ipv4-unicast disable
```

7.13.6 Setting for session reset behavior when an interface goes down

[Syntax]

bgp fast-external-failover *SWITCH*
no bgp fast-external-failover *SWITCH*

[Parameter]

SWITCH : Session reset behavior

Setting value	Description
enable	Enables session reset when a VLAN interface goes down
disable	Disables session reset when a VLAN interface goes down

[Initial value]

bgp fast-external-failover enable

[Input mode]

BGP mode

[Description]

The session is immediately reset when a VLAN interface used for communicating with an eBGP peer goes down.

When "disable" is set, the session is maintained until the Hold Time is elapsed.

During communications with an eBGP peer, the session is always maintained until the Hold Time is elapsed, when the VLAN interface that is being used goes down.

[Example]

This enables session reset when a VLAN interface goes down.

```
SWX3220(config-router)#bgp fast-external-failover enable
```

This disables session reset when a VLAN interface goes down.

```
SWX3220(config-router)#bgp fast-external-failover disable
```

7.13.7 Setting for output of logs related to state changes

[Syntax]

bgp log-neighbor-changes *SWITCH*
no bgp log-neighbor-changes [*SWITCH*]

[Parameter]

SWITCH : Display of detailed information related to the BGP

Setting value	Description
enable	Show detailed information related to the BGP
disable	Hide detailed information related to the BGP

[Initial value]

bgp log-neighbor-changes disable

[Input mode]

BGP mode

[Description]

Output a log of detailed information related to the BGP.

[Example]

This enables showing detailed information related to the BGP.

```
SWX3220(config-router)#bgp log-neighbor-changes enable
```

This disables showing detailed information related to the BGP.

```
SWX3220(config-router)#bgp log-neighbor-changes disable
```

7.13.8 Check interval setting for routes registered in the BGP routing table

[Syntax]

bgp scan-time *TIME*
no bgp scan-time [*TIME*]

[Parameter]

TIME	:	<0-60> seconds

[Initial value]

bgp scan-time 60

[Input mode]

BGP mode

[Description]

Sets the check interval time for routes registered in the BGP routing table.

Periodic checks are not performed if "0" is specified.

[Example]

This sets the check interval time for the route.

```
SWX3220(config-router)#bgp scan-time 60
```

7.13.9 Set administrative distance (BGP IPv4)

[Syntax]

distance *AD IP_SRC* [*ACL_NUM*]
no distance *AD IP_SRC* [*ACL_NUM*]
distance bgp *EBGP IBGP LOCAL*
no distance bgp [*EBGP IBGP LOCAL*]

[Parameter]

AD	:	<1-255> Administrative distance
IP_SRC	:	<A.B.C.D/M>
ACL_NUM	:	<1-2000> Access list number
EBGP	:	<1-255> Administrative distance of eBGP route
IBGP	:	<1-255> Administrative distance of iBGP route
LOCAL	:	<1-255> Administrative distance of local route that is acquired via the "network" command

[Initial value]

distance bgp 20 200 200

[Input mode]

BGP mode

[Description]

This sets the administrative distance of the IPv4 BGP.

Administrative distance settings can be applied only to routes advertised from BGP peers included in the segment specified by IP_SRC.

Further, if ACL_NUM is specified, the administrative distance settings can only be applied to routes among those advertised from a BGP peer that match the access list.

[Example]

This sets the administrative distance of the eBGP route to 69, and the administrative distance of iBGP routes and the local routes that are acquired via the "network" command to 100.

```
SWX3220(config-router)#distance bgp 69 100 100
```

7.13.10 Set administrative distance (BGP IPv6)

[Syntax]

distance bgp *EBGP IBGP LOCAL*
no distance bgp [*EBGP IBGP LOCAL*]

[Parameter]

EBGP : <1-255>

Administrative distance of eBGP route

IBGP : <1-255>

Administrative distance of iBGP route

LOCAL : <1-255>

Administrative distance of local route that is acquired via the "network" command

[Initial value]

distance bgp 20 200 200

[Input mode]

BGP IPv6 address-family mode

[Description]

This sets the administrative distance of the IPv6 BGP.

This cannot be executed if the stack is enabled.

[Example]

This sets the administrative distance of the eBGP route to 69, and the administrative distance of iBGP routes and the local routes that are acquired via the "network" command to 100.

```
SWX3220(config-router-af)#distance bgp 69 100 100
```

7.13.11 Set the AS_PATH access list

[Syntax]

ip as-path access-list *AS_ACL_NUM RULE REGEXP*
no ip as-path access-list *AS_ACL_NUM* [*RULE REGEXP*]

[Parameter]

AS_ACL_NUM : <1-100>

AS path access list number

RULE : Filtering operations

Setting value	Description
permit	Permits access to the list number equal to the setting value
deny	Denies access to the list number equal to the setting value

REGEXP : Regular expression for AS path

[Initial value]

None

[Input mode]

global configuration mode

[Description]

Sets the AS path access list used for filtering the AS_PATH attribute in the route information that is received from the BGP peer or advertised to the BGP peer.

The community list defined by this command can be referenced using the "neighbor filter-list" command.

7.13.12 Set community list

[Syntax]

ip community-list *LIST_NUM_STANDARD RULE COMMUNITY* [*COMMUNITY*...]
ip community-list *LIST_NUM_EXPAND RULE REGEXP*
no ip community-list *LIST_NUM_STANDARD* [*RULE* [*COMMUNITY* [*COMMUNITY*...]]]
no ip community-list *LIST_NUM_EXPAND* [*RULE* [*REGEXP*]]

[Parameter]

LIST_NUM_STANDARD : <1-99>

Standard community list number

LIST_NUM_EXPAND : <100-500>

Extended community list number

RULE : Community list rules

Setting value	Description
permit	Permit the specified community list
deny	Deny community lists used by a BGP

COMMUNITY : Community value

AA:NN : community value

Setting value	Description
AA	<1-65535> AS number
NN	<1-65535> Access list number for community values within the AS specified by AA

internet : Community value (0:0)

no-advertise : Well-known community value NO_ADVERTISE(65535-65282)

no-export : Well-known community value NO_EXPORT(65535-65281)

local-as : Well-known community value NO_EXPORT_SUBCONFED(65535-65283)

REGEXP : Regular expression for COMMUNITIES attributes

[Input mode]

global configuration mode

[Description]

This defines the community list used by a BGP.

The community list defined by this command can be referenced using the "match community" and "set comm-list delete" commands.

[Example]

Defines a community list with standard community list number 1, community list rule "permit", and community value "internet".

```
SWX3220(config)#ip community-list 1 permit internet
```

7.13.13 Set IPv4 prefix list

[Syntax]

ip prefix-list *PLIST_NUM* [*seq SEQ*] *RULE PREFIX* [*ge MASK*] [*le MASK*]
ip prefix-list *PLIST_NUM description DESCRIPTION*
no ip prefix-list *PLIST_NUM* [*seq SEQ*] *RULE PREFIX* [*ge MASK*] [*le MASK*]
no ip prefix-list *PLIST_NUM description DESCRIPTION*

[Parameter]

PLIST_NUM : <1-100>

Prefix list number

SEQ : <1-256>

Sequence number

RULE : Community list rules

Setting value	Description
permit	Permit the specified community list
deny	Deny the specified community list

PREFIX : <A.B.C.D/M>

IP prefix

MASK : <0-32>

Subnet mask

DESCRIPTION : Description of prefix list (up to 80 single-byte alphanumeric characters)

[Input mode]

global configuration mode

[Description]

This defines the community list used by a BGP.

The community list defined by this command can be referenced using the "neighbor prefix-list" and "clear ip prefix-list" commands.

When "seq" is omitted, the maximum sequence number for the existing prefix list + 1 is automatically assigned.

If an entry exists where "seq" is 256, you must explicitly specify an unused sequence number, as inputting without "seq" will cause an error.

If both ge and le are specified as MASK, a match occurs only if the M in PREFIX is greater than or equal to "ge" and less than or equal to "le".

If only "ge" is specified as MASK, "le" operates with the value of 32. ("ge–32" becomes the matching condition)

If only "le" is specified as MASK, "ge" operates with the value of PREFIX M. ("M–le" becomes the matching condition)

[Example]

This defines prefix list number 1, community list rule "permit", and a list with a subnet mask of 0.

```
SWX3220(config)#ip prefix-list 1 permit 192.168.100.240/24 ge 0
```

7.13.14 Set IPv6 prefix list

[Syntax]

ipv6 prefix-list *PLIST_NUM* [*seq SEQ*] *RULE PREFIX* [*ge MASK*] [*le MASK*]
ipv6 prefix-list *PLIST_NUM description DESCRIPTION*
no ipv6 prefix-list *PLIST_NUM* [*seq SEQ*] *RULE PREFIX* [*ge MASK*] [*le MASK*]
no ipv6 prefix-list *PLIST_NUM description DESCRIPTION*

[Parameter]

PLIST_NUM : <1-100>

Prefix list number

SEQ : <1-256>

Sequence number

RULE : Community list rules

Setting value	Description
permit	Permit the specified community list
deny	Deny the specified community list

PREFIX : <X:X::X:X/M>

IPv6 prefix

MASK : <0-128>

Subnet mask

DESCRIPTION : Description of prefix list (up to 80 single-byte alphanumeric characters)

[Input mode]

global configuration mode

[Description]

This defines the community list used by a BGP.

The community list defined by this command can be referenced using the "neighbor prefix-list" and "clear ipv6 prefix-list" commands.

When "seq" is omitted, the maximum sequence number for the existing prefix list + 1 is automatically assigned.

If an entry exists where "seq" is 256, you must explicitly specify an unused sequence number, as inputting without "seq" will cause an error.

If both ge and le are specified as MASK, a match occurs only if the M in PREFIX is greater than or equal to "ge" and less than or equal to "le".

If only "ge" is specified as MASK, "le" operates with the value of 128. ("ge–128" becomes the matching condition)

If only "le" is specified as MASK, "ge" operates with the value of PREFIX M. ("M–le" becomes the matching condition)

[Example]

Assigns a community list with standard community list and sequence numbers of 1, community list rule "permit", and the IPv6 address for PREFIX.

```
SWX3220(config)#ip community-list 1 permit 1::1/64
```

7.13.15 Keepalive-related timer settings

[Syntax]

timers bgp *KEEPALIVE HOLDTIME*
no timers bgp [*KEEPALIVE HOLDTIME*]

[Parameter]

KEEPALIVE : <0-65535>

Transmission time (seconds) for keepalive messages

HOLDTIME : 0 or <3-65535>

HoldTime time (seconds)

[Initial value]

timers bgp 30 90

[Input mode]

BGP mode

[Description]

Sets the time for the keepalive-related timer.

HoldTime is the time from when the keepalive message was last received from the BGP peer to the time when the session is considered down.

KEEPALIVE must be set to a time equal to or greater than HOLDTIME.

The setting value for this command is notified to the BGP peer via the OPEN message, and in actuality operates with the value set by negotiation.

[Example]

This sets the keepalive message transmission time to 100 seconds, and the HoldTime time to 300 seconds.

```
SWX3220(config-router)#timers bgp 100 300
```

7.13.16 Enable route exchange with BGP peers (BGP IPv4)

[Syntax]

neighbor *PEER* **activate**
no neighbor *PEER* **activate**

[Parameter]

PEER : Peer setting value

Setting value	Description
<A.B.C.D>	IPv4 address of the BGP peer
<X:X::X:X>	IPv6 address of the BGP peer
BGP peer group name	Up to 64 half-width alphanumeric characters

[Initial value]

None

[Input mode]

BGP mode

[Description]

This starts IPv4 route exchange with a BGP peer or BGP peer group.

When "bgp default ipv4 unicast disable" is set, IPv4 route exchange does not start until this command is executed.

When "bgp default ipv4 unicast disable" is not set, IPv4 route exchange starts regardless of the settings for this command.

[Example]

This enables route exchange with a BGP peer having the IP address of 192.168.100.240.

```
SWX3220(config-router)#neighbor 192.168.100.240 activate
```

7.13.17 Enable route exchange with BGP peers (BGP IPv6)

[Syntax]

neighbor *PEER* **activate**
no neighbor *PEER* **activate**

[Parameter]

PEER : Peer setting value

Setting value	Description
<X:X::X:X>	IPv6 address of the BGP peer
BGP peer group name	Up to 64 half-width alphanumeric characters

[Initial value]

None

[Input mode]

BGP IPv6 address-family mode

[Description]

This starts IPv6 route exchange with a BGP peer or BGP peer group.

For IPv6 BGP, routes are not exchanged directly after the session has been established. Instead, IPv6 route exchange starts when this command is set.

This cannot be executed if the stack is enabled.

[Example]

This enables route exchange with a BGP peer having the IPv6 address of 1000::1.

```
SWX3220(config-router-af)#neighbor 1000::1 activate
```

7.13.18 Set minimum transmission interval for UPDATE messages

[Syntax]

neighbor *PEER* **advertisement-interval** *INTERVAL*
no neighbor *PEER* **advertisement-interval** [*INTERVAL*]

[Parameter]

PEER : Peer setting value

Setting value	Description
<A.B.C.D>	IPv4 address of the BGP peer
<X:X::X:X>	IPv6 address of the BGP peer
BGP peer group name	Up to 64 half-width alphanumeric characters

INTERVAL : <0-65535>

Minimum transmission interval (sec.) for UPDATE messages

[Initial value]

neighbor advertisement-interval 30 for eBGP peers

neighbor advertisement-interval 5 for iBGP peers

[Input mode]

BGP mode

[Description]

This sets the minimum transmission interval for UPDATE messages.

[Example]

This sets the minimum transmission interval for UPDATE messages to a BGP peer with an IPv4 address of 192.168.100.240 to 10 seconds.

```
SWX3220(config-router)#neighbor 192.168.100.240 advertisement-interval 10
```

7.13.19 Setting for accepting routes even when the AS_PATH attribute of the received route contains the local AS number (BGP IPv4)

[Syntax]

neighbor *PEER* **allowas-in** [*AS_MAX_NUM*]
no neighbor *PEER* **allowas-in** [*AS_MAX_NUM*]

[Parameter]

PEER : Peer setting value

Setting value	Description
<A.B.C.D>	IPv4 address of the BGP peer
<X:X::X:X>	IPv6 address of the BGP peer
BGP peer group name	Up to 64 half-width alphanumeric characters

AS_MAX_NUM : <1-10>

Number of local AS numbers

[Initial value]

None

[Input mode]

BGP mode

[Description]

When the local AS numbers included in the AS_PATH attribute of the route received from a BGP peer is less than the number specified using this command, that route is loaded into the BGP routing table.

If AS_MAX_NUM is omitted, a value of 3 is used.

[Example]

This sets the IP address to 192.168.100.240 and the AS_MAX_NUM value to 1.

```
SWX3220(config-router)#neighbor 192.168.100.240 allowas-in 1
```

7.13.20 Setting for accepting routes even when the AS_PATH attribute of the received route contains the local AS number (BGP IPv6)

[Syntax]

neighbor *PEER* **allowas-in** [*AS_MAX_NUM*]
no neighbor *PEER* **allowas-in** [*AS_MAX_NUM*]

[Parameter]

PEER : Peer setting value

Setting value	Description
<X:X::X:X>	IPv6 address of the BGP peer
BGP peer group name	Up to 64 half-width alphanumeric characters

AS_MAX_NUM : <1-10>

Number of local AS numbers

[Initial value]

None

[Input mode]

BGP IPv6 address-family mode

[Description]

When the local AS numbers included in the AS_PATH attribute of the route received from a BGP peer is less than the number specified using this command, that route is loaded into the BGP routing table.

If AS_MAX_NUM is omitted, a value of 3 is used.

This cannot be executed if the stack is enabled.

7.13.21 Set minimum transmission interval for UPDATE messages, including local AS

[Syntax]

neighbor *PEER* **as-origination-interval** *INTERVAL*
no neighbor *PEER* **as-origination-interval** [*INTERVAL*]

[Parameter]

PEER : Peer setting value

Setting value	Description
<A.B.C.D>	IPv4 address of the BGP peer
<X:X::X:X>	IPv6 address of the BGP peer
BGP peer group name	Up to 64 half-width alphanumeric characters

INTERVAL : <1-65535>

Minimum transmission interval (sec.) for UPDATE messages

[Initial value]

no neighbor as-origination-interval

[Input mode]

BGP mode

[Description]

This sets the minimum transmission interval for UPDATE messages, including those originating from the local AS.

If this command has not been set, the "neighbor advertisement-interval" command value is used for the minimum transmission interval for UPDATE messages originating from the local AS.

7.13.22 Advertise routes without rewriting attributes (BGP IPv4)

[Syntax]

neighbor *PEER* **attribute-unchanged** [*ATTR* [*ATTR* [*ATTR*]]]
no neighbor *PEER* **attribute-unchanged** [*ATTR* [*ATTR* [*ATTR*]]]

[Parameter]

PEER : Peer setting value

Setting value	Description
<A.B.C.D>	IPv4 address of the BGP peer
<X:X::X:X>	IPv6 address of the BGP peer
BGP peer group name	Up to 64 half-width alphanumeric characters

ATTR : Attributes

Setting value	Description
as-path	AS_PATH attribute
med	MED attribute
next-hop	NEXT_HOP attribute

[Initial value]

None

[Input mode]

BGP mode

[Description]

This advertises routes to a BGP peer without rewriting the specified attributes.

This can only be set for eBGP peers, for which the "neighbor ebgp-multihop" command has been set to 2 or more.

If ATTR is omitted, this operates as if all (as-path, med, next-hop) are selected.

7.13.23 Advertise routes without rewriting attributes (BGP IPv6)

[Syntax]

neighbor *PEER* **attribute-unchanged** [*ATTR* [*ATTR* [*ATTR*]]]
no neighbor *PEER* **attribute-unchanged** [*ATTR* [*ATTR* [*ATTR*]]]

[Parameter]

PEER : Peer setting value

Setting value	Description
<A.B.C.D>	IPv4 address of the BGP peer
<X:X::X:X>	IPv6 address of the BGP peer
BGP peer group name	Up to 64 half-width alphanumeric characters

ATTR : Attributes

Setting value	Description
as-path	AS_PATH attribute
med	MED attribute
next-hop	NEXT_HOP attribute

[Initial value]

None

[Input mode]

BGP IPv6 address-family mode

[Description]

This advertises routes to a BGP peer without rewriting the specified attributes.

This can only be set for eBGP peers, for which the "neighbor ebgp-multihop" command has been set to 2 or more.

If ATTR is omitted, this operates as if all (as-path, med, next-hop) are selected.

This cannot be executed if the stack is enabled.

7.13.24 Advertise outbound route filtering capability (BGP IPv4)

[Syntax]

neighbor *PEER* **capability orf prefix-list** *DIRECTION*
no neighbor *PEER* **capability orf prefix-list** [*DIRECTION*]

[Parameter]

PEER : Peer setting value

Setting value	Description
<A.B.C.D>	IPv4 address of the BGP peer
<X:X::X:X>	IPv6 address of the BGP peer
BGP peer group name	Up to 64 half-width alphanumeric characters

DIRECTION : Target route

Setting value	Description
both	Route to transmit/receive is the target
medreceive	Route to receive is the target
send	Route to transmit is the target

[Initial value]

None

[Input mode]

BGP mode

[Description]

This advertises the outbound route filtering capability to a BGP peer.

Outbound Route Filtering (ORF) capability is a function that lets peers determine whether they support transmission/reception of inbound prefix lists when the session is established via the OPEN message.

By using this function, you can advertise only the necessary route information on the outbound side of the route information.

7.13.25 Advertise outbound route filtering capability (BGP IPv6)

[Syntax]

neighbor *PEER* **capability orf prefix-list** *DIRECTION*
no neighbor *PEER* **capability orf prefix-list** [*DIRECTION*]

[Parameter]

PEER : Peer setting value

Setting value	Description
<A.B.C.D>	IPv4 address of the BGP peer
<X:X::X:X>	IPv6 address of the BGP peer
BGP peer group name	Up to 64 half-width alphanumeric characters

DIRECTION : Target route

Setting value	Description
both	Route to transmit/receive is the target
medreceive	Route to receive is the target
send	Route to transmit is the target

[Initial value]

None

[Input mode]

BGP IPv6 address-family mode

[Description]

This advertises the outbound route filtering capability to a BGP peer.

Outbound Route Filtering (ORF) capability is a function that lets peers determine whether they support transmission/reception of inbound prefix lists when the session is established via the OPEN message.

By using this function, you can advertise only the necessary route information on the outbound side of the route information.

This cannot be executed if the stack is enabled.

7.13.26 Enable route refresh capability

[Syntax]

neighbor *PEER* **capability route-refresh** *SWITCH*
no neighbor *PEER* **capability route-refresh** [*SWITCH*]

[Parameter]

PEER : Peer setting value

Setting value	Description
<A.B.C.D>	IPv4 address of the BGP peer
<X:X::X:X>	IPv6 address of the BGP peer
BGP peer group name	Up to 64 half-width alphanumeric characters

SWITCH : Route refresh capability operations

Setting value	Description
enable	Enables route refresh capability
disable	Disables route refresh capability

[Initial value]

neighbor PEER capability route-refresh enable

[Input mode]

BGP mode

[Description]

Advertises route refresh capability to a BGP peer.

Route refresh capability is a function that lets peers determine whether they can retransmit route information or not, when the session is established via the OPEN message.

7.13.27 Advertise default route to BGP peers (BGP IPv4)

[Syntax]

neighbor *PEER* **default-originate** *SWITCH*
no neighbor *PEER* **default-originate** [*SWITCH*]

[Parameter]

PEER : Peer setting value

Setting value	Description
<A.B.C.D>	IPv4 address of the BGP peer
<X:X::X:X>	IPv6 address of the BGP peer
BGP peer group name	Up to 64 half-width alphanumeric characters

SWITCH : Default route operations

Setting value	Description
enable	Enables the default route advertisement
disable	Disables the default route advertisement

[Initial value]

neighbor PEER default-originate disable

[Input mode]

BGP mode

[Description]

This advertises the default route (0.0.0.0/0) to a BGP peer.

7.13.28 Advertise default route to BGP peers (BGP IPv6)

[Syntax]

neighbor *PEER* **default-originate** *SWITCH*
no neighbor *PEER* **default-originate** [*SWITCH*]

[Parameter]

PEER : Peer setting value

Setting value	Description
<A.B.C.D>	IPv4 address of the BGP peer
<X:X::X:X>	IPv6 address of the BGP peer
BGP peer group name	Up to 64 half-width alphanumeric characters

SWITCH : Default route operations

Setting value	Description
enable	Enables the default route advertisement
disable	Disables the default route advertisement

[Initial value]

neighbor PEER default-originate disable

[Input mode]

BGP IPv6 address-family mode

[Description]

This advertises the default route (0.0.0.0/0) to a BGP peer.

This cannot be executed if the stack is enabled.

7.13.29 BGP peer description

[Syntax]

neighbor *PEER* **description** [*LINE*]
no neighbor *PEER* **description** [*LINE*]

[Parameter]

PEER : Peer setting value

Setting value	Description
<A.B.C.D>	IPv4 address of the BGP peer
<X:X::X:X>	IPv6 address of the BGP peer
BGP peer group name	Up to 64 half-width alphanumeric characters

LINE : Description of BGP peer (up to 80 single-byte alphanumeric characters)

[Initial value]

None

[Input mode]

BGP mode

[Description]

Contains the BGP peer description.

7.13.30 Permit/deny peers advertising Hold Time of 0

[Syntax]

neighbor *PEER* **disallow-infinite-holdtime** *SWITCH*
no neighbor *PEER* **disallow-infinite-holdtime** [*SWITCH*]

[Parameter]

PEER : BGP peer setting

Setting value	Description
<A.B.C.D>	IPv4 address of the BGP peer
<X:X::X:X>	IPv6 address of the BGP peer
BGP peer group name	Up to 64 half-width alphanumeric characters

SWITCH : BGP peer operations

Setting value	Description
enable	Permit the BGP peer advertising Hold Time of 0
disable	Deny the BGP peer advertising Hold Time of 0

[Initial value]

neighbor disallow-infinite-holdtime disable

[Input mode]

BGP mode

[Description]

When a specified BGP peer advertises a Hold Time of 0, this sets whether to permit or deny the peer.

7.13.31 Restricting routes when transmitting/receiving an UPDATE message (BGP IPv4)

[Syntax]

neighbor *PEER* **distribute-list** *ACL_NUM DIRECTION*
no neighbor *PEER* **distribute-list** *ACL_NUM DIRECTION*

[Parameter]

PEER : Peer setting value

Setting value	Description
<A.B.C.D>	IPv4 address of the BGP peer
<X:X::X:X>	IPv6 address of the BGP peer
BGP peer group name	Up to 64 half-width alphanumeric characters

ACL_NUM : <1-2000>

IPv4 access list number

DIRECTION : Direction

Setting value	Description
in	Receiving
out	Transmitting

[Initial value]

None

[Input mode]

BGP mode

[Description]

When transmitting/receiving an UPDATE message, this filters routes that match the "dst-info" parameter of the IPv4 access list.

7.13.32 Restricting routes when transmitting/receiving an UPDATE message (BGP IPv6)

[Syntax]

neighbor *PEER* **distribute-list** *ACL_NUM DIRECTION*
no neighbor *PEER* **distribute-list** *ACL_NUM DIRECTION*

[Parameter]

PEER : Peer setting value

Setting value	Description
<A.B.C.D>	IPv4 address of the BGP peer
<X:X::X:X>	IPv6 address of the BGP peer
BGP peer group name	Up to 64 half-width alphanumeric characters

ACL_NUM : <3001-4000>

IPv6 access list number

DIRECTION : Direction

Setting value	Description
in	Receiving
out	Transmitting

[Initial value]

None

[Input mode]

BGP IPv6 address-family mode

[Description]

When transmitting/receiving an UPDATE message, this filters routes that match the "src-info" parameter of the IPv6 access list.

This cannot be executed if the stack is enabled.

7.13.33 Enable/disable capability advertisement

[Syntax]

neighbor *PEER* **capability-negotiate** *SWITCH*
no neighbor *PEER* **capability-negotiate** [*SWITCH*]

[Parameter]

PEER : Peer setting value

Setting value	Description
<A.B.C.D>	IPv4 address of the BGP peer
<X:X::X:X>	IPv6 address of the BGP peer
BGP peer group name	Up to 64 half-width alphanumeric characters

SWITCH : Capability advertisment operations

Setting value	Description
enable	Enables capability advertisment
disable	Disables capability advertisment

[Initial value]

neighbor PEER capability-negotiate enable

[Input mode]

BGP mode

[Description]

This sets whether to enable or disable capability advertisment.

When set to "disabled", capabilities are not advertised.

7.13.34 Establish BGP peer even if network is not the same

[Syntax]

neighbor *PEER* **ebgp-multihop** [*HOP_NUM*]
no neighbor *PEER* **ebgp-multihop** [*HOP_NUM*]

[Parameter]

PEER : Peer setting value

Setting value	Description
<A.B.C.D>	IPv4 address of the BGP peer
<X:X::X:X>	IPv6 address of the BGP peer
BGP peer group name	Up to 64 half-width alphanumeric characters

HOP_NUM : <2-255>

Number of hops

[Initial value]

None

[Input mode]

BGP mode

[Description]

Even if the eBGP peer is not on the same network, this allows sessions to be established as long as they are within the hop count specified by HOP_NUM.

If HOP_NUM is omitted, a default value of 255 is assumed.

7.13.35 Set filter to restrict AS_PATH attributes advertised to BGP peers (BGP IPv4)

[Syntax]

neighbor *PEER* **filter-list** *AS_ACL_NUM DIRECTION*
no neighbor *PEER* **filter-list** *AS_ACL_NUM DIRECTION*

[Parameter]

PEER : Peer setting value

Setting value	Description
<A.B.C.D>	IPv4 address of the BGP peer
<X:X::X:X>	IPv6 address of the BGP peer
BGP peer group name	Up to 64 half-width alphanumeric characters

AS_ACL_NUM : <1-100>

AS path access list number

DIRECTION : Direction

Setting value	Description
in	Receiving
out	Transmitting

[Initial value]

None

[Input mode]

BGP mode

[Description]

This filters out routes that have AS_PATH attributes matching the AS path access list when transmitting/receiving an UPDATE message.

AS_ACL_NUM specifies the AS path access list number for the "ip as-path access-list" command.

7.13.36 Set filter to restrict AS_PATH attributes advertised to BGP peers (BGP IPv6)

[Syntax]

neighbor *PEER* **filter-list** *AS_ACL_NUM DIRECTION*
no neighbor *PEER* **filter-list** *AS_ACL_NUM DIRECTION*

[Parameter]

PEER : Peer setting value

Setting value	Description
<A.B.C.D>	IPv4 address of the BGP peer
<X:X::X:X>	IPv6 address of the BGP peer
BGP peer group name	Up to 64 half-width alphanumeric characters

AS_ACL_NUM : <1-100>

AS access list number

DIRECTION : Direction

Setting value	Description
in	Receiving
out	Transmitting

[Initial value]

None

[Input mode]

BGP IPv6 address-family mode

[Description]

This filters out routes that have AS_PATH attributes matching the AS access list when transmitting/receiving an UPDATE message.

This cannot be executed if the stack is enabled.

7.13.37 Set interface for communicating with a BGP peer

[Syntax]

neighbor *PEER* **interface** *VLAN_IF*
no neighbor *PEER* **interface** *VLAN_IF*

[Parameter]

PEER : <X:X::X:X>

IPv6 address of the BGP peer

VLAN_IF : VLAN interface

[Initial value]

None

[Input mode]

BGP mode

[Description]

When specifying a BGP peer using an IPv6 link local address, this specifies the VLAN interface to which the BGP peer is connected.

7.13.38 Set number of routes that can be received from a BGP peer (BGP IPv4)

[Syntax]

neighbor *PEER* **maximum-prefix** *PREFIX_NUM* [*THRESHOLD*] [*warning-only*]
no neighbor *PEER* **maximum-prefix** [*PREFIX_NUM* [*THRESHOLD*] [*warning-only*]]

[Parameter]

PEER : Peer setting value

Setting value	Description
<A.B.C.D>	IPv4 address of the BGP peer
<X:X::X:X>	IPv6 address of the BGP peer
BGP peer group name	Up to 64 half-width alphanumeric characters

PREFIX_NUM : <1-4294967295>

Number of prefixes

THRESHOLD : <1-100>

Warning threshold (%)

[Initial value]

None

[Input mode]

BGP mode

[Description]

This disconnects the session with the BGP peer when the number of routes (prefixes) received from the BGP peer exceeds PREFIX_NUM.

If the number of routes received from the BGP peer exceeds the THRESHOLD specified as a percentage of PREFIX_NUM, a warning is logged.

If THRESHOLD is omitted, the system defaults to 75.

When "warning-only" is specified, this does not disconnect the session even if the number of routes (prefixes) received from the BGP peer exceeds PREFIX_NUM. In this case, a warning is logged.

The session is not reestablished for BGP peers whose sessions have been disconnected, until a reset is performed with the "clear ip bgp" command.

7.13.39 Set number of routes that can be received from a BGP peer (BGP IPv6)

[Syntax]

neighbor *PEER* **maximum-prefix** *PREFIX_NUM* [*THRESHOLD*] [*warning-only*]
no neighbor *PEER* **maximum-prefix** [*PREFIX_NUM* [*warning-only*]]

[Parameter]

PEER : Peer setting value

Setting value	Description
<A.B.C.D>	IPv4 address of the BGP peer
<X:X::X:X>	IPv6 address of the BGP peer
BGP peer group name	Up to 64 half-width alphanumeric characters

PREFIX_NUM : <1-4294967295>

Number of prefixes

THRESHOLD : <1-100>

Warning threshold (%)

[Initial value]

None

[Input mode]

BGP IPv6 address-family mode

[Description]

This disconnects the session with the BGP peer when the number of routes (prefixes) received from the BGP peer exceeds PREFIX_NUM.

If the number of routes received from the BGP peer exceeds the THRESHOLD specified as a percentage of PREFIX_NUM, a warning is logged.

If THRESHOLD is omitted, the system defaults to 75.

When "warning-only" is specified, this does not disconnect the session even if the number of routes (prefixes) received from the BGP peer exceeds PREFIX_NUM. In this case, a warning is logged.

The session is not reestablished for BGP peers whose sessions have been disconnected, until a reset is performed with the "clear ip bgp" command.

This cannot be executed if the stack is enabled.

7.13.40 Set whether to forcibly rewrite the NEXT_HOP attribute to this device's IP (BGP IPv4)

[Syntax]

neighbor *PEER* **next-hop-self** *SWITCH*
no neighbor *PEER* **next-hop-self** [*SWITCH*]

[Parameter]

PEER : Peer setting value

Setting value	Description
<A.B.C.D>	IPv4 address of the BGP peer
<X:X::X:X>	IPv6 address of the BGP peer
BGP peer group name	Up to 64 half-width alphanumeric characters

SWITCH : Operations when advertising routes to BGP peers

Setting value	Description
enable	Forcibly rewrites the NEXT_HOP attribute to the IP address of this device when the route is advertised
disable	Does not forcibly rewrite the NEXT_HOP attribute to the IP address of this device when the route is advertised

[Initial value]

neighbor next-hop-self disable

[Input mode]

BGP mode

[Description]

This forcibly rewrites the NEXT_HOP attribute to the IP address of this device when the route is advertised to the BGP peer.

7.13.41 Set whether to forcibly rewrite the NEXT_HOP attribute to this device's IP (BGP IPv6)

[Syntax]

neighbor *PEER* **next-hop-self** *SWITCH*

no neighbor *PEER* **next-hop-self** [*SWITCH*]

[Parameter]

PEER : Peer setting value

Setting value	Description
<A.B.C.D>	IPv4 address of the BGP peer
<X:X::X:X>	IPv6 address of the BGP peer
BGP peer group name	Up to 64 half-width alphanumeric characters

SWITCH : Operations when advertising routes to BGP peers

Setting value	Description
enable	Forcibly rewrites the NEXT_HOP attribute to the IP address of this device when the route is advertised
disable	Does not forcibly rewrite the NEXT_HOP attribute to the IP address of this device when the route is advertised

[Initial value]

neighbor next-hop-self disable

[Input mode]

BGP IPv6 address-family mode

[Description]

This forcibly rewrites the NEXT_HOP attribute to the IP address of this device when the route is advertised to the BGP peer.

This cannot be executed if the stack is enabled.

7.13.42 Set whether to follow advertised capability of BGP peer

[Syntax]

neighbor *PEER* **override-capability** *SWITCH*
no neighbor *PEER* **override-capability** [*SWITCH*]

[Parameter]

PEER : Peer setting value

Setting value	Description
<A.B.C.D>	IPv4 address of the BGP peer
<X:X::X:X>	IPv6 address of the BGP peer
BGP peer group name	Up to 64 half-width alphanumeric characters

SWITCH : Capability setting operations

Setting value	Description
enable	Follows the capability settings of this device
disable	Follows the capability determined via negotiation with the BGP peer

[Initial value]

neighbor override-capability disable

[Input mode]

BGP mode

[Description]

This ignores the capability determined via negotiation with the BGP peer, and follows the capability of this device.

7.13.43 Do not autonomously start sessions with BGP peers

[Syntax]

neighbor *PEER* **passive**
no neighbor *PEER* **passive**

[Parameter]

PEER : Peer setting value

Setting value	Description
<A.B.C.D>	IPv4 address of the BGP peer
<X:X::X:X>	IPv6 address of the BGP peer
BGP peer group name	Up to 64 half-width alphanumeric characters

[Initial value]

None

[Input mode]

BGP mode

[Description]

This sets the device so that it does not start sessions with BGP peers.

The device does respond to session requests from BGP peers.

7.13.44 Enable MD5 authentication between BGP peers

[Syntax]

neighbor *PEER* **password** *PASSWORD*
no neighbor *PEER* **password** [*PASSWORD*]

[Parameter]

PEER : Peer setting value

Setting value	Description
<A.B.C.D>	IPv4 address of the BGP peer
<X:X::X:X>	IPv6 address of the BGP peer
BGP peer group name	Up to 64 half-width alphanumeric characters

PASSWORD : Password (up to 64 half-width alphanumeric characters)

[Initial value]

None

[Input mode]

BGP mode

[Description]

This performs TCP MD5 authentication with a BGP peer.

The password must be set the same as the BGP peer.

7.13.45 Create BGP peer group

[Syntax]

neighbor *GROUPNAME* **peer-group**
no neighbor *GROUPNAME* **peer-group**

[Parameter]

GROUPNAME	:	Group name (maximum of 64 single-byte alphanumeric characters)

[Initial value]

None

[Input mode]

BGP mode

[Description]

This defines the contents of the BGP peer group.

When using a BGP peer group, the group must be registered by following the steps below.

1. Use this command to define the peer group.
2. Use the "neighbor remote-as" command to specify the AS number.
3. Use the "neighbor peer-group (v4)" command or the "neighbor peer-group (v6)" command to specify the peer IP address.

7.13.46 Add a peer to a BGP peer group (BGP IPv4)

[Syntax]

neighbor *PEER* **peer-group** *GROUPNAME*
no neighbor *PEER* **peer-group** *GROUPNAME*

[Parameter]

PEER	:	<A.B.C.D> IPv4 address of the BGP peer
GROUPNAME	:	Group name (maximum of 64 single-byte alphanumeric characters)

[Initial value]

None

[Input mode]

BGP mode

[Description]

This registers the IPv4-BGP peer in the BGP peer group.

Specify the peer group name defined by the "neighbor peer-group" command in GROUPNAME.

7.13.47 Add a peer to a BGP peer group (BGP IPv6)

[Syntax]

neighbor *PEER* **peer-group** *GROUPNAME*
no neighbor *PEER* **peer-group** *GROUPNAME*

[Parameter]

PEER	:	<X:X::X:X> IPv6 address of the BGP peer
GROUPNAME	:	Group name (maximum of 64 single-byte alphanumeric characters)

[Initial value]

None

[Input mode]

BGP IPv6 address-family mode

[Description]

This registers the IPv6-BGP peer in the BGP peer group.

Specify the peer group name defined by the "neighbor peer-group" command in GROUPNAME.

This cannot be executed if the stack is enabled.

7.13.48 Apply prefix list of routes received from a BGP peer (BGP IPv4)

[Syntax]

neighbor *PEER* **prefix-list** *PLIST_NUM DIRECTION*
no neighbor *PEER* **prefix-list** *PLIST_NUM DIRECTION*

[Parameter]

PEER : Peer setting value

Setting value	Description
<A.B.C.D>	IPv4 address of the BGP peer
<X:X::X:X>	IPv6 address of the BGP peer
BGP peer group name	Up to 64 half-width alphanumeric characters

PLIST_NUM : <1-100>

Prefix list number

DIRECTION : Direction

Setting value	Description
in	Receiving
out	Transmitting

[Initial value]

None

[Input mode]

BGP mode

[Description]

This filters prefixes in route information when UPDATE messages are transmitted/received.

PLIST_NUM specifies the prefix list number for the "ip prefix-list" command.

7.13.49 Apply prefix list of routes received from a BGP peer (BGP IPv6)

[Syntax]

neighbor *PEER* **prefix-list** *PLIST_NUM DIRECTION*
no neighbor *PEER* **prefix-list** *PLIST_NUM DIRECTION*

[Parameter]

PEER : Peer setting value

Setting value	Description
<A.B.C.D>	IPv4 address of the BGP peer
<X:X::X:X>	IPv6 address of the BGP peer
BGP peer group name	Up to 64 half-width alphanumeric characters

PLIST_NUM : Prefix list number

DIRECTION : Direction

Setting value	Description
in	Receiving
out	Transmitting

[Initial value]

None

[Input mode]

BGP IPv6 address-family mode

[Description]

This filters prefixes in route information when UPDATE messages are transmitted/received.

PLIST_NUM specifies the prefix list number for the "ipv6 prefix-list" command.

7.13.50 Set AS number for BGP peer

[Syntax]

neighbor *PEER* **remote-as** *AS_NUM*
no neighbor *PEER* **remote-as** [*AS_NUM*]

[Parameter]

PEER : Peer setting value

Setting value	Description
<A.B.C.D>	IPv4 address of the BGP peer
<X:X::X:X>	IPv6 address of the BGP peer
BGP peer group name	Up to 64 half-width alphanumeric characters

AS_NUM : <1-4294967295>

AS number

[Initial value]

None

[Input mode]

BGP mode

[Description]

This specifies the number of the AS to which a BGP peer belongs.

7.13.51 Remove private AS numbers from the AS_PATH attribute when advertising routes (BGP IPv4)

[Syntax]

neighbor *PEER* **remove-private-as** *SWITCH*
no neighbor *PEER* **remove-private-as** [*SWITCH*]

[Parameter]

PEER : Peer setting value

Setting value	Description
<A.B.C.D>	IPv4 address of the BGP peer
<X:X::X:X>	IPv6 address of the BGP peer
BGP peer group name	Up to 64 half-width alphanumeric characters

SWITCH : AS_PATH attribute operations

Setting value	Description
enable	When advertising routes to a BGP peer, private AS numbers are removed from the AS_PATH attribute.
disable	When advertising routes to a BGP peer, private AS numbers are not removed from the AS_PATH attribute.

[Initial value]

neighbor remove-private-as disable

[Input mode]

BGP mode

[Description]

This removes private AS numbers from the AS_PATH attribute when advertising routes to a BGP peer.

7.13.52 Remove private AS numbers from the AS_PATH attribute when advertising routes (BGP IPv6)

[Syntax]

neighbor *PEER* **remove-private-as** *SWITCH*
no neighbor *PEER* **remove-private-as** [*SWITCH*]

[Parameter]

PEER : Peer setting value

Setting value	Description
<A.B.C.D>	IPv4 address of the BGP peer
<X:X::X:X>	IPv6 address of the BGP peer
BGP peer group name	Up to 64 half-width alphanumeric characters

SWITCH : AS_PATH attribute operations

Setting value	Description
enable	When advertising routes to a BGP peer, private AS numbers are removed from the AS_PATH attribute.
disable	When advertising routes to a BGP peer, private AS numbers are not removed from the AS_PATH attribute.

[Initial value]

neighbor remove-private-as disable

[Input mode]

BGP IPv6 address-family mode

[Description]

This removes private AS numbers from the AS_PATH attribute when advertising routes to a BGP peer.
This cannot be executed if the stack is enabled.

7.13.53 Setting to apply route maps when advertisting routes to a BGP peer (BGP IPv4)

[Syntax]

neighbor *PEER* **route-map** *ROUTE-MAP-ID* [*DIRECTION*]
no neighbor *PEER* **route-map** *ROUTE-MAP-ID*

[Parameter]

PEER : Peer setting value

Setting value	Description
<A.B.C.D>	IPv4 address of the BGP peer
<X:X::X:X>	IPv6 address of the BGP peer
BGP peer group name	Up to 64 half-width alphanumeric characters

ROUTE-MAP-ID : <1-4094>

Route map ID

DIRECTION : Direction

Setting value	Description
in	Applied when an UPDATE message is received.
out	Applied when an UPDATE message is transmitted.

[Initial value]

None

[Input mode]

BGP mode

[Description]

This specifies route maps for BGP peers, and adds, deletes or modifies attributes for specific route information when transmitting and receiving UPDATE messages.

7.13.54 Apply route maps when advertisting routes to a BGP peer (BGP IPv6)

[Syntax]

neighbor *PEER* **route-map** *ROUTE-MAP-ID* [*DIRECTION*]
no neighbor *PEER* **route-map** *ROUTE-MAP-ID*

[Parameter]

PEER : Peer setting value

Setting value	Description
<A.B.C.D>	IPv4 address of the BGP peer
<X:X::X:X>	IPv6 address of the BGP peer
BGP peer group name	Up to 64 half-width alphanumeric characters

ROUTE-MAP-ID : <1-4094>

Route map ID

DIRECTION : Direction

Setting value	Description
in	Applied when an UPDATE message is received.
out	Applied when an UPDATE message is transmitted.

[Initial value]

None

[Input mode]

BGP IPv6 address-family mode

[Description]

This specifies route maps for BGP peers, and adds, deletes or modifies attributes for specific route information when transmitting and receiving UPDATE messages.

7.13.55 Specify BGP peer as route reflector client (BGP IPv4)

[Syntax]

neighbor *PEER* **route-reflector-client** *SWITCH*
no neighbor *PEER* **route-reflector-client** [*SWITCH*]

[Parameter]

PEER : Peer setting value

Setting value	Description
<A.B.C.D>	IPv4 address of the BGP peer
<X:X::X:X>	IPv6 address of the BGP peer
BGP peer group name	Up to 64 half-width alphanumeric characters

SWITCH : Route reflector operations

Setting value	Description
enable	Enables the route reflector.
disable	Disables the route reflector.

[Initial value]

neighbor route-reflector-client disable

[Input mode]

BGP mode

[Description]

This makes this device operate as a route reflector towards specified peers.

To use route reflection, you must use the "bgp client-to-client reflection" command to enable the route reflection function.

7.13.56 Specify BGP peer as route reflector client (BGP IPv6)

[Syntax]

neighbor *PEER* **route-reflector-client** *SWITCH*
no neighbor *PEER* **route-reflector-client** [*SWITCH*]

[Parameter]

PEER : Peer setting value

Setting value	Description
<A.B.C.D>	IPv4 address of the BGP peer
<X:X::X:X>	IPv6 address of the BGP peer
BGP peer group name	Up to 64 half-width alphanumeric characters

SWITCH : Route reflector operations

Setting value	Description
enable	Enables the route reflector.
disable	Disables the route reflector.

[Initial value]

neighbor route-reflector-client disable

[Input mode]

BGP IPv6 address-family mode

[Description]

This makes this device operate as a route reflector towards specified peers.

To use route reflection, you must use the "bgp client-to-client reflection" command to enable the route reflection function.

This cannot be executed if the stack is enabled.

7.13.57 Permit/deny advertisement of community attributes for a BGP peer (BGP IPv4)

[Syntax]

neighbor *PEER* **send-community** *SWITCH*
no neighbor *PEER* **send-community** [*SWITCH*]

[Parameter]

PEER : Peer setting value

Setting value	Description
<A.B.C.D>	IPv4 address of the BGP peer
<X:X::X:X>	IPv6 address of the BGP peer
BGP peer group name	Up to 64 half-width alphanumeric characters

SWITCH : COMMUNITIES attribute operations

Setting value	Description
enable	Advertises COMMUNITIES attributes to BGP peers
disable	Does not advertise COMMUNITIES attributes to BGP peers

[Initial value]

neighbor send-community enable

[Input mode]

BGP mode

[Description]

Advertises COMMUNITIES attributes to BGP peers

7.13.58 Permit/deny advertisement of community attributes for a BGP peer (BGP IPv6)

[Syntax]

neighbor *PEER* **send-community** *SWITCH*
no neighbor *PEER* **send-community** [*SWITCH*]

[Parameter]

PEER : Peer setting value

Setting value	Description
<A.B.C.D>	IPv4 address of the BGP peer
<X:X::X:X>	IPv6 address of the BGP peer
BGP peer group name	Up to 64 half-width alphanumeric characters

SWITCH : COMMUNITIES attribute operations

Setting value	Description
enable	Advertises COMMUNITIES attributes to BGP peers
disable	Does not advertise COMMUNITIES attributes to BGP peers

[Initial value]

neighbor send-community enable

[Input mode]

BGP IPv6 address-family mode

[Description]

Advertises COMMUNITIES attributes to BGP peers

This cannot be executed if the stack is enabled.

7.13.59 Disconnect session with BGP peer

[Syntax]

neighbor *PEER* **shutdown**
no neighbor *PEER* **shutdown**

[Parameter]

PEER : Peer setting value

Setting value	Description
<A.B.C.D>	IPv4 address of the BGP peer
<X:X::X:X>	IPv6 address of the BGP peer
BGP peer group name	Up to 64 half-width alphanumeric characters

[Initial value]

None

[Input mode]

BGP mode

[Description]

This stops communications with the BGP peer.

7.13.60 Retain/discard original route information (BGP IPv4)

[Syntax]

neighbor *PEER* **soft-reconfiguration inbound** *SWITCH*
no neighbor *PEER* **soft-reconfiguration inbound** [*SWITCH*]

[Parameter]

PEER : Peer setting value

Setting value	Description
<A.B.C.D>	IPv4 address of the BGP peer
<X:X::X:X>	IPv6 address of the BGP peer
BGP peer group name	Up to 64 half-width alphanumeric characters

SWITCH : Operations for the route before filtering

Setting value	Description
enable	Retains the route before filtering.
disable	Does not retain the route before filtering.

[Initial value]

neighbor soft-reconfiguration inbound disable

[Input mode]

BGP mode

[Description]

This retains the routes as received from the BGP peer before filtering.

7.13.61 Retain/discard original route information (BGP IPv6)

[Syntax]

neighbor *PEER* **soft-reconfiguration inbound** *SWITCH*
no neighbor *PEER* **soft-reconfiguration inbound** [*SWITCH*]

[Parameter]

PEER : Peer setting value

Setting value	Description
<A.B.C.D>	IPv4 address of the BGP peer
<X:X::X:X>	IPv6 address of the BGP peer
BGP peer group name	Up to 64 half-width alphanumeric characters

SWITCH : Operations for the route before filtering

Setting value	Description
enable	Retains the route before filtering.
disable	Does not retain the route before filtering.

[Initial value]

neighbor soft-reconfiguration inbound disable

[Input mode]

BGP IPv6 address-family mode

[Description]

This retains the routes as received from the BGP peer before filtering.

7.13.62 Various timer settings related to communications with BGP peers

[Syntax]

neighbor *PEER* **timers** *KEEPALIVE HOLDTIME*
neighbor *PEER* **timers** *connect CONNECT*
no neighbor *PEER* **timers** [*KEEPALIVE HOLDTIME*]
no neighbor *PEER* **timers** *connect* [*CONNECT*]

[Parameter]

PEER : Peer setting value

Setting value	Description
<A.B.C.D>	IPv4 address of the BGP peer
<X:X::X:X>	IPv6 address of the BGP peer
BGP peer group name	Up to 64 half-width alphanumeric characters

KEEPALIVE : <0-65535>

KEEPALIVE message transmission interval (in seconds) proposed by the BGP peer

HOLDTIME : 0 or <3-65535>

Hold Time interval (sec.) proposed to BGP peer

CONNECT : <1-65535>

Retry interval (sec.) for connection with BGP peer

[Initial value]

neighbor timers connect 120

[Input mode]

BGP mode

[Description]

This configures the various timers used during communication with BGP peers.

KEEPALIVE must be set to a time equal to or greater than HOLDTIME.

The values set for the KEEPALIVE and HOLDTIME parameters in this command take precedence over the settings provided by the "timers bgp" command. If not configured, the settings provided by the "timers bgp" command are used.

The KEEPALIVE and HOLDTIME parameters contain values that are proposed during negotiation with the BGP peer, so the values determined after negotiation are actually used.

When "0" is specified for the KEEPALIVE parameter, no liveness check is performed using KEEPALIVE messages.

7.13.63 Set weight of routes received from a BGP peer (BGP IPv4)

[Syntax]

neighbor *PEER* **weight** *WEIGHT*
no neighbor *PEER* **weight** [*WEIGHT*]

[Parameter]

PEER : Peer setting value

Setting value	Description
<A.B.C.D>	IPv4 address of the BGP peer
<X:X::X:X>	IPv6 address of the BGP peer
BGP peer group name	Up to 64 half-width alphanumeric characters

WEIGHT : <0-65535>

[Initial value]

neighbor weight 0

[Input mode]

BGP mode

[Description]

This sets the weight of routes advertised from a BGP peer.

If multiple routes with the same destination exist, the weight is given priority over the various attributes, and the routes with greater weight are used.

7.13.64 Set weight of routes received from a BGP peer (BGP IPv6)

[Syntax]

neighbor *PEER* **weight** *WEIGHT*
no neighbor *PEER* **weight** [*WEIGHT*]

[Parameter]

PEER : Peer setting value

Setting value	Description
<A.B.C.D>	IPv4 address of the BGP peer
<X:X::X:X>	IPv6 address of the BGP peer
BGP peer group name	Up to 64 half-width alphanumeric characters

WEIGHT : <0-65535>

[Initial value]

neighbor weight 0

[Input mode]

BGP IPv6 address-family mode

[Description]

This sets the weight of routes advertised from a BGP peer.

If multiple routes with the same destination exist, the weight is given priority over the various attributes, and the routes with greater weight are used.

This cannot be executed if the stack is enabled.

7.13.65 Set LOCAL_PREF attribute value

[Syntax]

bgp default local-preference *PREFERENCE*
no bgp default local-preference [*PREFERENCE*]

[Parameter]

PREFERENCE : <0-4294967295>

Default value of LOCAL_PREF attribute

[Initial value]

bgp default local-preference 100

[Input mode]

BGP mode

[Description]

This sets the default value of the LOCAL_PREF attribute for the route advertised to the BGP peer by iBGP.

7.13.66 Settings to retain/disregard messages when the expected AS is not at the start of the AS_PATH attribute

[Syntax]

bgp enforce-first-as *SWITCH*
no bgp enforce-first-as [*SWITCH*]

[Parameter]

SWITCH : Operations when the associated AS is not at the start of the AS_PATH attribute

Setting value	Description
enable	Discards the UPDATE message.
disable	Retains the UPDATE message.

[Initial value]

bgp enforce-first-as disable

[Input mode]

BGP mode

[Description]

When an UPDATE message is received from the eBGP peer, this sets whether to discard the UPDATE message if the AS to which the BGP peer belongs is not at the start of the AS_PATH attribute.

7.13.67 Setting to use/disregard MED when selecting routes advertised by eBGPs with different AS associations

[Syntax]

bgp always-compare-med *SWITCH*
no bgp always-compare-med [*SWITCH*]

[Parameter]

SWITCH : MED attribute operations

Setting value	Description
enable	Use the MED attribute.
disable	Do not use the MED attribute.

[Initial value]

bgp always-compare-med disable

[Input mode]

BGP mode

[Description]

When routes with identical destinations are obtained from multiple eBGP peers, this sets whether the MED attribute is used for route selection.

7.13.68 Set whether to use/disregard AS_PATH attribute in route selection

[Syntax]

bgp bestpath as-path ignore *SWITCH*
no bgp bestpath as-path ignore [*SWITCH*]

[Parameter]

SWITCH : AS_PATH attribute operations

Setting value	Description
enable	Use the AS_PATH attribute in route selection.
disable	Do not use the AS_PATH attribute in route selection.

[Initial value]

bgp bestpath as-path ignore disable

[Input mode]

BGP mode

[Description]

When routes with identical destinations are obtained from multiple BGP peers, this sets whether the AS_PATH attribute is used for route selection.

7.13.69 Setting to enable/disable use of AS_PATH length for AS confederations during route selection

[Syntax]

bgp bestpath compare-confed-aspath *SWITCH*
no bgp bestpath compare-confed-aspath [*SWITCH*]

[Parameter]

SWITCH : AS path length condition operations

Setting value	Description
enable	Enables conditions for AS path length.
disable	Disables conditions for AS path length.

[Initial value]

bgp bestpath compare-confed-aspath disable

[Input mode]

BGP mode

[Description]

When routes with identical destinations are obtained from multiple BGP peers, this sets whether the AS path length of AS confederations is used as a condition in selecting routes, if the AS_PATH attribute lengths are compared.

7.13.70 Set enable/disable router ID conditions for route selection

[Syntax]

bgp bestpath compare-routerid *SWITCH*
no bgp bestpath compare-routerid [*SWITCH*]

[Parameter]

SWITCH : Route ID operations

Setting value	Description
enable	Use the router ID for route selection.
disable	Do not use the router ID for route selection.

[Initial value]

bgp bestpath compare-routerid disable

[Input mode]

BGP mode

[Description]

When routes with identical destinations are obtained from multiple BGP peers, this sets whether the router ID is used for route selection.

If "enable" is specified, routes obtained from BGP peers with smaller route IDs are given priority.

7.13.71 Set enable/disable ORIGIN attribute conditions during multiple route selection

[Syntax]

bgp bestpath compare-originator-id *SWITCH*
no bgp bestpath compare-originator-id [*SWITCH*]

[Parameter]

SWITCH : ORIGIN attribute operations

Setting value	Description
enable	Use the ORIGIN attribute during route selection.
disable	Do not use the ORIGIN attribute during route selection.

[Initial value]

bgp bestpath compare-originator-id enable

[Input mode]

BGP mode

[Description]

When routes with identical destinations are obtained from multiple BGP peers, this sets whether the ORIGIN attribute is used for route selection.

7.13.72 Set parameter for MED attribute by route selection

[Syntax]

bgp bestpath med [*confed*] [*missing-as-worst*]
no bgp bestpath med [*confed*] [*missing-as-worst*]

[Keyword]

confed	:	Use MED for selecting the route obtained from the AS confederation eBGP peer.
missing-as-worst	:	If the MED attribute is not included in the route obtained from the BGP peer, consider the MED attribute value as the maximum.

[Initial value]

None

[Input mode]

BGP mode

[Description]

When routes with identical destinations are obtained from multiple BGP peers, this configures the MED attribute handling for route selection.

7.13.73 Delete MED attribute from received route information

[Syntax]

bgp bestpath med remove-recv-med
no bgp bestpath med remove-recv-med

[Initial value]

None

[Input mode]

BGP mode

[Description]

Deletes the MED attribute from route information that is received via the UPDATE command.

7.13.74 Delete MED attribute from transmitted route information

[Syntax]

bgp bestpath med remove-send-med
no bgp bestpath med remove-send-med

[Initial value]

None

[Input mode]

BGP mode

[Description]

Deletes the MED attribute from route information that is transmitted via the UPDATE command.

7.13.75 Set processing order for route selection if there are multiple routes with the same destination

[Syntax]

bgp deterministic-med *SWITCH*
no bgp deterministic-med [*SWITCH*]

[Parameter]

SWITCH : Operations for processing order of route selection

Setting value	Description
enable	Selects the optimal route for each AS from which the route is obtained, and determines the optimal route by comparing routes against each other.
disable	Determines the optimal route regardless of which AS the route was obtained from.

[Initial value]

bgp deterministic-med disable

[Input mode]

BGP mode

[Description]

Sets the processing order for route selection if there are multiple routes with the same destination.

If "enable" is set, this selects the optimal route for each AS from which the route that was obtained, and determines the optimal route by comparing the routes selected from each AS against each other.

If "enable" is not set, this selects the optimal route right when the route is obtained, regardless of the AS from which the route that was obtained.

7.13.76 Aggregate the advertised routes and register in the BGP routing table (BGP IPv4)

[Syntax]

aggregate-address *RANGE* [*as-set*] [*summary-only*]
no aggregate-address *RANGE* [*as-set*] [*summary-only*]

[Keyword]

as-set : If the AS_PATH attribute for each route before aggregation differs, include all AS numbers into the AS_PATH attribute of the route before aggregation. If this keyword has not been set and if the AS_PATH attribute for each route before aggregation differs, the AS_PATH attribute for the route after aggregation is cleared.

summary-only : Advertises only the route after aggregation using BGP peer route advertisement. If this keyword has not been set, each route before aggregation and the routes after aggregation are both advertised to the BGP peer.

[Parameter]

RANGE : <A.B.C.D/M>

Range of routes to aggregate

[Initial value]

None

[Input mode]

BGP mode

[Description]

When a route is registered with the BGP routing table, aggregate the routes within the range specified by RANGE and then register.

7.13.77 Aggregate the advertised route and register in the BGP routing table (BGP IPv6)

[Syntax]

aggregate-address *RANGE* [*as-set*] [*summary-only*]
no aggregate-address *RANGE* [*as-set*] [*summary-only*]

[Keyword]

as-set	:	If the AS_PATH attribute for each route before aggregation differs, include all AS numbers into the AS_PATH attribute of the route before aggregation. If this keyword has not been set and if the AS_PATH attribute for each route before aggregation differs, the AS_PATH attribute for the route after aggregation is cleared.
summary-only	:	Advertises only the route after aggregation using BGP peer route advertisement. If this keyword has not been set, each route before aggregation and the routes after aggregation are both advertised to the BGP peer.

[Parameter]

RANGE	:	<X:X::X:X/M> Range of routes to aggregate

[Initial value]

None

[Input mode]

BGP IPv6 address-family mode

[Description]

When a route is registered with the BGP routing table, aggregate the routes within the range specified by RANGE and then register.

This cannot be executed if the stack is enabled.

7.13.78 Setting to enable or disable advertising aggregated routes using classful addresses to peers

[Syntax]

auto-summary *SWITCH*
no auto-summary [*SWITCH*]

[Parameter]

SWITCH : BGP peer operations

Setting value	Description
enable	Advertises individual routes before aggregation to BGP peers.
disable	Does not advertise individual routes before aggregation to BGP peers.

[Initial value]

auto-summary disable

[Input mode]

BGP mode

[Description]

Aggregates routes into classful networks and advertises them to BGP peers.

Individual routes before aggregation are not advertised to BGP peers.

7.13.79 Prefix settings loaded into the BGP routing table (BGP IPv4)

[Syntax]

network *PREFIX_MASK* [*backdoor*]
network *PREFIX* [*mask MASK*] [*backdoor*]
no network *PREFIX_MASK* [*backdoor*]
no network *PREFIX* [*mask MASK*] [*backdoor*]

[Keyword]

backdoor	:	Specifies the BGP backdoor route

[Parameter]

PREFIX_MASK	:	<A.B.C.D/M> IPv4 network prefix
PREFIX	:	<A.B.C.D> IPv4 network prefix
MASK	:	<A.B.C.D> Subnet mask

[Initial value]

None

[Input mode]

BGP mode

[Description]

Advertises the specified IPv4 network prefix to the BGP peer as a route.

If the "network synchronization" command has been set, the route is advertised to the BGP peer only when the route specified by this command exists in the IP routing table.

When the "backdoor" keyword is used, you can advertise the specified IPv4 network prefix as 200 routes within the administrative distance.

7.13.80 Prefix settings loaded into the BGP routing table (BGP IPv6)

[Syntax]

network *PREFIX_MASK* [*backdoor*]

[Keyword]

backdoor	:	Specifies the BGP backdoor route

[Parameter]

PREFIX_MASK	:	<X:X::X:X/M> IPv6 network prefix

[Initial value]

None

[Input mode]

BGP IPv6 address-family mode

[Description]

Advertises the specified IPv6 network prefix to the BGP peer as a route.

If the "network synchronization" command has been set, the route is advertised to the BGP peer only when the route specified by this command exists in the IP routing table.

When the backdoor keyword is used, the specified IPv6 network prefix is advertised with an administrative distance of 200.

This cannot be executed if the stack is enabled.

7.13.81 Advertise routes to BGP peers only if present in the IP routing table (BGP IPv4)

[Syntax]

network synchronization *SWITCH*
no network synchronization [*SWITCH*]

[Parameter]

SWITCH : BGP peer operations

Setting value	Description
enable	Advertises the route to the BGP peer only when the specified route exists in the IP routing table.
disable	Advertises the route to the BGP peer regardless of whether the specified route exists in the IP routing table.

[Initial value]

network synchronization disable

[Input mode]

BGP mode

[Description]

The device only advertises routes to BGP peers when an equivalent route exists in the IP routing table for the IPv4 network prefix specified by the "network" command.

7.13.82 Advertise routes to BGP peers only if present in the IP routing table (BGP IPv6)

[Syntax]

network synchronization *SWITCH*
no network synchronization [*SWITCH*]

[Parameter]

SWITCH : BGP peer operations

Setting value	Description
enable	Advertises the route to the BGP peer only when the specified route exists in the IP routing table.
disable	Advertises the route to the BGP peer regardless of whether the specified route exists in the IP routing table.

[Initial value]

network synchronization disable

[Input mode]

BGP IPv6 address-family mode

[Description]

The device only advertises routes to BGP peers when an equivalent route exists in the IP routing table for the IPv6 network prefix specified by the "network" command.

This cannot be executed if the stack is enabled.

7.13.83 Use BGP to readvertise routes with the specified protocol (BGP IPv4)

[Syntax]

redistribute *KIND*

[Parameter]

connected : Readvertise connected route using BGP

ospf [PROCESS_ID] : Readvertise OSPF route using BGP

PROCESS_ID : <0-65535>

OSPF process ID

rip : Readvertise RIP route using BGP

static : Readvertise static route

[Initial value]

None

[Input mode]

BGP mode

[Description]

This readvertises routes of the specified type to BGP peers.

7.13.84 Use BGP to readvertise routes with the specified protocol (BGP IPv6)

[Syntax]

redistribute *KIND*

[Parameter]

connected : Readvertise connected route using BGP

ospf [PROCESS_ID] : Readvertise OSPF route using BGP

PROCESS_ID : <0-65535>

OSPF process ID

rip : Readvertise RIP route using BGP

static : Readvertise static route

[Initial value]

None

[Input mode]

BGP IPv6 address-family mode

[Description]

This readvertises routes of the specified type to BGP peers.

This cannot be executed if the stack is enabled.

7.13.85 Set whether to use route synchronization with the IGP (RIP, OSPF) or not (BGP IPv4)

[Syntax]

synchronization *SWITCH*

[Parameter]

SWITCH : Operation with routes learned from RIP or OSPF

Setting value	Description
enable	Use the route if it was not learned from RIP or OSPF.
disable	Do not use the route if it was not learned from RIP or OSPF.

[Initial value]

synchronization disable

[Input mode]

BGP mode

[Description]

When routes are received from an iBGP peer, the routes are used if they were learned via RIP or OSPF.

7.13.86 Set whether to use route synchronization with the IGP (RIP, OSPF) or not (BGP IPv6)

[Syntax]

synchronization

[Initial value]

None

[Input mode]

BGP IPv6 address-family mode

[Description]

When routes are received from an iBGP peer, the routes are used if they were learned via RIP or OSPF.

This cannot be executed if the stack is enabled.

7.13.87 Only aggregate routes with same NEXT_HOP attribute

[Syntax]

bgp aggregate-nexthop-check *SWITCH*
no bgp aggregate-nexthop-check [*SWITCH*]

[Parameter]

SWITCH : Route operation for same destination

Setting value	Description
enable	The next hop aggregates only the same routes.
disable	Routes are aggregated, regardless of the next hop.

[Initial value]

bgp aggregate-nexthop-check disable

[Input mode]

global configuration mode

[Description]

When aggregating routes with the same destination, only routes with the same next hop are aggregated.

7.13.88 Enable/disable BGP next hop trigger

[Syntax]

bgp nexthop-trigger *SWITCH*
no bgp nexthop-trigger [*SWITCH*]

[Parameter]

SWITCH : BGP next hop tracking operations

Setting value	Description
enable	Enables BGP next hop tracking.
disable	Disables BGP next hop tracking.

[Initial value]

bgp nexthop-trigger disable

[Input mode]

global configuration mode

[Description]

Enables BGP next hop tracking.

7.13.89 Set delay interval for BGP next hop tracking

[Syntax]

bgp nexthop-trigger delay *DELAY*
no bgp nexthop-trigger delay [*DELAY*]

[Parameter]

DELAY : <1-100> seconds

[Initial value]

bgp nexthop-trigger delay 5

[Input mode]

global configuration mode

[Description]

This sets the delay interval for BGP next hop tracking.

7.13.90 Enable route reflector (BGP IPv4)

[Syntax]

bgp client-to-client reflection *SWITCH*
no bgp client-to-client reflection [*SWITCH*]

[Parameter]

SWITCH : Route reflector operations

Setting value	Description
enable	Enables route reflector operations.
disable	Disables route reflector operations.

[Initial value]

bgp client-to-client reflection enable

[Input mode]

BGP mode

[Description]

Sets route reflection.

When this is set to "enable", the router operates as a route reflector.

The "neighbor route-reflector-client" command must be used to specify the route reflection peer.

When setting up multiple route reflectors in an AS, you must use the "bgp cluster-id" command to explicitly separate the clusters by setting the cluster ID.

7.13.91 Enable route reflector (BGP IPv6)

[Syntax]

bgp client-to-client reflection *SWITCH*
no bgp client-to-client reflection [*SWITCH*]

[Parameter]

SWITCH : Route reflector operations

Setting value	Description
enable	Enables route reflector operations.
disable	Disables route reflector operations.

[Initial value]

bgp client-to-client reflection enable

[Input mode]

BGP IPv6 address-family mode

[Description]

Sets route reflection.

When this is set to "enable", the router operates as a route reflector.

The "neighbor route-reflector-client" command must be used to specify the route reflection client.

When setting up multiple route reflectors in an AS, you must use the "bgp cluster-id" command to explicitly separate the clusters by setting the cluster ID.

This cannot be executed if the stack is enabled.

7.13.92 Cluster ID settings

[Syntax]

bgp cluster-id *ID*
no bgp cluster-id [*ID*]

[Parameter]

ID : Cluster ID

Setting value	Description
<0-4294967295>	4-byte integer
<A.B.C.D>	IPv4 format

[Initial value]

None

[Input mode]

BGP mode

[Description]

Sets the route reflection cluster ID.

When setting up multiple route reflectors in an AS, you must use this command to explicitly separate the clusters by assigning different cluster IDs.

7.13.93 Specify AS number of confederation to join

[Syntax]

bgp confederation identifier *AS_NUM*
no bgp confederation identifier [*AS_NUM*]

[Parameter]

AS_NUM : <1-4294967295>

AS number

[Initial value]

None

[Input mode]

BGP mode

[Description]

Joins the AS confederation identified by the specified AS number.

7.13.94 Specify AS number of other confederation

[Syntax]

bgp confederation peers *SUB_AS_NUM* [*SUB_AS_NUM* ...]
no bgp confederation peers [*SUB_AS_NUM* ...]

[Parameter]

SUB_AS_NUM : <1-4294967295>
Sub AS number

[Initial value]

None

[Input mode]

BGP mode

[Description]

Specifies the sub AS number of a sub AS other than the one that this device belongs to.

SUB_AS_NUM can specify up to 20 numbers, separated by single-byte spaces.

7.13.95 Set parameter for AS_PATH attribute

[Syntax]

match as-path *AS_ACL_NUM*
no match as-path

[Parameter]

AS_NUM : <1-100>
AS path access list number

[Initial value]

None

[Input mode]

Route map mode

[Description]

This sets the applicable parameters for BGP AS_PATH attributes in the route map entry.

If this command is executed with the "no" syntax, the applicable parameters for BGP AS_PATH attributes are deleted from the route map entry.

[Note]

For "permit" entries, the processing contents (set) will be executed if the AS_PATH of the transmitted/received BGP UPDATE message matches the AS path access list.

For "deny" entries, the processing contents (set) will not be executed if the AS_PATH attribute of the transmitted/received BGP UPDATE message matches the AS path access list, and the next applicable parameter is processed.

7.13.96 Set COMMUNITIES attribute parameter

[Syntax]

match community *LIST_NUM_STANDARD* [*exact-match*]
match community *LIST_NUM_EXPAND* [*exact-match*]
no match community [*LIST_NUM_STANDARD* [*exact-match*]]
no match community [*LIST_NUM_EXPAND* [*exact-match*]]

[Parameter]

LIST_NUM_STANDARD	:	<1-99>
		Standard community list number
LIST_NUM_EXPAND	:	<100-500>
		Extended community list number

[Initial value]

None

[Input mode]

Route map mode

[Description]

This sets the applicable parameters for BGP COMMUNITIES attributes in the route map entry.

If this command is executed with the "no" syntax, the applicable parameters for BGP COMMUNITIES attributes are deleted from the route map entry.

[Note]

For "permit" entries, the processing contents (set) will be executed if the COMMUNITIES attribute in the transmitted/received BGP UPDATE message matches the community list.

For "deny" entries, the processing contents (set) are not executed if the COMMUNITIES attribute in the transmitted/received BGP UPDATE message matches the community list, and the next applicable parameter is processed.

When "exact-match" is specified, the processing contents (set) are executed only when a perfect match with the community list exists. When this is omitted, the processing contents (set) are executed when a partial match exists.

7.13.97 Set destination address condition (BGP IPv4)

[Syntax]

match access-list *ACL-ID*
no match access-list [*ACL-ID*]

[Parameter]

ACL-ID	:	<1-2000>
		ID of IPv4 access list

[Initial value]

None

[Input mode]

Route map mode

[Description]

Sets the application parameters for route map entries.

If this command is executed with the "no" syntax, the application parameters are deleted from the route map entry.

[Note]

For a "permit" entry, the processing contents are executed when the routing information destination prefix matches the access list.

For a "deny" entry, the processing contents are not executed and the next applicable conditions are examined when the routing information destination prefix matches the access list.

7.13.98 Set condition for IPv4 next hop

[Syntax]

match ip next-hop *ACL-ID*
no match ip next-hop [*ACL_ID*]

[Parameter]

ACL-ID : <1-2000>

ID of IPv4 access list

[Initial value]

None

[Input mode]

Route map mode

[Description]

This sets the conditions under which route map entries are applied to BGP routes.

If this command is executed with the "no" syntax, the BGP applicability conditions are deleted from the route map entry.

[Note]

For "permit" entries, the processing contents (set) will be executed if the next hop for the route of the BGP UPDATE message to transmit/receive matches the IPv4 access list.

For "deny" entries, the processing contents (set) will not be executed and the next applicable conditions are examined, if the next hop for the route of the BGP UPDATE message to transmit/receive matches the IPv4 access list.

7.13.99 Set destination address condition (BGP IPv6)

[Syntax]

match access-list *ACL-ID*
no match access-list [*ACL-ID*]

[Parameter]

ACL-ID : <3001-4000>

ID of IPv6 access list

[Initial value]

None

[Input mode]

Route map mode

[Description]

Sets the application parameters for route map entries.

If this command is executed with the "no" syntax, the application parameters are deleted from the route map entry.

[Note]

For a "permit" entry, the processing contents are executed when the routing information destination prefix matches the access list.

For a "deny" entry, the processing contents are not executed and the next applicable conditions are examined when the routing information destination prefix matches the access list.

7.13.100 Set condition for IPv6 next hop

[Syntax]

match ipv6 next-hop *NEXTHOP*
match ipv6 next-hop *ACL-ID*
no match ipv6 next-hop [*NEXTHOP*]
no match ipv6 next-hop [*ACL_ID*]

[Parameter]

ACL-ID : <3001-4000>

ID of IPv6 access list

NEXTHOP : <X:X::X:X>

IPv6 next hop

[Initial value]

None

[Input mode]

Route map mode

[Description]

This sets the conditions under which route map entries are applied to BGP routes.

If this command is executed with the "no" syntax, the BGP applicability conditions are deleted from the route map entry.

[Note]

For "permit" entries, the processing contents (set) will be executed if the next hop for the route of the BGP UPDATE message to transmit/receive matches NEXTHOP or the IPv6 access list.

For "deny" entries, the processing contents (set) will not be executed and the next applicable conditions are examined, if the next hop for the route of the BGP UPDATE message to transmit/receive matches NEXTHOP or the IPv6 access list.

7.13.101 Set metric value conditions

[Syntax]

match metric *METRIC*
no match metric [*METRIC*]

[Parameter]

METRIC	:	<0-4294967295>
		MED value

[Initial value]

None

[Input mode]

Route map mode

[Description]

This sets the applicable parameters for BGP MED attributes in the route map entry.

If this command is executed with the "no" syntax, the applicable parameters for BGP MED attributes are deleted from the route map entry.

[Note]

For "permit" entries, the processing contents (set) will be executed if the MED attribute value of the BGP UPDATE message to transmit/receive matches the set MED value.

For "deny" entries, the processing contents (set) will not be executed and the next applicable parameter is processed, if the MED attribute of the BGP UPDATE message to transmit/receive matches the MED value.

7.13.102 Set parameter for ORIGIN attribute

[Syntax]

match origin *ORIGIN*
no match origin [*ORIGIN*]

[Parameter]

ORIGIN	:	ORIGIN attribute value
	:	egp
	:	igp
	:	incomplete

[Initial value]

None

[Input mode]

Route map mode

[Description]

This sets the applicable parameters for BGP ORIGIN attributes in the route map entry.

If this command is executed with the "no" syntax, the applicable parameters for BGP ORIGIN attributes are deleted from the route map entry.

[Note]

For "permit" entries, the processing contents (set) will be executed if the MED attribute of the transmitted/received BGP UPDATE message matches the ORIGIN attribute value.

For "deny" entries, the processing contents (set) will not be executed if the MED attribute of the transmitted/received BGP UPDATE message matches the ORIGIN attribute value, and the next applicable parameter is processed.

7.13.103 Adding AGGREGATOR attributes

[Syntax]

set aggregator as *AS_NUM ROUTER-ID*
no set aggregator as [*AS_NUM*]

[Parameter]

AS_NUM : <1-4294967295>

AS number to which a BGP peer with aggregated routes belongs

AS_NUM : <X.X.X.X>

Router ID for a BGP peer with aggregated routes

[Initial value]

None

[Input mode]

Route map mode

[Description]

This sets the processing contents in the route map entry, to which the BGP AGGREGATOR attribute is added.

If this command is executed with the "no" syntax, this deletes the processing contents in the route map entry to which the BGP AGGREGATOR attribute is added.

[Note]

The AGGREGATOR attribute is granted to the BGP UPDATE message that matches the applicable conditions (match).

7.13.104 Adding to the start of the AS_PATH attribute

[Syntax]

set as-path prepend *AS_PATH* [*AS_PATH*...]
no set as-path prepend

[Parameter]

AS_PATH : <1-4294967295>

AS number

[Initial value]

None

[Input mode]

Route map mode

[Description]

This sets the processing contents in the route map entry, to which the BGP AS_PATH attribute is added.

If this command is executed with the "no" syntax, this deletes the processing contents in the route map entry to which the BGP AS_PATH attribute is added.

[Note]

The AS number specified by this command is added to the start of the AS_PATH attribute of the BGP UPDATE message that matches the applicable conditions (match).

7.13.105 Adding ATOMIC_AGGREGATE attributes

[Syntax]

set atomic-aggregator
no set atomic-aggregator

[Initial value]

None

[Input mode]

Route map mode

[Description]

This sets the processing contents in the route map entry, to which the BGP ATOMIC_AGGREGATOR attribute is added.

If this command is executed with the "no" syntax, this deletes the processing contents in the route map entry to which the BGP ATOMIC_AGGREGATOR attribute is added.

[Note]

The ATOMIC_AGGREGATOR attribute is granted to the BGP UPDATE message that matches the applicable conditions (match).

7.13.106 Delete COMMUNITIES attribute from a community

[Syntax]

set comm-list *LIST_NUM_STANDARD* **delete**
set comm-list *LIST_NUM_EXPAND* **delete**
no set comm-list delete *LIST_NUM_STANDARD* **delete**
no set comm-list delete *LIST_NUM_EXPAND* **delete**

[Parameter]

LIST_NUM_STANDARD	:	<1-99>
		Standard community list number
LIST_NUM_EXPAND	:	<100-500>
		Extended community list number

[Initial value]

None

[Input mode]

Route map mode

[Description]

This sets the processing contents for changing the BGP COMMUNITIES attributes in the route map entry.

If this command is executed with the "no" syntax, the processing contents for changing the BGP COMMUNITIES attributes are deleted from the route map entry.

[Note]

The command value specified by this command is deleted from the COMMUNITIES attribute of the BGP UPDATE message that matches the applicable conditions (match).

7.13.107 Rewriting and adding COMMUNITIES attributes

[Syntax]

set community *COMMUNITY* [*COMMUNITY...*] [*additive*]
set community *none*

no set community *COMMUNITY* [*COMMUNITY*...] [*additive*]
no set community *none*

[Parameter]

COMMUNITY : Community value

AA:NN : community value

Setting value	Description
AA	<1-65534> AS number
NN	<1-65534> Access list number for community values within the AS specified by AA

internet : Community value (0:0)

no-advertise : Well-known community value NO_ADVERTISE(65535:65282)

no-export : Well-known community value NO_EXPORT(65535:65281)

local-as : Well-known community value NO_EXPORT_SUBCONFED(65535:65283)

additive : Specified when adding a COMMUNITIES attribute. When omitted, the COMMUNITIES attribute is rewritten

none : Specified when deleting a COMMUNITIES attribute

[Initial value]

None

[Input mode]

Route map mode

[Description]

This sets the processing contents for adding or deleting the BGP COMMUNITIES attributes in the route map entry.

If this command is executed with the "no" syntax, the processing contents for adding or deleting the BGP COMMUNITIES attributes are deleted from the route map entry.

[Note]

The COMMUNITIES attributes are added or deleted from the BGP UPDATE message that matches the applicable conditions (match).

7.13.108 Rewrite settings for IPv4 next hop

[Syntax]

set ip next-hop *NEXTHOP*
no set ip next-hop [*NEXTHOP*]

[Parameter]

NEXTHOP : <A.B.C.D>

Next hop in IPv4 address format

[Initial value]

None

[Input mode]

Route map mode

[Description]

This sets the rewrite processing content for the BGP route's next hop in the route map entry.

If this command is executed with the "no" syntax, this deletes the rewrite processing content for the BGP route's next hop from the route map entry.

[Note]

Rewrites the next hop for the route of the BGP UPDATE message that matches the applicable parameters (match).

7.13.109 Rewrite settings for IPv6 next hop

[Syntax]

set ipv6 next-hop *NEXTHOP*
no set ipv6 next-hop [*NEXTHOP*]

[Parameter]

NEXTHOP : <X:X::X:X>

Next hop in IPv6 address format

[Initial value]

None

[Input mode]

Route map mode

[Description]

This sets the rewrite processing content for the BGP route's next hop in the route map entry.

If this command is executed with the "no" syntax, this deletes the rewrite processing content for the BGP route's next hop from the route map entry.

[Note]

Rewrites the next hop for the route of the BGP UPDATE message that matches the applicable parameters (match).

7.13.110 Rewrite LOCAL_PREF attribute value

[Syntax]

set local-preference *PREFERENCE*
no set local-preference [*PREFERENCE*]

[Parameter]

PREFERENCE : <0-4294967295>

LOCAL_PREF attribute value

[Initial value]

None

[Input mode]

Route map mode

[Description]

This sets the processing contents in the route map entry, to which the BGP LOCAL_PREF attribute is added.

If this command is executed with the "no" syntax, this deletes the processing contents in the route map entry to which the BGP LOCAL_PREF attribute is added.

[Note]

The LOCAL_PREF attribute is added to the BGP UPDATE message that matches the applicable conditions (match).

7.13.111 Rewrite settings for MULTI_EXIT_DISC(MED) attributes

[Syntax]

set metric [+/-]*METRIC*
no set metric [[+/-]*METRIC*]

[Parameter]

METRIC : <1-4294967295>

MULTI_EXIT_DISC(MED) attribute value

[Initial value]

None

[Input mode]

Route map mode

[Description]

This sets the processing contents in the route map entry, to which the BGP MULTI_EXIT_DISC(MED) attribute is added.

If this command is executed with the "no" syntax, this deletes the processing contents from the route map entry, to which the BGP MULTI_EXIT_DISC(MED) attribute is added.

[Note]

Adds the MULTI_EXIT_DISC(MED) attribute to the BGP UPDATE message that matches the applicable parameters (match).

When a METRIC value is specified with [+/-] added, the specified METRIC value is added or subtracted from the original MED value.

When the METRIC value is specified without adding the [+/-], the value is overwritten with the METRIC value that specifies the original MED value.

7.13.112 Adding ORIGIN attributes

[Syntax]

set origin *ORIGIN*
no set origin [*ORIGIN*]

[Parameter]

ORIGIN	:	ORIGIN attribute value
	:	egp
	:	igp
	:	incomplete

[Initial value]

None

[Input mode]

Route map mode

[Description]

This adds the ORIGIN attribute with the specified value to BGP route information matching the route map entry.

[Note]

The ORIGIN attribute is added to the BGP UPDATE message that matches the applicable conditions (match).

7.13.113 Adding ORIGINATOR_ID attributes

[Syntax]

set originator-id *ORING_ID*
no set originator-id [*ORING_ID*]

[Parameter]

ORING_ID	:	<A.B.C.D> ORIGINATOR_ID attribute (IPv4 address)

[Initial value]

None

[Input mode]

Route map mode

[Description]

This sets the processing contents in the route map entry, to which the BGP ORIGINATOR_ID attribute is added.

If this command is executed with the "no" syntax, this deletes the processing contents in the route map entry to which the BGP ORIGINATOR_ID attribute is added.

[Note]

The ORIGINATOR_ID attribute is added to the BGP UPDATE message that matches the applicable conditions (match).

7.13.114 Set route weight

[Syntax]

set weight *WEIGHT*
no set weight [*WEIGHT*]

[Parameter]

WEIGHT	:	<0-4294967295>
		Route weight

[Initial value]

None

[Input mode]

Route map mode

[Description]

This specifies how BGP route weights are applied in a route map entry.

If this command is executed with the "no" syntax, this deletes the processing content for weighting BGP routes from the route map entry.

[Note]

This assigns weights to the routes of the BGP UPDATE message that matches the applicable parameters (match).

7.13.115 Show the status of BGP next hop tracking

[Syntax]

show bgp nexthop-tracking

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

Shows the status of BGP next hop tracking

[Example]

```
SWX3220# show bgp nexthop-tracking
Configured NHT: ENABLED
NHT Delay time-interval : 5
BGP Instance: (Default), AS: 20000, router-id 192.168.100.240
NHT is Enabled
Recvd Msg count from RIB: 0
NHT delay-timer remaining seconds: 0
BGP nexthop(s):
Total number of IPV4 nexthops : 0
Total number of IPV6 nexthops : 0
```

7.13.116 Display the status of the BGP next hop tree

[Syntax]

show bgp nexthop-tree-detailed

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

This shows the BGP next hop tree information.

[Example]

```
SWX3220#show bgp nexthop-tree-details
BGP Instance: (Default), AS: 20000, router-id 192.168.100.240
AFI_IP Nexthop count : 0
AFI_IP6 Nexthop count : 0
```

7.13.117 Show AS_PATH access list

[Syntax]

show ip as-path-access-list [*AS_ACL_NUM*]

[Parameter]

AS_ACL_NUM : <1-100>

AS path access list number

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

This shows the AS path access list setting status.

[Example]

```
SWX3220#show ip as-path-access-list
AS path access list 100
    permit [65000-65010]
```

7.13.118 Show IPv4 prefix list

[Syntax]

show ip prefix-list [*PLIST_NUM* [*seq SEQ*]]
show ip prefix-list detail [*PLIST_NUM*]
show ip prefix-list summary [*PLIST_NUM*]

[Parameter]

PLIST_NUM : <1-100>

Prefix list number

SEQ : <1-4294967295>

Sequence number

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

Shows the prefix list setting status.

7.13.119 Show IPv6 prefix list

[Syntax]

show ipv6 prefix-list [*PLIST_NUM* [*seq SEQ*]]
show ipv6 prefix-list detail [*PLIST_NUM*]
show ipv6 prefix-list summary [*PLIST_NUM*]

[Parameter]

PLIST_NUM : <1-100>

Prefix list number

SEQ : <1-4294967295>

Sequence number

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

Shows the prefix list setting status.

7.13.120 Show IPv4 BGP routes

[Syntax]

show ip bgp [*DESTINATION*]
show ip bgp [*PREFIX* [*longer-prefixes*]]

[Keyword]

longer-prefixes	:	Shows all routes contained in destination prefixes specified by PREFIX.

[Parameter]

DESTINATION	:	A.B.C.D Destination IP address
PREFIX	:	A.B.C.D/M Destination prefix

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

This shows the BGP routing table.

When DESTINATION is specified, routes used in communicating to destination IP addresses are shown.

When PREFIX is specified, only routes that match the destination prefix are shown. When the "longer-prefixes" keyword is specified, all routes included in the destination prefix are shown.

[Example]

```
SWX3220#show ip bgp
BGP table version is 64, local router ID is 192.168.100.240
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, l -
labeled
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight   Path
*>i  1.1.1.0/24       192.168.100.101      0        100          0        ?
*>i  2.2.2.0/24       192.168.100.102      0        100          0        ?
*>   3.3.3.0/24       192.168.100.241      0        100          32768    ?
*>   4.4.4.0/24       192.168.100.242      0        100          32768    ?
*>i  22.22.22.0/24    192.168.200.111      0        100          0        ?
*>i  33.33.33.0/24    192.168.200.112      0        100          0        ?

Total number of prefixes 6
```

7.13.121 Show IPv6 BGP routes

[Syntax]

show ipv6 bgp [*DESTINATION*]
show ipv6 bgp [*PREFIX* [*longer-prefixes*]]

[Keyword]

longer-prefixes	:	Shows all routes contained in destination prefixes specified by PREFIX.

[Parameter]

DESTINATION	:	X:X::X:X Destination IP address
PREFIX	:	X:X::X:X/M Destination prefix

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

This shows the BGP routing table.

When DESTINATION is specified, routes used in communicating to destination IP addresses are shown.

When PREFIX is specified, only routes that match the destination prefix are shown. When the "longer-prefixes" keyword is specified, all routes included in the destination prefix are shown.

This cannot be executed if the stack is enabled.

7.13.122 Show IPv4 BGP routes permitted by a specific community name

[Syntax]

show ip bgp community [*COMMUNITY* [*COMMUNITY*...] [*exact-match*]]

[Keyword]

exact-match : Only routes that have communities that perfectly match the specified community are shown

[Parameter]

COMMUNITY : Community value

Setting value	Description
AA:NN	Specified community number (1-65535)
internet	Internet community (community number 0:0)
local-as	Well-known community NO_EXPORT_SUBCONFED(65535:65283)
no-advertise	Well-known community NO_ADVERTISE(65535:65282)
no-export	Well-known community NO_EXPORT(65535:65281)

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

Shows routes with the specified community value.

7.13.123 Show IPv6 BGP routes permitted by a specific community name

[Syntax]

show ipv6 bgp community [*COMMUNITY* [*COMMUNITY*...] [*exact-match*]]

[Keyword]

exact-match : Only routes that have communities that perfectly match the specified community are shown.

[Parameter]

COMMUNITY : Community value

Setting value	Description
AA:NN	Specified community number (1-65535)
internet	Internet community (community number 0:0)
local-as	Well-known community NO_EXPORT_SUBCONFED(65535:65283)
no-advertise	Well-known community NO_ADVERTISE(65535:65282)
no-export	Well-known community NO_EXPORT(65535:65281)

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

Shows routes with the specified community value.

This cannot be executed if the stack is enabled.

7.13.124 Show IPv4 BGP routes permitted by a specified community list

[Syntax]

show ip bgp community-list *COMMUNITY_LIST* [*exact-match*]

[Parameter]

COMMUNITY_LIST : Community list name

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

Show IPv4 BGP routes permitted by the specified community list name.

7.13.125 Show IPv6 BGP routes permitted by a specified community list

[Syntax]

show ipv6 bgp community-list *COMMUNITY_LIST* [*exact-match*]

[Parameter]

COMMUNITY_LIST : Community list name

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

Show IPv6 BGP routes permitted by the specified community list name.

7.13.126 Show IPv4 BGP routes permitted by a specific list

[Syntax]

show ip bgp filter-list *AS_PATH_LIST_NUM* [*exact-match*]

[Keyword]

exact-match : Only shows routes that perfectly match the conditions of the AS path access list

[Parameter]

AS_PATH_LIST_NUM : <1-100>

AS path access list number

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

This shows the information for routes that match the conditions of the AS path access list.

[Example]

```
SWX3220#show ip bgp filter-list 1
BGP table version is 47, local router ID is 192.168.100.240
Status codes: s suppressed, d damped, h history, * valid,
> best, i - internal, l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

     Network          Next Hop             Metric   LocPrf     Weight Path
*>   192.168.1.0/24   40.0.0.11            0        100        0       200 4001 ?

Total number of prefixes 1
```

7.13.127 Show IPv6 BGP routes permitted by a specific list

[Syntax]

show ipv6 bgp filter-list *AS_PATH_LIST_NUM* [*exact-match*]

[Keyword]

exact-match : Only shows routes that perfectly match the conditions of the AS path access list

[Parameter]

AS_PATH_LIST_NUM : <1-100>

AS path access list number

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

This shows the information for routes that match the conditions of the AS path access list.

[Example]

```
SWX3220#show ipv6 bgp filter-list 1
BGP table version is 10, local router ID is 192.168.100.240
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

     Network          Next Hop             Metric   LocPrf     Weight Path
*>i  100::/64         100::100(fe80::ae44:f2ff:fe84:efd1)
                                          0        100        0        200, 4001

Total number of prefixes 1
```

7.13.128 Show IPv4 routes to the same destination with different AS_PATH origins

[Syntax]

show ip bgp inconsistent-as

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

This shows routes to the same destination with different AS_PATH attribute origins.

7.13.129 Show IPv6 routes to the same destination with different AS_PATH origins

[Syntax]

show ipv6 bgp inconsistent-as

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

This shows routes to the same destination with different AS_PATH attribute origins.

This cannot be executed if the stack is enabled.

7.13.130 Show IPv4 BGP peers

[Syntax]

show ip bgp neighbors [*NEIGHBOR*]

[Parameter]

NEIGHBOR : Address value

Setting value	Description
A.B.C.D	IPv4 address of the BGP neighbor
X:X::X:X	IPv6 address of the BGP neighbor

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

Shows BGP neighbor information.

If the NEIGHBOR parameter is specified, this shows only the specified BGP neighbor.

Both "show ip bgp neighbors" and "show ipv6 bgp neighbors" result in equivalent output.

[Example]

```
SWX3220#show ip bgp neighbors 192.168.100.100
BGP neighbor is 192.168.100.100, remote AS 20000, local AS 20000, internal link
  BGP version 4, remote router ID 192.168.100.100
  BGP state = Established, up for 03:06:58
  Last read 03:06:58, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 441 messages, 0 notifications, 0 in queue
  Sent 377 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 193, neighbor version 193
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  Outbound path policy configured
  Outgoing update AS path filter list is *100
  2 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 192.168.100.240, Local port: 179
Foreign host: 192.168.100.100, Foreign port: 44114
Nexthop: 192.168.100.240
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
```

7.13.131 Show IPv6 BGP peers

[Syntax]

show ipv6 bgp neighbors [*NEIGHBOR*]

[Parameter]

NEIGHBOR : Address value

Setting value	Description
A.B.C.D	IPv4 address of the BGP neighbor
X:X::X:X	IPv6 address of the BGP neighbor

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

Shows BGP neighbor information.

If the NEIGHBOR parameter is specified, this shows only the specified BGP neighbor.

Both "show ip bgp neighbors" and "show ipv6 bgp neighbors" result in equivalent output.

This cannot be executed if the stack is enabled.

[Example]

```
SWX3220#show ipv6 bgp neighbors
BGP neighbor is 100::100, remote AS 65000, local AS 65000, internal link
  BGP version 4, remote router ID 192.168.100.250
  BGP state = Established, up for 00:00:16
  Last read 00:00:16, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    4-Octet ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
  Received 3 messages, 0 notifications, 0 in queue
  Sent 2 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds

 For address family: IPv4 Unicast
  BGP table version 5, neighbor version 5
  Index 2, Offset 0, Mask 0x4
  Community attribute sent to this neighbor (both)
  Outbound path policy configured
  Outgoing update AS path filter list is *2
  3 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 100::240, Local port: 57666
Foreign host: 100::100, Foreign port: 179
Nexthop: 192.168.100.240
Nexthop global: 100::240
Nexthop local: fe80::ae44:f2ff:fea2:8b52
BGP connection: shared network
```

7.13.132 Show routes advertised to IPv4 BGP peers

[Syntax]

show ip bgp neighbors *NEIGHBOR* **advertised-routes**

[Parameter]

NEIGHBOR : Address value

Setting value	Description
A.B.C.D	IPv4 address of the BGP neighbor
X:X::X:X	IPv6 address of the BGP neighbor

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

This shows the routes advertised to the BGP neighbor specified by the NEIGHBOR parameter.

[Example]

```
SWX3220#show ip bgp neighbors 192.168.100.100 advertised-routes
BGP table version is 197, local router ID is 192.168.100.240
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight  Path
*>i  3.3.3.0/24       192.168.100.241     0        100          32768    ?
*>i  4.4.4.0/24       192.168.100.242     0        100          32768    ?

Total number of prefixes 2
```

7.13.133 Show routes advertised to IPv6 BGP peers

[Syntax]

show ipv6 bgp neighbors *NEIGHBOR* **advertised-routes**

[Parameter]

NEIGHBOR : Address value

Setting value	Description
X:X::X:X	IPv6 address of the BGP neighbor

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

This shows the routes advertised to the BGP neighbor specified by the NEIGHBOR parameter.

This cannot be executed if the stack is enabled.

[Example]

```
SWX3220#show ipv6 bgp neighbors 100::100 advertised-routes
BGP table version is 14, local router ID is 192.168.100.240
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

     Network          Next Hop             Metric   LocPrf     Weight Path
*>i  100::/64         100::240(fe80::ae44:f2ff:fea2:8b52)
                                          0        100        32768    ?

Total number of prefixes 1
```

7.13.134 Show Hold time for BGP peers

[Syntax]

show ip bgp neighbors *NEIGHBOR* **hold-time**

[Parameter]

NEIGHBOR : Address value

Setting value	Description
A.B.C.D	IPv4 address of the BGP neighbor
X:X::X:X	IPv6 address of the BGP neighbor

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

This shows the Hold Time for the BGP neighbor specified in the NEIGHBOR parameter.

[Example]

```
SWX3220#show ip bgp neighbors 192.168.100.100 hold-time
 Hold time for this session is 90 seconds
```

7.13.135 Show number of inbound/outbound keepalive messages for a BGP peer

[Syntax]

show ip bgp neighbors *NEIGHBOR* **keepalive**

[Parameter]

NEIGHBOR : Address value

Setting value	Description
A.B.C.D	IPv4 address of the BGP neighbor
X:X::X:X	IPv6 address of the BGP neighbor

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

This shows information related to the number of keepalive messages sent/received with the BGP neighbor specified by the NEIGHBOR parameter.

[Example]

```
SWX3220#show ip bgp neighbors 192.168.100.100 keepalive
 Received 454 KEEPALIVE messages and Sent 389 KEEPALIVE messages
```

7.13.136 Keepalive transmission interval for BGP peers

[Syntax]

show ip bgp neighbors *NEIGHBOR* **keepalive-interval**

[Parameter]

NEIGHBOR : Address value

Setting value	Description
A.B.C.D	IPv4 address of the BGP neighbor
X:X::X:X	IPv6 address of the BGP neighbor

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

This shows the keepalive interval with the BGP neighbor specified by the NEIGHBOR parameter.

[Example]

```
SWX3220#show ip bgp neighbors 192.168.100.100 keepalive-interval
 Keepalive interval for this session is 30 seconds
```

7.13.137 Show number of inbound/outbound notification messages for a BGP peer

[Syntax]

show ip bgp neighbors *NEIGHBOR* **notification**

[Parameter]

NEIGHBOR : Address value

Setting value	Description
A.B.C.D	IPv4 address of the BGP neighbor
X:X::X:X	IPv6 address of the BGP neighbor

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

This shows the number of notification messages sent/received with the BGP neighbor specified by the NEIGHBOR parameter.

[Example]

```
SWX3220#show ip bgp neighbors 192.168.100.100 notification
 Received 0 Notification messages and Sent 0 Notification messages
```

7.13.138 Show number of open messages sent/received from a BGP peer

[Syntax]

show ip bgp neighbors *NEIGHBOR* **open**

[Parameter]

NEIGHBOR : Address value

Setting value	Description
A.B.C.D	IPv4 address of the BGP neighbor
X:X::X:X	IPv6 address of the BGP neighbor

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

This shows the number of open messages sent/received with the BGP neighbor specified by the NEIGHBOR parameter.

[Example]

```
SWX3220#show ip bgp neighbors 192.168.100.100 open
 Received 1 OPEN messages and Sent 1 OPEN messages
```

7.13.139 Show number of messages received from a BGP peer

[Syntax]

show ip bgp neighbors *NEIGHBOR* **rcvd-msgs**

[Parameter]

NEIGHBOR : Address value

Setting value	Description
A.B.C.D	IPv4 address of the BGP neighbor
X:X::X:X	IPv6 address of the BGP neighbor

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

This shows the total number of all BGP messages sent/received with the BGP neighbor specified by the NEIGHBOR parameter.

[Example]

```
SWX3220#show ip bgp neighbors 192.168.100.100 rcvd-msgs
  Received 489 messages
```

7.13.140 Show prefix filter information received from a BGP peer

[Syntax]

show ip bgp neighbors *NEIGHBOR* **received prefix-filter**

[Parameter]

NEIGHBOR : Address value

Setting value	Description
A.B.C.D	IPv4 address of the BGP neighbor
X:X::X:X	IPv6 address of the BGP neighbor

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

This shows the prefix filter for the ORF (outbound route filtering) information received from the BGP neighbor specified by the NEIGHBOR parameter.

7.13.141 Show all routes received from IPv4 BGP peers

[Syntax]

show ip bgp neighbors *NEIGHBOR* **received-routes**

[Parameter]

NEIGHBOR : Address value

Setting value	Description
A.B.C.D	IPv4 address of the BGP neighbor
X:X::X:X	IPv6 address of the BGP neighbor

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

This shows all routes received from the BGP neighbor specified by the NEIGHBOR parameter.

This includes the routes discarded by filters and so forth.

The "neighbor soft-reconfiguration inbound" command must be configured beforehand.

7.13.142 Show all routes received from IPv6 BGP peers

[Syntax]

show ipv6 bgp neighbors *NEIGHBOR* **received-routes**

[Parameter]

NEIGHBOR : Address value

Setting value	Description
X:X::X:X	IPv6 address of the BGP neighbor

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

This shows all routes received from the BGP neighbor specified by the NEIGHBOR parameter.

This includes the routes discarded by filters and so forth.

The "neighbor soft-reconfiguration inbound" command must be configured beforehand.

This cannot be executed if the stack is enabled.

[Example]

```
SWX3220#show ipv6 bgp neighbors 100::100 received-routes
BGP table version is 10, local router ID is 192.168.100.240
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

     Network          Next Hop             Metric   LocPrf     Weight Path
*>i  100::/64         100::100(fe80::ae44:f2ff:fe84:efd1)
```

```
                                          0        100        0        ?
*>i  200::/64         100::100(fe80::ae44:f2ff:fe84:efd1)
                                          0        100        0        ?
*>i  300::/64         100::100(fe80::ae44:f2ff:fe84:efd1)
                                          0        100        0        ?

Total number of prefixes 3
```

7.13.143 Show all routes received from IPv4 BGP peers and filtered

[Syntax]

show ip bgp neighbors *NEIGHBOR* **routes**

[Parameter]

NEIGHBOR : Address value

Setting value	Description
A.B.C.D	IPv4 address of the BGP neighbor
X:X::X:X	IPv6 address of the BGP neighbor

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

This shows routes received from the BGP neighbor specified by the NEIGHBOR parameter.

Routes discarded by filters and so forth are not included.

[Example]

```
SWX3220#show ip bgp neighbors 192.168.100.100 routes
BGP table version is 227, local router ID is 192.168.100.240
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, l -
labeled
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric     LocPrf       Weight    Path
*>i  1.1.1.0/24       192.168.100.101      0         100          0         ?
*>i  2.2.2.0/24       192.168.100.102      0         100          0         ?

Total number of prefixes 2
```

7.13.144 Show all routes received from IPv6 BGP peers and filtered

[Syntax]

show ipv6 bgp neighbors *NEIGHBOR* **routes**

[Parameter]

NEIGHBOR : Address value

Setting value	Description
X:X::X:X	IPv6 address of the BGP neighbor

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

This shows routes received from the BGP neighbor specified by the NEIGHBOR parameter.

Routes discarded by filters and so forth are not included.

This cannot be executed if the stack is enabled.

[Example]

```
SWX3220#show ipv6 bgp neighbors 100::100 routes
BGP table version is 6, local router ID is 192.168.100.240
Status codes: s suppressed, d damped, h history, * valid,
```

```
              > best, i - internal, l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

     Network          Next Hop             Metric   LocPrf     Weight Path
*>i  100::/64         100::100(fe80::ae44:f2ff:fe84:efd1)
                                           0        100        0        ?
*>i  200::/64         100::100(fe80::ae44:f2ff:fe84:efd1)
                                           0        100        0        ?
*>i  300::/64         100::100(fe80::ae44:f2ff:fe84:efd1)
                                           0        100        0        ?

Total number of prefixes 3
```

7.13.145 Show number of messages transmitted to a BGP peer

[Syntax]

show ip bgp neighbors *NEIGHBOR* **sent-msgs**

[Parameter]

NEIGHBOR : Address value

Setting value	Description
A.B.C.D	IPv4 address of the BGP neighbor
X:X::X:X	IPv6 address of the BGP neighbor

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

This shows the number of BGP messages sent to the BGP neighbor specified by the NEIGHBOR parameter.

[Example]

```
SWX3220#show ip bgp neighbors 192.168.100.100 sent-msgs
  Sent 448 messages
```

7.13.146 Show number of UPDATE messages sent/received from a BGP peer

[Syntax]

show ip bgp neighbors *NEIGHBOR* **update**

[Parameter]

NEIGHBOR : Address value

Setting value	Description
A.B.C.D	IPv4 address of the BGP neighbor
X:X::X:X	IPv6 address of the BGP neighbor

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

This shows the number of UPDATE messages sent/received with the BGP neighbor specified by the NEIGHBOR parameter.

[Example]

```
SWX3220#show ip bgp neighbors 192.168.100.100 update
 Received 2 UPDATE messages and Sent 2 UPDATE messages
```

7.13.147 Show BGP scan status

[Syntax]

show ip bgp scan

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

This shows information related to the BGP scan.

[Example]

```
SWX3220#show ip bgp scan
BGP Instance: (Default) AS 20000, router-id 192.168.100.240
BGP scan interval is 60
scan remain-time: 22
Current BGP nexthop cache:
 192.168.100.101 valid [IGP metric 0]
 192.168.100.102 valid [IGP metric 0]
 192.168.200.111 valid [IGP metric 0]
 192.168.200.112 valid [IGP metric 0]
```

7.13.148 Show IPv4 BGP peer summary

[Syntax]

show ip bgp summary

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

Show a summary of information for the IPv4 BGP peer.

[Example]

```
SWX3220#show ip bgp summary
BGP router identifier 192.168.100.240, local AS number 20000
BGP table version is 235
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down
State/PfxRcd
192.168.100.100          4 20000  537        461     235      0      0
03:48:34            2
192.168.200.100          4 20000  464        467     235      0      0
03:48:02            2

Total number of neighbors 2

Total number of Established sessions 2
```

7.13.149 Show IPv6 BGP peer summary

[Syntax]

show ipv6 bgp summary

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

Show a summary of information for the IPv6 BGP peer.

This cannot be executed if the stack is enabled.

[Example]

```
SWX3220#show ipv6 bgp summary
BGP router identifier 192.168.100.240, local AS number 65000
BGP table version is 5
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down
State/PfxRcd
100::100                 4 65000   51         41       5      0      0
00:00:40               3

Total number of neighbors 1

Total number of Established sessions 1
```

7.13.150 Update the session targeting the IPv4 BGP peer

[Syntax]

clear ip bgp *TARGET* [*DIRECTION* [*prefix-filter*]]

[Keyword]

prefix-filter : <1-100> prefix list numbers

[Parameter]

TARGET : BGP peer operations

TARGET	Description
*	Applies to connections with all BGP peers
<1-4294967295>	Applies to connections with BGP peers having the specified AS number
A.B.C.D	IPv4 address of the BGP neighbor
X:X::X:X	Applies to connections with the specified IPv6 BGP peer
external	Applies to connections with all eBGP peers
peer-group GROUP	Applies to connections with BGP peer groups with the group name specified by the "neighbor peer-group" command

DIRECTION : Reset operations

Setting value	Description
soft	Resets both the routes received from the specified TARGET and the routes sent to the TARGET.
soft in	Resets the route received from the specified TARGET.
soft out	Resets the route sent to the specified TARGET.

GROUP : BGP peer group name

[Input mode]

privileged EXEC mode

[Description]

This resets the connection with the target specified by TARGET.

If the DIRECTION option has not been specified, disconnect the BGP session with the target, and start from reconnection.

If the DIRECTION option has been specified, delete the route information while maintaining the BGP session with the target, and update the route information by exchanging routes again.

The prefix-filter option can only be specified when DIRECTION is set to "soft in". The prefix filter information is advertised to the BGP peer while maintaining the BGP session, and retransmission of the route to which the prefix filter is applied is requested.

X:X::X:X cannot be specified as the TARGET if the stack is enabled.

[Example]

This resets the route received from the BGP peer with the specified IPv4 address.

```
SWX3220#clear ip bgp 192.168.100.240 soft in
```

7.13.151 Update the session targeting the IPv6 BGP peer

[Syntax]

clear ipv6 bgp *TARGET* [*DIRECTION* [*prefix-filter*]]

[Keyword]

prefix-filter : <1-100> prefix list numbers

[Parameter]

TARGET : BGP peer operations

TARGET	Description
*	Applies to connections with all BGP peers
<1-4294967295>	Applies to connections with BGP peers having the specified AS number
X:X::X:X	Applies to connections with the specified IPv6 BGP peer
external	Applies to connections with all eBGP peers
peer-group GROUP	Applies to connections with BGP peer groups with the group name specified by the "neighbor peer-group" command

DIRECTION : Reset operations

Setting value	Description
soft	Resets both the routes received from the specified TARGET and the routes sent to the TARGET.
soft in	Resets the route received from the specified TARGET.
soft out	Resets the route sent to the specified TARGET.

GROUP : BGP peer group name

[Input mode]

privileged EXEC mode

[Description]

This resets the connection with the target specified by TARGET.

If the DIRECTION option has not been specified, disconnect the BGP session with the target, and start from reconnection.

If the DIRECTION option has been specified, delete the route information while maintaining the BGP session with the target, and update the route information by exchanging routes again.

The prefix-filter option can only be specified when DIRECTION is set to "soft in". The prefix filter information is advertised to the BGP peer while maintaining the BGP session, and retransmission of the route to which the prefix filter is applied is requested.

This cannot be executed if the stack is enabled.

[Example]

This resets the route received from the BGP peer with the specified IPv6 address.

```
SWX3220#clear ipv6 bgp 1000::1 soft in
```

7.13.152 Clear IPv4 prefix list statistical information

[Syntax]

clear ip prefix-list [*PLIST_NUM* [*PREFIX*]]

[Parameter]

PLIST_NUM : <1-100>

Prefix list number

PREFIX : <A.B.C.D/M>

Prefix

[Input mode]

privileged EXEC mode

[Description]

This clears the statistical information for the prefix list.

When PREFIX is specified, this clears only the statistical information from the prefix list with the specified prefix.

[Example]

This deletes the statistical information of the prefix list whose number is 1, and whose IPv4 address is 192.168.100.240/24.

```
SWX3220#clear ip prefix-list 1 192.168.100.240/26
```

7.13.153 Clear IPv6 prefix list statistical information

[Syntax]

clear ipv6 prefix-list [*PLIST_NUM* [*PREFIX*]]

[Parameter]

PLIST_NUM : <1-100>

Prefix list number

PREFIX : <X:X::X:X/M>

Prefix

[Input mode]

privileged EXEC mode

[Description]

This clears the statistical information for the prefix list.

When PREFIX is specified, this clears only the statistical information from the prefix list with the specified prefix.

[Example]

This deletes the statistical information of the prefix list whose number is 1, and whose IPv6 address is 1000::1/64.

```
SWX3220#clear ipv6 prefix-list 1 1000::1/64
```

7.13.154 Output the BGP log

[Syntax]

bgp log *LOG_TYPE* [*DIRECTION*]
no bgp log [*LOG_TYPE*] [*DIRECTION*]

[Parameter]

LOG_TYPE : Operations when outputting the log

Setting value	Description
filters	Outputs the log related to route filtering.
keepalives	Outputs the log related to keepalive.
nht	Outputs the log related to next hop tracking.
out	Outputs the log related to the UPDATE messages that are transmitted/received.

DIRECTION : Operations when transmitting/receiving

Setting value	Description
in	Sets the received UPDATE messages as the target.
out	Sets the transmitted UPDATE messages as the target.

[Initial value]

no bgp log

[Input mode]

global configuration mode

[Description]

Outputs the log related to each element of the BGP.

The DIRECTION parameter can only be specified when LOG_TYPE is "updates".

[Example]

This specifies that the route filtering-related log should be output.

```
SWX3220(config)#bgp log filters
```

7.14 OSPF

7.14.1 Move to OSPFv2 mode (IPv4)

[Syntax]

router ospf [*process_id*]
no router ospf [*process_id*]

[Parameter]

process_id	:	<0-65535> OSPF process ID

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Transition to OSPFv2 mode and make OSPF-related settings.

If using multiple OSPF processes, specify *process_id*. However, the use of multiple OSPF processes is not supported.

[Note]

If this command is executed with the "no" syntax, all settings of the specified OSPF process are deleted.

To move from OSPFv2 mode to global configuration mode, use the **exit** command.

[Example]

```
SWX3220(config)# router ospf
SWX3220(config-router)#
SWX3220(config-router)# exit
SWX3220(config)#
```

7.14.2 Move to OSPFv3 mode (IPv6)

[Syntax]

router ipv6 ospf [*name*]
no router ipv6 ospf [*name*]

[Parameter]

name	:	OSPFv3 process ID

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Transition to OSPFv3 mode and make OSPF-related settings.

If using multiple OSPF processes, specify *name*. However, the use of multiple OSPF processes is not supported.

[Note]

If this command is executed with the "no" syntax, all settings of the specified OSPFv3 process are deleted.

To move from OSPFv3 mode to global configuration mode, use the **no router ospf** or **exit** command.

This command cannot be used if the stack function is enabled.

[Example]

```
SWX3220(config)# router ipv6 ospf
SWX3220(config-router)#
SWX3220(config-router)# exit
SWX3220(config)#
```

7.14.3 Set authentication for an OSPF area

[Syntax]

area *area_id* **authentication** [**message-digest**]
no area *area_id* **authentication**

[Keyword]

message-digest : Use MD5 digest authentication

[Parameter]

area_id : Area ID

Setting value	Description
A.B.C.D	OSPF area ID in IPv4 address format
<0-4294967295>	OSPF area ID in four-octet integer format

[Initial value]

none

[Input mode]

OSPFv2 mode

[Description]

Enables authentication in the OSPF area.

If "message-digest" is not specified, simple password authentication is used. In this case, the authentication key is specified for each interface by the **ip ospf authentication-key** command.

If "message-digest" is specified, MD5 digest authentication is used. In this case, the authentication key is specified for each interface by the **ip ospf message-digest-key** command.

This command applies to all interfaces. To enable/disable authentication for an individual interface, use the **ip ospf authentication** command.

[Example]

Enable simple password authentication in the OSPF backbone area.

Specify "yamaha" as the authentication key for the VLAN #1 interface.

```
SWX3220(config-router)# area 0.0.0.0 authentication
SWX3220(config-router)# exit
SWX3220(config)# interface vlan1
SWX3220(config-if)# ip ospf authentication-key yamaha
```

Enable MD5 digest authentication in OSPF area 1.

Specify "yamaha" as the authentication key for the VLAN #10 interface.

```
SWX3220(config-router)# area 1 authentication message-digest
SWX3220(config-router)# exit
```

```
SWX3220(config)# interface vlan10
SWX3220(config-if)# ip ospf message-digest-key 1 md5 yamaha
```

7.14.4 Set metric value for default route (OSPFv2)

[Syntax]

area *area_id* **default-cost** *metric*
no area *area_id* **default-cost**

[Parameter]

area_id : Area ID

Setting value	Description
A.B.C.D	OSPF area ID in IPv4 address format
<0-4294967295>	OSPF area ID in four-octet integer format

metric : <0-16777215>

Metric value of default route advertised to NSSA or stub area

[Initial value]

area *area_id* default-cost 1

[Input mode]

OSPFv2 mode

[Description]

Sets the metric value of the default route that is advertised to an NSSA or stub area.

This is enabled only for the ABR of an NSSA or stub area.

[Example]

With area 1 as a stub area, specify the default route's metric value as 10.

```
SWX3220(config-router)# area 1 stub no-summary
SWX3220(config-router)# area 1 default-cost 10
```

7.14.5 Set filtering for route information advertised between areas

[Syntax]

area *area_id* **filter-list access** *access_list_id direction*
no area *area_id* **filter-list access** *access_list_id direction*

[Parameter]

area_id : Area ID

Setting value	Description
A.B.C.D	OSPF area ID in IPv4 address format
<0-4294967295>	OSPF area ID in four-octet integer format

access_list_id : Access list number specified by the "access-list" command

direction : Direction of the route advertisement to which the filter applies

Setting value	Description
in	Filter the route information that is advertised to the area specified by this command from another area
out	Filter the route information that is advertised from the area specified by this command to another area

[Initial value]

none

[Input mode]

OSPFv2 mode

[Description]

Sets filtering for route information advertised between areas.

This is valid only for an ABR.

[Example]

Using an access list, prevent all route information other than 203.0.113.0/24 from being advertised to area 1.

```
SWX3220(config)# access-list 1 deny 203.0.113.0 0.0.0.255
SWX3220(config)# access-list 1 permit any
SWX3220(config)# router ospf
SWX3220(config-router)# area 1 filter-list access 1 in
```

7.14.6 Set area as NSSA (OSPFv2)

[Syntax]

area *area_id* **nssa** [*option* [*option* ...]]
no area *area_id* **nssa** [*option* [*option* ...]]

[Parameter]

area_id : Area ID

Setting value	Description
A.B.C.D	OSPF area ID in IPv4 address format
<0-4294967295>	OSPF area ID in four-octet integer format

option : Option (Valid only for the ABR of the applicable NSSA)

Setting value	Description
default-information-originate [metric <0-16777214>] [metric-type <1-2>]	Notifies the applicable NSSA of the default route LSA (type 7). Use the "metric" option to specify the metric value of the default route's LSA (type 7). If omitted, this is 1. Use the "metric-type" option to specify the metric type. If omitted, this is 2.
no-redistribution	Route information of other areas is not provided to the applicable NSSA.
no-summary	Route information of other areas is not provided to the applicable NSSA.
stability-interval <0-2147483647>	Specifies the time (seconds) to continue LSA (type 7) notification to the applicable NSSA. This is used when transitioning the NSSA's translator to another device; by using this setting to inform the applicable NSSA of the external route via LSA (type 7), this setting minimizes unnecessary LSDB updates, and allows the translator to transition in a more stable manner.
translator-role *role*	Specifies the operation of the applicable NSSA as an ABR. If *role* is specified as "always", LSA (type 7) is always converted to LSA (type 5). If *role* is specified as "candidate", LSA (type 7) is converted to LSA (type 5) only if this is the applicable NSSA's translator. If *role* is specified as "never", LSA (type 7) is not converted. If *role* is omitted, this will be "candidate".

[Initial value]

none

[Input mode]

OSPFv2 mode

[Description]

Sets the specified area as an NSSA.

If the "no" syntax is used with a specified option, the specified option can be disabled.

[Example]

Set area 1 as an NSSA.

```
SWX3220(config-router)# area 1 nssa
```

7.14.7 Summarize route information of a specified network address region, and advertise to other areas (OSPFv2)

[Syntax]

area *area_id* **range** *range* [*type*]
no area *area_id* **range** *range* [*type*]

[Parameter]

area_id : Area ID

Setting value	Description
A.B.C.D	OSPF area ID in IPv4 address format
<0-4294967295>	OSPF area ID in four-octet integer format

range : Summary destination network address

Setting value	Description
A.B.C.D/M	Network range in IPv4 address format
A.B.C.D W.X.Y.Z	Network range in IP address and subnet mask format

type : Advertise route information

Setting value	Description
advertise	The summarized route information is advertised to other areas.
not-advertise	Route information of the specified network address region is not advertised to other areas.

[Initial value]

none

[Input mode]

OSPFv2 mode

[Description]

Of the route information within the applicable area, summarizes the route information within the specified network address region, and advertises it to other areas.

This is valid only for an ABR.

If *type* is omitted, it is considered that "advertise" is set.

[Example]

The route information of the area 1 region 203.0.113.0/24 is summarized in 203.0.113.0/24 and advertised to other areas.

```
SWX3220(config-router)# area 1 range 203.0.113.0/24
```

7.14.8 Set area as stub area (OSPFv2)

[Syntax]

area *area_id* **stub** [**no-summary**]
no area *area_id* **stub** [**no-summary**]

[Keyword]

no-summary : Route information to other areas is not advertised to the applicable stub area (specify as a totally stubby area).

[Parameter]

area_id : Area ID

Setting value	Description
A.B.C.D	OSPF area ID in IPv4 address format
<0-4294967295>	OSPF area ID in four-octet integer format

[Initial value]

none

[Input mode]

OSPFv2 mode

[Description]

Sets the specified area as a stub area.

If the "no" syntax is used with a specified option, the specified option can be disabled.

[Example]

Set area 1 as a stub area.

```
SWX3220(config-router)# area 1 stub
```

Set area 1 as a totally stubby area.

```
SWX3220(config-router)# area 1 stub no-summary
```

7.14.9 Specify virtual link on area (OSPFv2)

[Syntax]

area *area_id* **virtual-link** *router_id* [*option* [*option* ...]]
no area *area* **id virtual-link** *router_id* [*option* [*option* ...]]

[Parameter]

area_id : Area ID

Setting value	Description
A.B.C.D	OSPF area ID in IPv4 address format
<0-4294967295>	OSPF area ID in four-octet integer format

router_id : Router ID (A.B.C.D) of the ABR that is the other end of the virtual link

option : Option

Setting value	Description
authentication [*type*]	Enables authentication for the virtual link. If *type* is not specified, authentication is performed using the simple password specified by the "authentication-key" option. If *type* is specified as "message-digest", authentication is performed using the MD5 digest authentication key specified by the "message-digest-key" option. If *type* is specified as "null", authentication is not performed on the virtual link.
authentication-key *string*	Specify the simple password as eight characters or fewer. Specify this parameter at the end of the command line.
message-digest-key <1-255> md5 *string*	Specify the MD5 digest authentication key as 16 characters or fewer. Specify this parameter at the end of the command line.
dead-interval <1-65535>	Specify the wait time from when Hello packets stop being received from the ABR that is the other end of the virtual link until a down state is determined. If omitted, this is 40.
hello-interval <1-65535>	Specify the interval at which Hello packets are transmitted to the ABR that is the other end of the virtual link. If omitted, this is 10.
retransmit-interval <1-3600>	Specifies the OSPF packet retransmission interval. If omitted, this is 5.
transmit-delay <1-3600>	Specifies the OSPF packet transmission delay time. If omitted, this is 1.

[Initial value]

none

[Input mode]

OSPFv2 mode

[Description]

Specifies a virtual link on the specified area.

If the "no" syntax is used with a specified option, the specified option can be disabled.

This command must also be used to specify a virtual link on the ABR that is the other end of the virtual link, and the options must be the same.

[Example]

On area 1, specify a virtual link with ABR (203.0.113.1).

```
SWX3220(config-router)# area 1 virtual-link 203.0.113.1
```

7.14.10 Set bandwidth of interface (OSPFv2)

[Syntax]

auto-cost reference-bandwidth *bandwidth*
no auto-cost reference-bandwidth *bandwidth*

[Parameter]

bandwidth : <1-4294967>

Bandwidth (Mbps)

[Initial value]

auto-cost reference-bandwidth 100

[Input mode]

OSPFv2 mode

[Description]

Specifies the bandwidth value used when calculating the default metric value of the interface.

[Example]

Calculate the default metric value with 100 Mbps as the bandwidth of the interface.

```
SWX3220(config-router)# auto-cost reference-bandwidth 100
```

7.14.11 Set Opaque-LSA

[Syntax]

capability opaque *mode*
no capability opaque

[Parameter]

mode : Opaque-LSA

Setting value	Description
enable	Enable the Opaque-LSA.
disable	Disable the Opaque-LSA.

[Initial value]

capability opaque enable

[Input mode]

OSPFv2 mode

[Description]

Enables the Opaque-LSA.

7.14.12 Set method for calculating the summary route metric

[Syntax]

compatible rfc1583
no compatible rfc1583

[Initial value]

no compatible rfc1583

[Input mode]

OSPFv2 mode

[Description]

Sets the method for calculating the metric of a route summarized as an ABR.

This is valid only for an ABR.

If this command is not specified, metric calculation is performed as specified by RFC2328.

7.14.13 Set LSDB summary list optimization (OSPFv2)

[Syntax]

db-summary-opt *mode*
no db-summary-opt

[Parameter]

mode : Mode

Setting value	Description
enable	Enables optimization of the LSDB summary list.
disable	Disables optimization of the LSDB summary list.

[Initial value]

mode : disable

[Input mode]

OSPFv2 mode

[Description]

Enables optimization of the LSDB summary list.

When this function is enabled, if the LSA in the LSDB summary list is the same or newer when compared to the LSA included in the DD (Database Description) packet received from the neighbor, then that LSA is deleted from the LSDB summary list, thereby optimizing exchange of database information.

7.14.14 Set default external route (OSPFv2)

[Syntax]

default-information originate [*option* [*option* ...]]
no default-information originate [*option* [*option* ...]]

[Parameter]

option : Option

Setting value	Description
always	Notify default route information even if no default route information is held. If this is omitted, default external route information is advertised only if default route information is held.
metric <0-16777214>	Specifies the metric value used when advertising default external route information to the OSPF routing domain. If omitted, this is 10.
metric-type <1-2>	Specifies the metric type of the default external route information. If omitted, this is 2.

[Initial value]

none

[Input mode]

OSPFv2 mode

[Description]

This specifies whether the default external route is advertised to the OSPF routing domain.

This is valid only for an ASBR.

If the "no" syntax is used with a specified option, the specified option can be disabled.

[Example]

Always advertise the default external route to the OSPF routing domain with a metric value of 10 and a metric type of 1.

```
SWX3220(config-router)# default-information originate always metric 10 metric-type 1
```

7.14.15 Set metric value when advertising to OSPF routing domain (OSPFv2)

[Syntax]

default-metric *metric*

no default-metric

[Parameter]

metric : <1-16777214>

Default metric value

[Initial value]

none

[Input mode]

OSPFv2 mode

[Description]

Specifies the metric value used when advertising external route information to the OSPF routing domain.

This is used in conjunction with the **redistribute** command.

7.14.16 Set priority of route taken from OSPF into FIB (OSPFv2)

[Syntax]

distance *priority*
distance ospf [*option* [*option*]]
no distance
no distance ospf

[Parameter]

priority : <1-255>

Priority of route taken from OSPF into FIB

option : Option

Setting value	Description
intra-area <1-255>	Priority of route information within the area
inter-area <1-255>	Priority of route information between areas
external <1-255>	Priority of external routing information

[Initial value]

priority : 110

[Input mode]

OSPFv2 mode

[Description]

Sets priority of route taken from OSPF into FIB.

If *priority* is specified, it is handled as the priority for all routing information.

[Example]

Set 200 as the priority of route taken from OSPF into FIB.

```
SWX3220(config-router)# distance 200
```

As the priority of the route taken from OSPF into the FIB, set route information within the area as priority 100, route information between areas as priority 120, and external route information as priority 140.

```
SWX3220(config-router)# distance ospf intra-area 100 inter-area 120 external 140
```

7.14.17 Set filtering for route information between RIB and OSPF routing table (OSPFv2)

[Syntax]

distribute-list *access_list_id* **out** *kind*
distribute-list *access_list_id* **in**
no distribute-list *access_list_id* **out** [*kind*]

no distribute-list *access_list_id* **in**

[Parameter]

access_list_id : Access list number specified by the access-list command

kind : Type of route

Setting value	Description
connected	Applies to direct routes.
ospf [*process_id*]	Applies to route information held by OSPF.
rip	Applies to route information held by RIP.
static	Applies to static route information.

process_id : <0-65535> OSPF process ID (This can be used only if "ospf" is specified for "kind")

[Initial value]

none

[Input mode]

OSPFv2 mode

[Description]

Sets filtering for route information between the RIB (Routing Information Base) and the OSPF routing table.

This is valid only for an ASBR.

[Example]

Of the statically specified routes, the route 203.0.113.0/24 is not installed from the RIB into the OSPF routing table.

```
SWX3220(config)# access-list 1 deny 203.0.113.0/24
SWX3220(config)# access-list 1 permit any
SWX3220(config)# router ospf
SWX3220(config-router)# distribute-list 1 out static
```

The 203.0.113.0/24 route obtained from OSFP is not installed into the RIB.

```
SWX3220(config)# access-list 1 deny 203.0.113.0/24
SWX3220(config)# access-list 1 permit any
SWX3220(config)# router ospf
SWX3220(config-router)# distribute-list 1 in
```

7.14.18 Set stub host route (OSPFv2)

[Syntax]

host *host* **area** *area_id* [**cost** *cost*]
no host *host* **area** *area_id* [**cost** *cost*]

[Parameter]

host : A.B.C.D

IP address of host

area_id : Area ID

Setting value	Description
A.B.C.D	OSPF area ID in IPv4 address format
<0-4294967295>	OSPF area ID in four-octet integer format

cost : <0-65535>

Cost value

[Initial value]

none

[Input mode]

OSPFv2 mode

[Description]

For the specified area, advertises the specified IP address as the stub host route.

[Example]

Advertise 203.0.113.1 to area 1 as the stub host route.

```
SWX3220(config-router)# host 203.0.113.1 area 1
```

7.14.19 Set number of concurrent DD exchange processes (OSPFv2)

[Syntax]

max-concurrent-dd *dd_num*
no max-concurrent-dd [*dd_num*]

[Parameter]

dd_num : <1-65535>

Number of concurrent DD exchange processes

[Initial value]

max-concurrent-dd 5

[Input mode]

OSPFv2 mode

[Description]

Sets the number of DD exchange processes that can occur concurrently.

At the maximum, DD exchange can be performed for the specified number of neighbors that are in the Exchange state.

7.14.20 Associate areas with interface running OSPF

[Syntax]

network *network* **area** *area_id*

[Parameter]

network : Network range. OSPF runs on the interface to which the specified IP address range is assigned. The input format is as follows.

Setting value	Description
A.B.C.D/M	IPv4 address with specified subnet mask length
A.B.C.D E.F.G.H	IPv4 address (A.B.C.D) with wildcard bits (E.F.G.H)

area_id : Area ID

Setting value	Description
A.B.C.D	OSPF area ID in IPv4 address format
<0-4294967295>	OSPF area ID in four-octet integer format

[Initial value]

none

[Input mode]

OSPFv2 mode

[Description]

Associates areas with an interface running OSPF. OSPF runs on the interface to which is assigned the IP address included in the network range specified by *network,* and is associated with the area specified by *area_id*.

[Example]

Associate the 203.0.113.0/24 network connected to the VLAN #1 interface with the backbone area, and associate network 172.16.0.0/16 connected to the VLAN #2 interface with area 1.

```
SWX3220(config)# interface vlan1
SWX3220(config-if)# ip address 203.0.113.1/24
SWX3220(config-if)# exit
SWX3220(config)# interface vlan2
SWX3220(config-if)# ip address 172.16.0.1/16
SWX3220(config-if)# exit
SWX3220(config)# router ospf
SWX3220(config-router)# network 203.0.113.0/24 area 0
SWX3220(config-router)# network 172.16.0.0/16 area 1
```

7.14.21 Set OSPF router ID

[Syntax]

ospf router-id *router_id*
router-id *router_id*
no ospf router-id
no router-id [*router_id*]

[Parameter]

router_id : Router ID (IPv4 format IP address)

[Initial value]

none

[Input mode]

OSPFv2 mode

[Description]

Sets the OSPF router ID.

Although several ways to specify the OSPF router ID are provided, the decision is based on the following priority order.

1. Value set by the **router-id** command or the **ospf router-id** command entered in OSPFv2 mode
2. Value set by the **router-id** command entered in global configuration mode
3. Highest IP address of those specified for the VLAN interface

[Note]

If the router ID is changed, the changed router ID takes effect when this unit is restarted or when the OSPF process is restarted.

7.14.22 Set upper limit of link status advertisements handled by OSPF process

[Syntax]

overflow database *lsa_num* [*action*]
no overflow database

[Parameter]

lsa_num : <0-4294967294>

Upper limit of link status advertisements

action : Operation when the number of link status advertisements exceeds the setting. If omitted, "hard" is used.

Setting value	Description
hard	Shut down the OSPF process
soft	Output a warning message

[Initial value]

lsa_num : None (No upper limit)

[Input mode]

OSPFv2 mode

[Description]

Sets the upper limit for the link status advertisements that can be handled by the OSPF process.

If an upper limit is specified, the operation specified by *action* is executed when the number of link status advertisements reaches the upper limit.

7.14.23 Set upper limit of receivable AS external LSA

[Syntax]

overflow database external *lsa_num time*
no_overflow database external

[Parameter]

lsa_num	:	<0-2147483647>
		Upper limit of AS external LSA
time	:	<0-65535>
		Time until recovery from overflow condition (seconds)

[Initial value]

none

[Input mode]

OSPFv2 mode

[Description]

c

If *time* is set as 0, do not recover automatically.

7.14.24 Set OSPF passive interface (OSPFv2)

[Syntax]

passive-interface [*interface* [**disable**]]
no passive-interface [*interface* [**disable**]]

[Parameter]

interface	:	Interface name

[Initial value]

none

[Input mode]

OSPFv2 mode

[Description]

Sets the OSPF passive interface.

If *interface* is not specified, all interfaces will no longer send OSPF Hello messages.

If *interface* is specified, that interface will no longer send OSPF Hello messages. However, information of the network connected to the passive interface is subject to OSPF processing.

[Example]

On the OSPF router connected to the three networks 172.16.1.0/24 (VLAN #1), 172.16.2.0/24 (VLAN #2), and 172.16.3.0/24 (VLAN #3), associate these networks with the backbone area, but for network 172.16.3.0/24 on the VLAN #3 interface load only the routing information without running OSPF.

```
SWX3220(config-router)# network 172.16.0.0/16 area 0
SWX3220(config-router)# passive-interface vlan3
```

7.14.25 Advertise the specified external route information to the OSPF area as an AS external LSA (OSPFv2)

[Syntax]

redistribute *kind* [*option* [*option* ...]]
no redistribute *kind* [*option* [*option* ...]]

[Parameter]

kind : >Type of route

Setting value	Description
connected	Applies to direct routes.
ospf [*process_id*]	Applies to route information held by OSPF.
rip	Applies to route information held by RIP.
static	Applies to static route information.

option : Option

Setting value	Description
metric <0-16777214>	Sets the metric value used when redistributing external routing information into the OSPF area. If omitted, the value set by the **default-metric** command is used as the metric value.
metric-type <1-2>	Specifies the metric type of the external route information. If omitted, this is 2.
tag <0-4294967295>	Specifies the route tag number.

[Initial value]

none

[Input mode]

OSPFv2 mode

[Description]

Advertises the specified external route information to the OSPF area as an AS external LSA.

This is valid only for an ASBR.

[Example]

Advertise the statically set route information with metric value 10 to the OSPF area.

```
SWX3220(config-router)# redistribute static metric 10
```

7.14.26 Set summary destination network address when advertising to OSPF area (OSPFv2)

[Syntax]

summary-address *network* [**not-advertise**] [**tag** *tag*]
no summary-address *network* [**not-advertise**] [**tag** *tag*]

[Keyword]

not-advertise : External route information whose destination is included in the summary destination network address is no longer advertised to the OSPF area.

[Parameter]

network : Network range. OSPF runs on the interface to which the specified IP address range is assigned. The input format is as follows.

Setting value	Description
A.B.C.D/M	IPv4 address with specified subnet mask length
A.B.C.D E.F.G.H	IPv4 address (A.B.C.D) with wildcard bits (E.F.G.H)

tag : <0-4294967295>

Route tag number

[Initial value]

none

[Input mode]

OSPFv2 mode

[Description]

Specifies the summary destination network address for when summarizing external route information and advertising it to the OSPF area.

Summarization applies to the external route information with destinations that are included in the specified network address.

This is valid only for an ASBR.

[Example]

When 172.16.1.0/24 and 172.16.2.0/24 are registered in the RIB as external route information, summarize them to 172.16.0.0/16 and advertise them to the OSPF area.

```
SWX3220(config-router)# summary-address 172.16.0.0/16
```

Of the external route information that is held, don't advertise the route information that is included in 172.16.0.0/16.

```
SWX3220(config-router)# summary-address 172.16.0.0/16 not-advertise
```

7.14.27 Set minimum wait time until LSA is received

[Syntax]

timers lsa arrival *time*
no timers lsa arrival

[Parameter]

time : <0-600000>

Minimum wait time (milliseconds)

[Initial value]

timers lsa arrival 1000

[Input mode]

OSPFv2 mode

[Description]

Of the LSAs transmitted by the adjacent router, sets the minimum wait time until receiving the same LSA as previously received.

If the same LSA as previously received within the specified time is received, that LSA is discarded.

7.14.28 Set delay time for changes related to the shortest path calculation

[Syntax]

timers spf exp *min max*
no timers spf exp

[Parameter]

min : <0-2147483647>

Minimum delay time (milliseconds)

max : <0-2147483647>

Maximum delay time (milliseconds)

[Initial value]

timers spf exp 500 50000

[Input mode]

OSPFv2 mode

[Description]

Sets the delay time when notified of changes related to the shortest path calculation (SPF calculation).

7.14.29 Set transmission wait time for link state advertisements

[Syntax]

timers throttle lsa all *start hold max*
no timers throttle lsa all

[Parameter]

start : <0-600000>

LSA transmission wait time when topology change occurs (milliseconds)

hold : <0-600000>

LSA transmission wait time when successive topology change occurs (milliseconds)

max : <0-600000>

LSA transmission wait time when topology does not change (milliseconds)

[Initial value]

timers throttle lsa all 0 0 0

[Input mode]

OSPFv2 mode

[Description]

Sets the transmission wait time for link state advertisements.

start specifies the wait time from when the topology changes until a link state advertisement reflecting the change is transmitted.

hold specifies the wait time from when successive topology changes occur until the first link state advertisement is transmitted.

max specifies the wait time until the same link state advertisement as previously is transmitted, no topology change having occurred.

7.14.30 Set metric value for default route (OSPFv3)

[Syntax]

area *area_id* **default-cost** *metric*
no area *area_id* **default-cost**

[Parameter]

area_id : Area ID

Setting value	Description
A.B.C.D	OSPF area ID in IPv4 address format
<0-4294967295>	OSPF area ID in four-octet integer format

metric : <0-16777215>

Metric value of default route advertised to NSSA or stub area

[Initial value]

area *area_id* default-cost 1

[Input mode]

OSPFv3 mode

[Description]

Metric value of default route advertised to NSSA or stub area.

This is enabled only for the ABR of an NSSA or stub area.

[Example]

With area 1 as a stub area, specify the default route's metric value as 10.

```
SWX3220(config-router)# area 1 stub no-summary
SWX3220(config-router)# area 1 default-cost 10
```

7.14.31 Set area as NSSA (OSPFv3)

[Syntax]

area *area_id* **nssa** [*option* [*option* ...]]
no area *area_id* **nssa** [*option* [*option* ...]]

[Parameter]

area_id : Area ID

Setting value	Description
A.B.C.D	OSPF area ID in IPv4 address format
<0-4294967295>	OSPF area ID in four-octet integer format

option : Option (Valid only for the ABR of the applicable NSSA)

Setting value	Description
default-information-originate [metric <0-16777214>] [metric-type <1-2>]	Notifies the applicable NSSA of the default route LSA (type 7). Use the "metric" option to specify the metric value of the default route's LSA (type 7). If omitted, this is 1. Use the "metric-type" option to specify the metric type. If omitted, this is 2.
no-redistribution	Route information of other areas is not provided to the applicable NSSA.
no-summary	Route information of other areas is not provided to the applicable NSSA.
stability-interval <0-2147483647>	Specifies the time (seconds) to continue LSA (type 7) notification to the applicable NSSA. This is used when transitioning the NSSA's translator to another device; by using this setting to inform the applicable NSSA of the external route via LSA (type 7), this setting minimizes unnecessary LSDB updates, and allows the translator to transition in a more stable manner.
translator-role *role*	Specifies the operation of the applicable NSSA as an ABR. If *role* is specified as "always", LSA (type 7) is always converted to LSA (type 5). If *role* is specified as "candidate", LSA (type 7) is converted to LSA (type 5) only if this is the applicable NSSA's translator. If *role* is specified as "never", LSA (type 7) is not converted. If *role* is omitted, this will be "candidate".

[Initial value]

none

[Input mode]

OSPFv3 mode

[Description]

Sets the specified area as an NSSA.

If the "no" syntax is used with a specified option, the specified option can be disabled.

[Example]

Set area 1 as an NSSA.

```
SWX3220(config-router)# area 1 nssa
```

7.14.32 Summarize route information of a specified network address region, and advertise to other areas (OSPFv3)

[Syntax]

area *area_id* **range** *range* [*type*]
no area *area_id* **range** *range* [*type*]

[Parameter]

area_id : Area ID

Setting value	Description
A.B.C.D	OSPF area ID in IPv4 address format
<0-4294967295>	OSPF area ID in four-octet integer format

range : Summary destination network address

Setting value	Description
X:X::X:X/M	Specifies the IPv6 network address that will be the summary destination. This can be specified for OSPFv3 mode.

type : Advertise route information

Setting value	Description
advertise	The summarized route information is advertised to other areas.
not-advertise	Route information of the specified network address region is not advertised to other areas.

[Initial value]

none

[Input mode]

OSPFv3 mode

[Description]

Route information of the specified network address region is not advertised to other areas.

This is valid only for an ABR.

If "advertise" is specified, summarized route information is advertised to other areas.

If "not-advertise" is specified, route information of the specified network address region is not advertised to other areas.

If omitted, it is considered that "advertise" is set.

7.14.33 Set area as stub area (OSPFv3)

[Syntax]

area *area_id* **stub** [**no-summary**]
no area *area_id* **stub** [**no-summary**]

[Keyword]

no-summary : Route information to other areas is not advertised to the applicable stub area (specify as a totally stubby area).

[Parameter]

area_id : Area ID

Setting value	Description
A.B.C.D	OSPF area ID in IPv4 address format
<0-4294967295>	OSPF area ID in four-octet integer format

[Initial value]

none

[Input mode]

OSPFv3 mode

[Description]

Sets the specified area as a stub area.

If the "no" syntax is used with a specified option, the specified option can be disabled.

7.14.34 Specify virtual link on area (OSPFv3)

[Syntax]

area *area_id* **virtual-link** *router_id* [*option* [*option* ...]]
no area *area_id* **virtual-link** *router_id* [*option* [*option* ...]]

[Parameter]

area_id : Area ID

Setting value	Description
A.B.C.D	OSPF area ID in IPv4 address format
<0-4294967295>	OSPF area ID in four-octet integer format

router_id : Router ID (A.B.C.D) of the ABR that is the other end of the virtual link

option : Option

Setting value	Description
dead-interval <1-65535>	Specify the wait time from when Hello packets stop being received from the ABR that is the other end of the virtual link until a down state is determined. If omitted, this is 40.
hello-interval <1-65535>	Specify the interval at which Hello packets are transmitted to the ABR that is the other end of the virtual link. If omitted, this is 10.
retransmit-interval <1-3600>	Specifies the OSPF packet retransmission interval. If omitted, this is 5.
transmit-delay <1-3600>	Specifies the OSPF packet transmission delay time. If omitted, this is 1.

[Initial value]

none

[Input mode]

OSPFv3 mode

[Description]

Specifies a virtual link on the specified area.

If the "no" syntax is used with a specified option, the specified option can be disabled.

This command must also be used to specify a virtual link on the ABR that is the other end of the virtual link, and the options must be the same.

7.14.35 Set bandwidth of interface (OSPFv3)

[Syntax]

auto-cost reference-bandwidth *bandwidth*
no auto-cost reference-bandwidth *bandwidth*

[Parameter]

bandwidth : <1-4294967>

Bandwidth (Mbps)

[Initial value]

auto-cost reference-bandwidth 100

[Input mode]

OSPFv3 mode

[Description]

Specifies the bandwidth value used when calculating the default metric value of the interface.

[Example]

Calculate the default metric value with 100 Mbps as the bandwidth of the interface.

```
SWX3220(config-router)# auto-cost reference-bandwidth 100
```

7.14.36 Set LSDB summary list optimization (OSPFv3)

[Syntax]

db-summary-opt *mode*
no db-summary-opt

[Parameter]

mode : Mode

Setting value	Description
enable	Enables optimization of the LSDB summary list.
disable	Disables optimization of the LSDB summary list.

[Initial value]

db-summary-opt disable

[Input mode]

OSPFv3 mode

[Description]

Enables optimization of the LSDB summary list.

When this function is enabled, if the LSA in the LSDB summary list is the same or newer when compared to the LSA included in the DD (Database Description) packet received from the neighbor, then that LSA is deleted from the LSDB summary list, thereby optimizing exchange of database information.

7.14.37 Set default external route (OSPFv3)

[Syntax]

default-information originate [*option* [*option* ...]]
no default-information originate [*option* [*option* ...]]

[Parameter]

option : Option

Setting value	Description
always	Notify default route information even if no default route information is held. If this is omitted, default external route information is advertised only if default route information is held.
metric <0-16777214>	Specifies the metric value used when advertising default external route information to the OSPF routing domain. If omitted, this is 10.
metric-type <1-2>	Specifies the metric type of the default external route information. If omitted, this is 2.

[Initial value]

none

[Input mode]

OSPFv3 mode

[Description]

This specifies whether the default external route is advertised to the OSPF routing domain.

This is valid only for an ASBR.

If the "no" syntax is used with a specified option, the specified option can be disabled.

[Example]

Always advertise the default external route to the OSPF routing domain with a metric value of 10 and a metric type of 1.

```
SWX3220(config-router)# default-information originate always metric 10 metric-type 1
```

7.14.38 Set metric value when advertising to OSPF routing domain (OSPFv3)

[Syntax]

default-metric *metric*
no default-metric

[Parameter]

metric : <1-16777214>

Default metric value

[Initial value]

none

[Input mode]

OSPFv3 mode

[Description]

Specifies the metric value used when advertising external route information to the OSPF routing domain.

This is used in conjunction with the **redistribute** command.

7.14.39 Set priority of route taken from OSPF into FIB (OSPFv3)

[Syntax]

distance *priority*
distance ospfv3 [*option* [*option*]]
no distance
no distance ospfv3

[Parameter]

priority : <1-254>

Priority of route taken from OSPF into FIB

option : Option

Setting value	Description
intra-area <1-254>	Priority of route information within the area
inter-area <1-254>	Priority of route information between areas
external <1-254>	Priority of external routing information

[Initial value]

priority 110

[Input mode]

OSPFv3 mode

[Description]

Sets priority of route taken from OSPF into FIB.

If *priority* is specified, it is handled as the priority for all routing information.

7.14.40 Set filtering for route information between RIB and OSPF routing table (OSPFv3)

[Syntax]

distribute-list *access_list_id* **out** *kind*
distribute-list *access_list_id* **in**
no distribute-list *access_list_id* **out** [*kind*]
no distribute-list *access_list_id* **in**

[Parameter]

access_list_id : Access list number specified by the access-list command

kind : Type of route

Setting value	Description
connected	Applies to direct routes.
ospf [*process_id*]	Applies to route information held by OSPF.
rip	Applies to route information held by RIP.
static	Applies to static route information.

process_id : <0-65535> OSPF process ID (This can be used only if "ospf" is specified for "kind")

[Initial value]

none

[Input mode]

OSPFv3 mode

[Description]

Sets filtering for route information between the RIB (Routing Information Base) and the OSPF routing table.

This is valid only for an ASBR.

7.14.41 Set stub host route (OSPFv3)

[Syntax]

host *host* **area** *area_id*
no host *host* **area** *area_id*

[Parameter]

host : X:X::X:X

IPv4 address of host

area_id : Area ID

Setting value	Description
A.B.C.D	OSPF area ID in IPv4 address format
<0-4294967295>	OSPF area ID in four-octet integer format

[Initial value]

none

[Input mode]

OSPFv3 mode

[Description]

For the specified area, advertises the specified IP address as the stub host route.

[Example]

Advertise 1000::1 to area 1 as the stub host route.

```
SWX3220(config-router)# host 1000::1 area 1
```

7.14.42 Set number of concurrent DD exchange processes (OSPFv3)

[Syntax]

max-concurrent-dd *dd_num*
no max-concurrent-dd [*dd_num*]

[Parameter]

dd_num	:	<1-65535> Number of concurrent DD exchange processes

[Initial value]

max-concurrent-dd 5

[Input mode]

OSPFv3 mode

[Description]

Sets the number of DD exchange processes that can occur concurrently.

At the maximum, DD exchange can be performed for the specified number of neighbors that are in the Exchange state.

7.14.43 Set OSPF passive interface (OSPFv3)

[Syntax]

passive-interface [*interface* [**disable**]]
no passive-interface [*interface* [**disable**]]

[Parameter]

interface	:	Interface name

[Initial value]

none

[Input mode]

OSPFv3 mode

[Description]

Sets the OSPF passive interface.

If *interface* is not specified, all interfaces will no longer send OSPF Hello messages.

If *interface* is specified, that interface will no longer send OSPF Hello messages. However, information of the network connected to the passive interface is subject to OSPF processing.

7.14.44 Advertise the specified external route information to the OSPF area as an AS external LSA (OSPFv3)

[Syntax]

redistribute *kind* [*option* [*option* ...]]
no redistribute *kind* [*option* [*option* ...]]

[Parameter]

kind	:	Type of route

Setting value	Description
connected	Applies to direct routes.
ospf [*process_id*]	Applies to route information held by OSPF.
rip	Applies to route information held by RIP.
static	Applies to static route information.

option : Option

Setting value	Description
metric <0-16777214>	Sets the metric value used when redistributing external routing information into the OSPF area. If omitted, the value set by the **default-metric** command is used as the metric value.
metric-type ><1-2>	Specifies the metric type of the external route information. If omitted, this is 2.
tag <0-4294967295>	Specifies the route tag number.

[Initial value]

none

[Input mode]

OSPFv3 mode

[Description]

Advertises the specified external route information to the OSPF area as an AS external LSA.

This is valid only for an ASBR.

[Example]

Advertise the statically set route information with metric value 10 to the OSPF area.

```
SWX3220(config-router)# redistribute static metric 10
```

7.14.45 Set OSPF router ID (OSPFv3)

[Syntax]

router-id *router_id*
no router-id [*router_id*]

[Parameter]

router-id : Router ID (IPv4 format IP address)

[Initial value]

none

[Input mode]

OSPFv3 mode

[Description]

Sets the OSPF router ID.

Although several ways to specify the OSPF router ID are provided, the decision is based on the following priority order.

1. Value set by the **router-id** command or the **ospf router-id** command entered in OSPFv3 mode
2. Value set by the **router-id** command entered in global configuration mode
3. Highest IP address of those specified for the VLAN interface

[Note]

If the router ID is changed, the changed router ID takes effect when this unit is restarted or when the OSPF process is restarted.

7.14.46 Set summary destination network address when advertising to OSPF area (OSPFv3)

[Syntax]

summary-address *network* [**not-advertise**] [**tag** *tag*]
no summary-address *network* [**not-advertise**] [**tag** *tag*]

[Keyword]

not-advertise : External route information whose destination is included in the summary destination network address is no longer advertised to the OSPF area.

[Parameter]

network : Network range. OSPF runs on the interface to which the specified IP address range is assigned. The input format is as follows.

Setting value	Description
X:X::X:X/M	Network range in IPv6 address format

tag : <0-4294967295>

Route tag number

[Initial value]

none

[Input mode]

OSPFv3 mode

[Description]

Specifies the summary destination network address for when summarizing external route information and advertising it to the OSPF area.

Summarization applies to the external route information with destinations that are included in the specified network address.

This is valid only for an ASBR.

7.14.47 Set area authentication for each interface

[Syntax]

ip ospf [*ip_address*] **authentication** [*type*]
no ip ospf [*ip_address*] **authentication**

[Parameter]

ip_address : IP address of interface (IPv4 format)

type : Authentication type

Setting value	Description
null	Do not use area authentication.
message-digest	Use digest authentication.

[Initial value]

none

[Input mode]

interface mode

[Description]

For each interface, enables authentication within the area.

If *type* is not specified, simple password authentication is used. In this case, use the **ip ospf authentication-key** command to specify the authentication key.

If "message-digest" is specified as the *type*, MD5 digest authentication is used. In this case, use the **ip ospf message-digest-key** command to specify the authentication key.

This command takes priority over the **area authentication** command.

If this command is not specified, authentication enable/disable within the area is determined by the value of the **area authentication** command.

7.14.48 Set authentication key used for area authentication

[Syntax]

ip ospf [*ip_address*] **authentication-key** *key*
no ip ospf [*ip_address*] **authentication-key**

[Parameter]

ip_address	:	IP address of interface (IPv4 format)
key	:	Character string to be the authentication key (single byte 8 characters or less)

[Initial value]

none

[Input mode]

interface mode

[Description]

Sets the authentication key used for simple password authentication in an area.

The authentication key specified by this command is used when simple password authentication is enabled by the **ip ospf authentication** command or the **area authentication** command.

[Example]

Enable area authentication on the VLAN #1 interface, and set the authentication key to "yamaha".

```
SWX3220(config)# interface vlan1
SWX3220(config-if)# ip ospf authentication
SWX3220(config-if)# ip ospf authentication-key yamaha
```

7.14.49 Set fixed cost for an interface

[Syntax]

ip ospf [*ip_address*] **cost** *cost*
no ip ospf [*ip_address*] **cost**

[Parameter]

ip_address	:	IP address of interface (IPv4 format)
cost	:	<1-65535> Cost value

[Initial value]

none

[Input mode]

interface mode

[Description]

Sets a fixed cost for the specified interface.

7.14.50 Reduce LSA flooding for an interface

[Syntax]

ip ospf [*ip_address*] **database-filter all out**
no ip ospf [*ip_address*] **database-filter all out**

[Parameter]

ip_address	:	IP address of interface (IPv4 format)

[Initial value]

none

[Input mode]

interface mode

[Description]

Reduces LSA flooding for the specified interface.

7.14.51 Set time until neighboring router is considered down

[Syntax]

ip ospf [*ip_address*] **dead-interval** *interval*
no ip ospf [*ip_address*] **dead-interval**

[Parameter]

ip_address	:	IP address of interface (IPv4 format)
interval	:	<1-65535> Interval time (seconds)

[Initial value]

ip ospf dead-interval 40

[Input mode]

interface mode

[Description]

Sets the time from when Hello packets are no longer received until the neighboring router is considered to be down.

7.14.52 Disable OSPF

[Syntax]

ip ospf disable all
no ip ospf disable all

[Initial value]

none

[Input mode]

interface mode

[Description]

Stops OSPF on the specified interface.

7.14.53 Set transmission interval of Hello packets

[Syntax]

ip ospf [*ip_address*] **hello-interval** *interval*
no ip ospf [*ip_address*] **hello-interval**

[Parameter]

ip_address	:	IP address of interface
interval	:	<1-65535> Interval time (seconds)

[Initial value]

ip ospf hello-interval 10

[Input mode]

interface mode

[Description]

Sets transmission interval of Hello packets.

7.14.54 Set MD5 digest authentication key used for OSPF authentication

[Syntax]

ip ospf [*ip_address*] **message-digest-key** *id* **md5** *key*
no ip ospf [*ip_address*] **message-digest-key** *id*

[Parameter]

ip_address : IP address of interface (IPv4 format)

id : <1-255>
ID number of key

key : Character string to be the key (Single byte 16 characters or less)

[Initial value]

none

[Input mode]

interface mode

[Description]

Sets the MD5 digest authentication key used for OSPF authentication on the specified interface.

[Note]

The value set by this command is used only if MD5 digest authentication is enabled by the **area authentication** command or the **ip ospf authentication** command.

7.14.55 Configuring the OSPF network type (OSPFv2)

[Syntax]

ip ospf network *NETWORK*
no ip ospf network

[Parameter]

NETWORK : OSPF network type

Setting value	Description
broadcast	Broadcast network
point-to-point	P2P network

[Initial value]

broadcast

[Input mode]

interface mode

[Description]

Configures the OSPF network type.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be specified only for VLAN interfaces.

7.14.56 Set priority for selecting designated router (DR)

[Syntax]

ip ospf priority *priority*
no ip ospf priority

[Parameter]

priority : <0-255>
Priority

[Initial value]

priority : 1

[Input mode]

interface mode

[Description]

Sets the priority for selecting the designated router (DR).
The device with the highest priority in the OSPF network is selected as the designated router.
If there are multiple devices that have the same priority, the designated router is selected by router ID.
If the priority is specified as 0, the device will not be selected as the designed router.

7.14.57 Set packet retransmission interval

[Syntax]

ip ospf [*ip_address*] **retransmit-interval** *interval*
no ip ospf [*ip_address*] **retransmit-interval**

[Parameter]

ip_address : IP address of interface (IPv4 format)

interval : <1-1800>
Interval time (seconds)

[Initial value]

ip ospf retransmit-interval 5

[Input mode]

interface mode

[Description]

Sets the time interval at which Link State Request, Link State Update, and Database Description packets are retransmitted.

7.14.58 Set increment value when transmitting age field of Link State Update packets

[Syntax]

ip ospf [*ip_address*] **transmit-delay** *delay*
no no ip ospf [*ip_address*] **transmit-delay**

[Parameter]

ip_address : IP address of interface (IPv4 format)

delay : <1-3600>
Transmission delay time (seconds)

[Initial value]

ip ospf transmit-delay 1

[Input mode]

interface mode

[Description]

Link State Update packets are transmitted with their "age" field value incremented by the value specified by this command.

7.14.59 Set fixed cost for an interface (IPv6)

[Syntax]

ipv6 ospf cost *cost* [**instance-id** *id*]
no ipv6 ospf cost [**instance-id** *id*]

[Parameter]

cost	:	<1-65535>
		Cost value
id	:	<0-31><64-95>
		Instance ID

[Initial value]

none

[Input mode]

interface mode

[Description]

Sets a fixed cost for the specified interface.

[Note]

This command cannot be used if the stack function is enabled.

7.14.60 Set time until neighboring router is considered down (IPv6)

[Syntax]

ipv6 ospf dead-interval *interval* [**instance-id** *id*]
no ipv6 ospf dead-interval [**instance-id** *id*]

[Parameter]

interval	:	<1-65535>
		Interval time (seconds)
id	:	<0-31><64-95>
		Instance ID

[Initial value]

ipv6 ospf dead-interval 40

[Input mode]

interface mode

[Description]

Sets the time from when Hello packets are no longer received until the neighboring router is considered to be down.

[Note]

This command cannot be used if the stack function is enabled.

7.14.61 Set transmission interval of Hello packets (IPv6)

[Syntax]

ipv6 ospf hello-interval *interval* [**instance-id** *id*]
no ipv6 ospf hello-interval [**instance-id** *id*]

[Parameter]

interval	:	<1-65535>

Interval time (seconds)

id : <0-31><64-95>

Instance ID

[Initial value]

ipv6 ospf hello-interval 10

[Input mode]

interface mode

[Description]

Sets transmission interval of Hello packets

[Note]

This command cannot be used if the stack function is enabled.

7.14.62 Configuring the OSPF network type (OSPFv3)

[Syntax]

ipv6 ospf network *NETWORK*
no ipv6 ospf network

[Parameter]

NETWORK : OSPF network type

Setting value	Description
broadcast	Broadcast network
point-to-point	P2P network

[Initial value]

broadcast

[Input mode]

interface mode

[Description]

Configures the OSPF network type.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be specified only for VLAN interfaces.

7.14.63 Set priority for selecting designated router (DR) (IPv6)

[Syntax]

ipv6 ospf priority *priority* [**instance-id** *id*]
no ipv6 ospf priority [**instance-id** *id*]

[Parameter]

priority : <0-255>

Priority

id : <0-31><64-95>

Instance ID

[Initial value]

ipv6 ospf priority 1

[Input mode]

interface mode

[Description]

Sets the priority for selecting the designated router (DR).

The device with the highest priority in the OSPF network is selected as the designated router.

If there are multiple devices that have the same priority, the designated router is selected by router ID.

If the priority is specified as 0, the device will not be selected as the designed router.

[Note]

This command cannot be used if the stack function is enabled.

7.14.64 Set packet retransmission interval (IPv6)

[Syntax]

ipv6 ospf retransmit-interval *interval* [**instance-id** *id*]
no ipv6 ospf retransmit-interval [**instance-id** *id*]

[Parameter]

interval : <1-1800>

Interval time (seconds)

id : <0-31><64-95>

Instance ID

[Initial value]

ipv6 ospf retransmit-interval 5

[Input mode]

interface mode

[Description]

Sets the time interval at which Link State Request, Link State Update, and Database Description packets are retransmitted.

[Note]

This command cannot be used if the stack function is enabled.

7.14.65 Specify area in the interface (IPv6)

[Syntax]

ipv6 router ospf area *area_id* [**instance-id** *id*] [**tag** *tag*]
no ipv6 router ospf area *area_id* [**instance-id** *id*] [**tag** *tag*]

[Parameter]

area_id : Area ID

Settting value	Description
A.B.C.D	OSPF area ID in IPv4 address format
<0-4294967295>	OSPF area ID in four-octet integer format

id : <0-31><64-95>

Instance ID

tag : <0-4294967295>

OSPFv3 process tag

[Initial value]

none

[Input mode]

interface mode

[Description]

Specifies the OSPFv3 associated area for the specified interface.

[Note]

This command cannot be used if the stack function is enabled.

7.14.66 Set increment value when transmitting age field of Link State Update packets (IPv6)

[Syntax]

ipv6 ospf transmit-delay *delay* [**instance-id** *id*]
no ipv6 ospf transmit-delay [**instance-id** *id*]

[Parameter]

delay	:	<1-1800>
		Transmission delay time (seconds)
id	:	<0-31><64-95>
		Instance ID

[Initial value]

ipv6 ospf transmit-delay 1

[Input mode]

interface mode

[Description]

Link State Update packets are transmitted with their "age" field value incremented by the value specified by this command.

[Note]

This command cannot be used if the stack function is enabled.

7.14.67 Restart OSPF process (IPv4)

[Syntax]

clear ip ospf [*process_id*] **process**

[Parameter]

process_id	:	<0-65535>
		OSPF process ID

[Input mode]

privileged EXEC mode

[Description]

Restarts the OSPF process, and performs OSPF processing from the beginning.

If the *process_id* parameter is not specified, all OSPF processes are affected.

7.14.68 Show OSPF process information (IPv4)

[Syntax]

show ip ospf [*process_id*]

[Parameter]

process_id	:	<0-65535>
		OSPF process ID

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows OSPF process information.

If the *process_id* parameter is omitted, information is shown for all currently running OSPF processes.

7.14.69 Show ABR and ASBR route information (IPv4)

[Syntax]

show ip ospf [*process_id*] **border-routers**

[Parameter]

process_id : <0-65535>

OSPF process ID

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows route information for Area Border Router (ABR) and AS border router (ASBR).

If the **process_id** parameter is omitted, this applies to all currently running OSPF processes.

7.14.70 Show LSA information in the link state database matching the specified conditions (IPv4)

[Syntax]

show ip ospf [*process_id*] **database** [*condition*]

[Parameter]

process_id : <0-65535>

OSPF process ID

condition : Information to show

Setting value	Description
adv-router A.B.C.D	Show only the LSAs of the IP address specified by the advertisement source.
max-age	Show only the LSAs whose link status age is the maximum value (3600 seconds).
self-originate	Show only the LSAs whose advertisement source is its own router ID.

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows LSA information in the link state database matching the specified conditions.

If conditions are not specified, all LSA information is shown.

7.14.71 Show ASBR summary LSA information in the link state database

[Syntax]

show ip ospf [*process_id*] **database asbr-summary** [*condition*]

[Parameter]

process_id : <0-65535>

OSPF process ID

condition : Information to show

Setting value	Description
A.B.C.D	Show only the LSAs that match the ID specified by the link state ID in the ASBR.
adv-router A.B.C.D	Show only the LSAs of the IP address specified by the advertisement source.
self-originate	Show only the LSAs whose advertisement source is its own router ID.

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Show ASBR summary LSA information (type 4) in the link state database.

7.14.72 Show AS external LSA information in the link state database (IPv4)

[Syntax]

show ip ospf [*process_id*] **database external** [*condition*]

[Parameter]

process_id : <0-65535>

OSPF process ID

condition : Information to show

Setting value	Description
A.B.C.D	Show only the LSAs that match the ID specified by the link state ID in the ASBR.
adv-router A.B.C.D	Show only the LSAs of the IP address specified by the advertisement source.
self-originate	Show only the LSAs whose advertisement source is its own router ID.

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Show AS external LSA information (type 5) in the link state database.

7.14.73 Show network LSA information in the link state database (IPv4)

[Syntax]

show ip ospf [*process_id*] **database network** [*condition*]

[Parameter]

process_id : <0-65535>

OSPF process ID

condition : Information to show

Setting value	Description
A.B.C.D	Show only the LSAs that match the ID specified by the link state ID in the ASBR.
adv-router A.B.C.D	Show only the LSAs of the IP address specified by the advertisement source.
self-originate	Show only the LSAs whose advertisement source is its own router ID.

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Show network LSA information (type 2) in the link state database.

7.14.74 Show NSSA AS external LSA information in the link state database

[Syntax]

show ip ospf [*process_id*] **database nssa-external** [*condition*]

[Parameter]

process_id : <0-65535>

OSPF process ID

condition : Information to show

Setting value	Description
A.B.C.D	Show only the LSAs that match the ID specified by the link state ID in the ASBR.
adv-router A.B.C.D	Show only the LSAs of the IP address specified by the advertisement source.
self-originate	Show only the LSAs whose advertisement source is its own router ID.

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Show NSSA AS external LSA information (type 7) in the link state database.

7.14.75 Show router LSA information in the link state database (IPv4)

[Syntax]

show ip ospf [*process_id*] **database router** [*condition*]

[Parameter]

process_id : <0-65535>

OSPF process ID

condition : Information to show

Setting value	Description
A.B.C.D	Show only the LSAs that match the ID specified by the link state ID in the ASBR.
adv-router A.B.C.D	Show only the LSAs of the IP address specified by the advertisement source.
self-originate	Show only the LSAs whose advertisement source is its own router ID.

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Show router LSA information (type 1) in the link state database.

7.14.76 Show network summary LSA information in the link state database

[Syntax]

show ip ospf [*process_id*] **database summary** [*condition*]

[Parameter]

process_id : <0-65535>

OSPF process ID

condition : Information to show

Setting value	Description
A.B.C.D	Show only the LSAs that match the ID specified by the link state ID in the ASBR.
adv-router A.B.C.D	Show only the LSAs of the IP address specified by the advertisement source.
self-originate	Show only the LSAs whose advertisement source is its own router ID.

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Show networkR summary LSA information (type 3) in the link state database.

7.14.77 Show OSPF interface information (IPv4)

[Syntax]

show ip ospf interface [*interface*]

[Parameter]

interface : VLAN interface

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows OSPF interface information.

7.14.78 Show OSPF neighbor information for the specified neighbor (IPv4)

[Syntax]

show ip ospf [*process_id*] **neighbor** [*condition*]

[Parameter]

process_id : <0-65535>

OSPF process ID

condition : Information to show

Setting value	Description
A.B.C.D [detail]	Show information for the specified neighbor. If "detail" is specified, detailed information is shown.
interface A.B.C.D	Show information for the neighbor adjacent to the OSPF interface that has the specified IP address.
[detail] all	Show information for all neighbors. If "detail" is specified, detailed information is shown.

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows OSPF neighbor information.

7.14.79 Show OSPF routing table (IPv4)

[Syntax]

show ip ospf [*process_id*] **route** [*condition*]

[Parameter]

process_id : <0-65535>

OSPF process ID

condition : Information to show

Setting value	Description
A.B.C.D	Show specified route information.
A.B.C.D/M	Show route information within the specified network.
summary	Show the route information summary.

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows OSPF routing table.

7.14.80 Show OSPF virtual link information (IPv4)

[Syntax]

show ip ospf [*process_id*] **virtual-links**

[Parameter]

process_id : <0-65535>

OSPF process ID

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows OSPF virtual link information.

7.14.81 Show OSPF settings and status (IPv4)

[Syntax]

show ip protocols ospf

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the OSPF settings and status.

7.14.82 Restart OSPF process (IPv6)

[Syntax]

clear ipv6 ospf [*process_id*] **process**

[Parameter]

process_id : <0-65535>

OSPF process ID

[Input mode]

privileged EXEC mode

[Description]

Restarts the OSPF process, and performs OSPF processing from the beginning.

If the *process_id* parameter is not specified, all OSPF processes are affected.

[Note]

This command cannot be used if the stack function is enabled.

7.14.83 Show OSPF process information (IPv6)

[Syntax]

show ipv6 ospf [*process_id*]

[Parameter]

process_id	:	<0-65535> OSPF process ID

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows OSPF process information.

If the *process_id* parameter is omitted, information is shown for all currently running OSPF processes.

[Note]

This command cannot be used if the stack function is enabled.

7.14.84 Show ABR and ASBR route information (IPv6)

[Syntax]

show ipv6 ospf [*process_id*] **border-routers**

[Parameter]

process_id	:	<0-65535> OSPF process ID

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows route information for Area Border Router (ABR) and AS border router (ASBR).

If the **process_id** parameter is omitted, this applies to all currently running OSPF processes.

[Note]

This command cannot be used if the stack function is enabled.

7.14.85 Show LSA information in the link state database matching the specified conditions (IPv6)

[Syntax]

show ipv6 ospf [*process_id*] **database** [*condition*]

[Parameter]

process_id	:	<0-65535> OSPF process ID
condition	:	Information to show

Setting value	Description
adv-router A.B.C.D	Show only the LSAs of the IP address specified by the advertisement source.
max-age	Show only the LSAs whose link status age is the maximum value (3600 seconds).
self-originate	Show only the LSAs whose advertisement source is its own router ID.

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows LSA information in the link state database matching the specified conditions.

If conditions are not specified, all LSA information is shown.

[Note]

This command cannot be used if the stack function is enabled.

7.14.86 Show AS external LSA information in the link state database matching the specified conditions (IPv6)

[Syntax]

show ipv6 ospf [*process_id*] **database external** [*condition*]

[Parameter]

process_id : <0-65535>

OSPF process ID

condition : Information to show

Setting value	Description
A.B.C.D	Show only the LSAs that match the ID specified by the link state ID in the ASBR.
adv-router A.B.C.D	Show only the LSAs of the IP address specified by the advertisement source.
self-originate	Show only the LSAs whose advertisement source is its own router ID.

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Show AS external LSA information (type 5) in the link state database.

[Note]

This command cannot be used if the stack function is enabled.

7.14.87 Show Inter-Area-Prefix LSA information in the link state database (IPv6)

[Syntax]

show ipv6 ospf [*process_id*] **database inter-prefix** [*condition*]

[Parameter]

process_id : <0-65535>

OSPF process ID

condition : Information to show

Setting value	Description
A.B.C.D	Show only the LSAs that match the ID specified by the link state ID in the ASBR.
adv-router A.B.C.D	Show only the LSAs of the IP address specified by the advertisement source.
self-originate	Show only the LSAs whose advertisement source is its own router ID.

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Show Inter-Area-Prefix LSA information (type 3) in the link state database.

[Note]

This command cannot be used if the stack function is enabled.

7.14.88 Show Inter-Area-Router LSA information in the link state database (IPv6)

[Syntax]

show ipv6 ospf [*process_id*] **database inter-router** [*condition*]

[Parameter]

process_id : <0-65535>

OSPF process ID

condition : Information to show

Setting value	Description
A.B.C.D	Show only the LSAs that match the ID specified by the link state ID in the ASBR.
adv-router A.B.C.D	Show only the LSAs of the IP address specified by the advertisement source.
self-originate	Show only the LSAs whose advertisement source is its own router ID.

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Show Inter-Area-Router LSA information (type 4) in the link state database.

[Note]

This command cannot be used if the stack function is enabled.

7.14.89 Show Intra-Area-Prefix LSA information in the link state database (IPv6)

[Syntax]

show ipv6 ospf [*process_id*] **database intra-prefix** [*condition*]

[Parameter]

process_id : <0-65535>

OSPF process ID

condition : Information to show

Setting value	Description
A.B.C.D	Show only the LSAs that match the ID specified by the link state ID in the ASBR.
adv-router A.B.C.D	Show only the LSAs of the IP address specified by the advertisement source.
self-originate	Show only the LSAs whose advertisement source is its own router ID.

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Show Intra-Area-Prefix LSA information (type 9) in the link state database.

[Note]

This command cannot be used if the stack function is enabled.

7.14.90 Show Link LSA information in the link state database (IPv6)

[Syntax]

show ipv6 ospf [*process_id*] **database link** [*condition*]

[Parameter]

process_id : <0-65535>

OSPF process ID

condition : Information to show

Setting value	Description
A.B.C.D	Show only the LSAs that match the ID specified by the link state ID in the ASBR.
adv-router A.B.C.D	Show only the LSAs of the IP address specified by the advertisement source.
self-originate	Show only the LSAs whose advertisement source is its own router ID.

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Show Link LSA information (type 8) in the link state database.

[Note]

This command cannot be used if the stack function is enabled.

7.14.91 Show network LSA information in the link state database (IPv6)

[Syntax]

show ipv6 ospf [*process_id*] **database network** [*condition*]

[Parameter]

process_id : <0-65535>

OSPF process ID

condition : Information to show

Setting value	Description
A.B.C.D	Show only the LSAs that match the ID specified by the link state ID in the ASBR.
adv-router A.B.C.D	Show only the LSAs of the IP address specified by the advertisement source.
self-originate	Show only the LSAs whose advertisement source is its own router ID.

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Show network LSA information (type 2) in the link state database.

[Note]

This command cannot be used if the stack function is enabled.

7.14.92 Show router LSA information in the link state database (IPv6)

[Syntax]

show ipv6 ospf [*process_id*] **database router** [*condition*]

[Parameter]

process_id : <0-65535>

OSPF process ID

condition : Information to show

Setting value	Description
A.B.C.D	Show only the LSAs that match the ID specified by the link state ID in the ASBR.
adv-router A.B.C.D	Show only the LSAs of the IP address specified by the advertisement source.
self-originate	Show only the LSAs whose advertisement source is its own router ID.

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Show router LSA information (type 1) in the link state database.

[Note]

This command cannot be used if the stack function is enabled.

7.14.93 Show OSPF interface information (IPv6)

[Syntax]

show ipv6 ospf interface [*interface*]

[Parameter]

interface : VLAN interface

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows OSPF interface information.

[Note]

This command cannot be used if the stack function is enabled.

7.14.94 Show OSPF neighbor information (IPv6)

[Syntax]

show ipv6 ospf [*process_id*] **neighbor** [*condition*]

[Parameter]

process_id : <0-65535>

OSPF process ID

condition : Information to show

Setting value	Description
A.B.C.D [detail]	Show information for the specified neighbor. If "detail" is specified, detailed information is shown.
interface A.B.C.D	Show information for the neighbor adjacent to the OSPF interface that has the specified IP address.
[detail] all	Show information for all neighbors. If "detail" is specified, detailed information is shown.

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows OSPF neighbor information.

[Note]

This command cannot be used if the stack function is enabled.

7.14.95 Show OSPF routing table (IPv6)

[Syntax]

show ipv6 ospf [*process_id*] **route**

[Parameter]

process_id : <0-65535>

OSPF process ID

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows OSPF routing table.

[Note]

This command cannot be used if the stack function is enabled.

7.14.96 Show OSPF virtual link information (IPv6)

[Syntax]

show ipv6 ospf [*process_id*] **virtual-links**

[Parameter]

process_id : <0-65535>

OSPF process ID

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows OSPF virtual link information.

[Note]

This command cannot be used if the stack function is enabled.

7.14.97 Show OSPF settings and status (IPv6)

[Syntax]

show ipv6 protocols ospf

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the OSPF settings and status.

[Note]

This command cannot be used if the stack function is enabled.

7.15 RIP

7.15.1 Move to RIP mode

[Syntax]

router rip
no router rip

[Input mode]

global configuration mode

[Description]

Transition to RIP mode and make settings related to RIPv1 and RIPv2.

[Note]

If this command is executed with the "no" syntax, all RIP mode settings are deleted.

To transition from RIP mode to global configuration mode, use the **exit** command.

7.15.2 Move to RIPng mode

[Syntax]

router ipv6 rip
no router ipv6 rip

[Input mode]

global configuration mode

[Description]

Transition to RIPng mode and make settings related to RIPng.

[Note]

If this command is executed with the "no" syntax, all RIPng mode settings are deleted.

To transition from RIPng mode to global configuration mode, use the **exit** command.

This command cannot be used if the stack function is enabled.

7.15.3 Set default external route

[Syntax]

default-information originate [**always**]
no default-information originate [**always**]

[Keyword]

always : Register default route in RIP routing table even if the default route is not held

[Initial value]

none

[Input mode]

RIP mode, RIPng mode

[Description]

Register default route (0.0.0.0/0) in RIP routing table.

If "always" is not specified, the default route is registered in the RIP routing table only when that default route is held.

If "always" is specified, the default route is registered in the RIP routing table even if the default route is not held.

"always" can be specified only in RIP mode.

7.15.4 Set default metric value when redistributing external route in RIP

[Syntax]

default-metric *metric*
no default-metric [*metric*]

[Parameter]

metric : Metric value (for RIP mode : 1 .. 15, for RIPng mode : 1 .. 16)

[Initial value]

default-metric 1

[Input mode]

RIP mode, RIPng mode

[Description]

Set default metric value when redistributing an external route in RIP.

If a metric value has been specified by the **redistribute** command, the setting of the **redistribute** command takes priority.

7.15.5 Set priority of route taken from RIP into RIB

[Syntax]

distance *priority*
no distance [*priority*]

[Parameter]

priority : <1-255>

Priority of route taken from RIP into RIB

[Initial value]

distance 120

[Input mode]

RIP mode, RIPng mode

[Description]

Set the priority (Administrative Distance value) of a route taken from RIP into RIB.

7.15.6 Set filtering for RIB and RIP routing table

[Syntax]

distribute-list *access_list_id type* [*vlan_interface*]
no distribute-list *access_list_id type* [*vlan_interface*]

[Parameter]

access_list_id : Access list number

type : Direction

Setting value	Description
in	in direction
out	out direction

vlan_interface : VLAN interface

[Initial value]

none

[Input mode]

RIP mode, RIPng mode

[Description]

Filters the route information between the RIB and RIP routing table.

Specify the "in" direction if, within the route information received in the RIP packet, you want to filter routes that are not registered in the RIB.

Specify the "out" direction if you want to filter so that of the route information registered in the RIB, the specified route is not advertised by RIP.

7.15.7 Set neighbor RIP router

[Syntax]

neighbor *ip_address* [*vlan_interface*]
no neighbor *ip_address* [*vlan_interface*]

[Parameter]

ip_address : IP address registered as neighbor

vlan_interface : VLAN interface

[Initial value]

none

[Input mode]

RIP mode, RIPng mode

[Description]

Explicitly specifies the neighbor RIP router. RIP packets for the specified RIP router are transmitted as unicast.

The *vlan_interface* parameter can be selected only in RIPng mode.

If this command is set, both unicast communication and multicast communication is performed to the specified IP address.

If you want to configure RIPng only with the neighbor specified by this command, you can use the **passive-interface** command to stop RIP packet transmission as multicast.

7.15.8 Set network advertised by RIP

[Syntax]

network *prefix*
network *vlan_interface*
no network *prefix*
no network *vlan_interface*

[Parameter]

prefix : Network address advertised by RIP

vlan_interface : VLAN interface

[Initial value]

none

[Input mode]

RIP mode

[Description]

Specifies a network address advertised by RIP or the VLAN interface that is associated with that network address.

RIP advertises the network that is included in the network address range specified in the direct route.

7.15.9 Offset metric value for route information matching the access list

[Syntax]

offset-list *access_list_id type metric* [*vlan_interface*]
no offset-list *access_list_id type metric* [*vlan_interface*]

[Parameter]

access_list_id : Access list number

type : Direction

Setting value	Description
in	in direction
out	out direction

metric : <0-16>

Metric value

vlan_interface : VLAN interface

[Initial value]

none

[Input mode]

RIP mode, RIPng mode

[Description]

Adds an offset metric value for route information that matches the specified access list.

If this is specified with the "in" direction, the specified metric value is added when registering from the RIP routing table to the RIB.

If this is specified with the "out" direction, the specified metric value is added to the advertisement when the route information registered to the RIB is advertised by RIP.

If VLAN interface is specified, this applies only to the route information that is transmitted and received on that VLAN interface.

7.15.10 Set VLAN interface for RIP packet reception only

[Syntax]

passive-interface *vlan_interface*
no passive-interface *vlan_interface*

[Parameter]

vlan_interface : VLAN interface

[Initial value]

none

[Input mode]

RIP mode, RIPng mode

[Description]

The specified VLAN interface will only receive RIP packets, and will not transmit RIP packets.

However, RIP packets are transmitted to the RIP router that is specified by the **neighbor** command.

7.15.11 Redistribute external route information to RIP network

[Syntax]

redistribute *kind* [**metric** *metric*]
no redistribute *kind* [**metric** *metric*]

[Parameter]

kind : Type of route

Setting value	Description
connected	Directly connected routes are redistributed.
ospf	OSPFv2 routes are redistributed. This can be selected only in RIP mode.
ospf6	OSPFv3 routes are redistributed. This can be selected only in RIPng mode.
static	Statically connected routes are redistributed.

metric : <0-16>

Metric value

[Initial value]

none

[Input mode]

RIP mode, RIPng mode

[Description]

Redistributes the specified external route information to the RIP network.

7.15.12 Set RIP-related timers

[Syntax]

timers basic *update timeout garbage*
no timers basic

[Parameter]

update : <5-2147483647>

RIP update packet transmission interval timer (seconds)

timeout : <5-2147483647>

Interval from when the route stopped being updated until that route is considered invalid (seconds)

garbage : <5-2147483647>

Interval that route information considered invalid is maintained (seconds)

[Initial value]

timers basic 30 180 120

[Input mode]

RIP mode, RIPng mode

[Description]

Sets RIP-related timers.

7.15.13 Set RIP version

[Syntax]

version *version*
no version

[Parameter]

version : <1-2>
RIP version

[Initial value]

version 2

[Input mode]

RIP mode

[Description]

Sets the RIP version.

If the **ip rip send version** command and **ip rip receive version** command are set, those settings take priority.

7.15.14 Set key chain used for RIPv2 authentication

[Syntax]

ip rip authentication key-chain *key_name* [*key_name* ...]
no ip rip authentication key-chain [*key_name* [*key_name* ...]]

[Parameter]

key_name : Key chain name

[Initial value]

none

[Input mode]

interface mode

[Description]

Specifies the key chain used for RIPv2 authentication.

You must use the **key chain** command to create a key chain in advance.

7.15.15 Set authentication method used for RIPv2

[Syntax]

ip rip authentication mode *mode*
no ip rip authentication mode [*mode*]

[Parameter]

mode : Authentication method

Setting value	Description
text	Authenticate using a simple password.
md5	Authenticate using MD5 digest.

[Initial value]

ip rip authentication mode text

[Input mode]

interface mode

[Description]

Sets the authentication method used for RIPv2.

7.15.16 Set password used for RIPv2 authentication

[Syntax]

ip rip authentication string *password*
no ip rip authentication string [*password*]

[Parameter]

password : Authentication password

[Initial value]

none

[Input mode]

interface mode

[Description]

Sets the password used for RIPv2 authentication.

7.15.17 Set operation when a route whose metric is 0 is received

[Syntax]

ip rip metric-zero-accept *mode*
no ip rip metric-zero-accept

[Parameter]

mode : Operation when a route whose metric is 0 is received

Setting value	Description
enable	If a route whose metric is 0 is received, it is applied to the routing information.
disable	If a route whose metric is 0 is received, it is not applied to the routing information.

[Initial value]

ip rip metric-zero-accept disable

[Input mode]

interface mode

[Description]

Sets the operation when a route whose metric is 0 is received.

7.15.18 Set RIP packet reception

[Syntax]

ip rip receive-packet *mode*
no ip rip receive-packet [*mode*]

[Parameter]

mode : RIP packet reception

Setting value	Description
enable	Receive RIP packets at the applicable interface.
disable	Don't receive RIP packets at the applicable interface.

[Initial value]

ip rip receive-packet enable

[Input mode]

interface mode

[Description]

Specifies whether RIP packets are received.

7.15.19 Set RIP version that can be received

[Syntax]

ip rip receive version *version* [*version*]
no ip rip receive version [*version* [*version*]]

[Parameter]

version : RIP version

Setting value	Description
1	RIPv1 packets will be received.
2	RIPv2 packets will be received.

[Initial value]

None (follow the setting of the "version" command)

[Input mode]

interface mode

[Description]

Specifies the RIP version that can be received at the applicable interface.

The setting of this command takes priority over the setting of the **version** command.

7.15.20 Set RIP packet transmission

[Syntax]

ip rip send-packet *mode*
no ip rip send-packet [*mode*]

[Parameter]

mode : RIP packet transmission

Setting value	Description
enable	Transmit RIP packets at the applicable interface.
disable	Don't transmit RIP packets at the applicable interface.

[Initial value]

ip rip send-packet enable

[Input mode]

interface mode

[Description]

Specifies whether RIP packets are transmitted.

7.15.21 Set RIP version that can be transmitted

[Syntax]

ip rip send version *version* [*version*]
no ip rip send version [*version* [*version*]]

[Parameter]

version : RIP version

Setting value	Description
1	Transmit RIPv1 packets.
1-compatible	Transmit RIPv2 packets to broadcast address.
2	Transmit RIPv2 packets.

[Initial value]

None (follow the setting of the "version" command)

[Input mode]

interface mode

[Description]

Specifies the RIP version that can be transmitted at the applicable interface.

The setting of this command takes priority over the setting of the **version** command.

7.15.22 Set split horizon (IPv4)

[Syntax]

ip rip split-horizon *mode*
no ip rip split-horizon

[Parameter]

mode : Split horizon

Setting value	Description
enable	Enable split horizon.
disable	Disable split horizon.

[Initial value]

ip rip split-horizon enable

[Input mode]

interface mode

[Description]

Specifies whether split horizon is enabled or disabled.

7.15.23 Set poison reverse (IPv4)

[Syntax]

ip rip poison-reverse *mode*
no ip rip poison-reverse

[Parameter]

mode : Poison reverse

Setting value	Description
enable	Enable poison reverse.
disable	Disable poison reverse.

[Initial value]

ip rip poison-reverse enable

[Input mode]

interface mode

[Description]

Specifies whether to disable or enable poison reverse.

7.15.24 Set metric for offsetting route information of the transmitted and received RIPng packets

[Syntax]

ipv6 rip metric-offset *metric*
no ipv6 rip metric-offset *metric*

[Parameter]

metric : <1-16>
Metric value

[Initial value]

none

[Input mode]

interface mode

[Description]

Adds the specified metric value to the route information of the RIPng packets that are transmitted and received by the applicable interface.

[Note]

This command cannot be used if the stack function is enabled.

7.15.25 Set split horizon (IPv6)

[Syntax]

ipv6 rip split-horizon *mode*
no ipv6 rip split-horizon

[Parameter]

mode : Split horizon

Setting value	Description
enable	Enable split horizon.
disable	Disable split horizon.

[Initial value]

ipv6 rip split-horizon enable

[Input mode]

interface mode

[Description]

Specifies whether split horizon is enabled or disabled.

[Note]

This command cannot be used if the stack function is enabled.

7.15.26 Set poison reveerse (IPv6)

[Syntax]

ipv6 rip poison-reverse *mode*
no ipv6 rip poison-reverse

[Parameter]

mode : Poizon reverse

Setting value	Description
enable	Enable poison reverse.
disable	Disable poison reverse.

[Initial value]

ipv6 rip poison-reverse enable

[Input mode]

interface mode

[Description]

Specifies whether to disable or enable poison reverse.

[Note]

This command cannot be used if the stack function is enabled.

7.15.27 Set RIPng

[Syntax]

ipv6 router rip
no ipv6 router rip

[Initial value]

Disabled

[Input mode]

interface mode

[Description]

Enables RIPng for the applicable interface.

[Note]

This command cannot be used if the stack function is enabled.

7.15.28 Generate key chain used for RIPv2 authentication

[Syntax]

key chain *key_name*
no key chain *key_name*

[Parameter]

key_name : Key chain name

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Generates a key chain used for RIPv2 authentication. Also transitions to key chain mode in order to generate key information for the key chain.

To transition from key chain key mode to global configuration mode, use the **exit** command.

7.15.29 Generate key for registration in key chain

[Syntax]

key *number*

no key *number*

[Parameter]

number : <0-2147483647>

Key number

[Initial value]

none

[Input mode]

key chain mode

[Description]

Generates a key for registration in the key chain. Also transitions to key chain key mode in order to specify key information for the key chain.

To transition from key chain key mode to global configuration mode, use the **exit** command.

7.15.30 Set password used for RIPv2 authentication

[Syntax]

key-string *password*
no key-string

[Parameter]

password : Password (80 characters or less)

[Initial value]

none

[Input mode]

key chain key mode

[Description]

Sets the password used for RIPv2 authentication.

7.15.31 Set the term in which key received for use in RIPv2 authentication is accepted as valid

[Syntax]

accept-lifetime *start end*
no accept-lifetime

[Parameter]

start : Day and time at which to start accepting the "time date" key as valid

Setting value	Description
time	<0-23>:<0-59>:<0-59> Time at which to start accepting the key as valid
date	<1-31> month <1993-2035> Date on which to start receiving the key as valid "month" is the first three characters of the English name of the month

end : Day and time at which to stop accepting the key as valid, or the duration of the term of validity

Setting value	Description
time date	Date and time at which to stop receiving the key as valid The same format as the above "start" parameter
duration	<1-2147483646> Duration during which to accept the key as valid, starting from the time and date specified by the above "start" parameter
infinite	Unlimited term of validity

[Initial value]

none

[Input mode]

key chain key mode

[Description]

Sets the term in which a key received for use in RIPv2 authentication is accepted as valid.

[Example]

Create a key chain named "KeyName" and specify the password "yamaha" for key number 100.

Set this key's term of validity to be from April 1, 2020 at 12:00:00 until March 31, 2025 at 11:59:59.

```
SWX3220(config)# key chain KeyName
SWX3220(config-keychain)# key 100
SWX3220(config-keychain-key)# key-string yamaha
SWX3220(config-keychain-key)# accept-lifetime 12:0:0 1 apr 2020 11:59:59 31 mar 2025
```

7.15.32 Set the term in which key for use in RIPv2 authentication is valid for transmission

[Syntax]

send-lifetime *start end*
no send-lifetime

[Parameter]

start : Day and time at which to start using the "time date" key as valid for transmission

Setting value	Description
time	<0-23>:<0-59>:<0-59> Time at which to start transmitting the key as valid
date	<1-31> month <1993-2035> Date on which to start transmitting the key as valid "month" is the first three characters of the English name of the month

end : Day and time at which to stop transmitting the key as valid, or the duration of the term of validity

Setting value	Description
time date	Date and time at which to stop transmitting the key as valid The same format as the above "start" parameter
duration	<1-2147483646> Duration during which to transmit the key as valid, starting from the time and date specified by the above "start" parameter
infinite	Unlimited term of validity

[Initial value]

none

[Input mode]

key chain key mode

[Description]

Sets the term in which a key is transmitted as valid for use in RIPv2 authentication.

[Example]

Create a key chain named "KeyName" and specify the password "yamaha" for key number 100.

Set this key's term of validity for transmission to be from April 1, 2020 at 12:00:00 until March 31, 2025 at 11:59:59.

```
SWX3220(config)# key chain KeyName
SWX3220(config-keychain)# key 100
SWX3220(config-keychain-key)# send-lifetime 12:0:0 1 apr 2020 11:59:59 31 mar 2025
```

7.15.33 Delete route information from the RIP routing table (IPv4)

[Syntax]

clear ip rip route *type*

[Parameter]

type : Type of route

Setting value	Description
A.B.C.D/M	Deletes the route information matching the specified prefix from the RIP routing table.
all	Deletes all routes from the RIP routing table.
connected	Deletes directly connected routes from the RIP routing table.
ospf	Deletes OSPF routes from the RIP routing table.
rip	Deletes RIP routes from the RIP routing table.
static	Deletes static routes from the RIP routing table.

[Input mode]

privileged EXEC mode

[Description]

Deletes the specified type of route information from the RIP routing table.

7.15.34 Clear RIP statistical information

[Syntax]

clear ip rip statistics [*vlan_interface*]

[Parameter]

vlan_interface : VLAN interface

[Input mode]

privileged EXEC mode

[Description]

Clears the RIP statistical information. If the *vlan_interface* parameter is specified, RIP statistical information is cleared only for that VLAN interface.

7.15.35 Delete route information from the RIPng routing table (IPv6)

[Syntax]

clear ipv6 rip route *type*

[Parameter]

type : Type of route

Setting value	Description
X:X::X:X/M	Deletes the route information matching the specified prefix from the RIPng routing table.
all	Deletes all routes from the RIPng routing table.
connected	Deletes directly connected routes from the RIPng routing table.
ospf6	Deletes OSPFv3 routes from the RIPng routing table.
rip	Deletes RIPng routes from the RIPng routing table.
static	Deletes static routes from the RIPng routing table.

[Input mode]

privileged EXEC mode

[Description]

Deletes the specified type of route information from the RIPng routing table.

[Note]

This command cannot be used if the stack function is enabled.

7.15.36 Show RIP settings and status (IPv4)

[Syntax]

show ip protocols rip

[Input mode]

privileged EXEC mode

[Description]

Shows the RIP settings and status.

7.15.37 Show RIPng settings and status (IPv6)

[Syntax]

show ipv6 protocols rip

[Input mode]

privileged EXEC mode

[Description]

Shows the RIPng settings and status.

[Note]

This command cannot be used if the stack function is enabled.

7.15.38 Show RIP routing table (IPv4)

[Syntax]

show ip rip

[Input mode]

privileged EXEC mode

[Description]

Shows the RIP routing table.

7.15.39 Show RIPng routing table (IPv6)

[Syntax]

show ipv6 rip

[Input mode]

privileged EXEC mode

[Description]

Shows the RIPng routing table.

[Note]

This command cannot be used if the stack function is enabled.

7.15.40 Show RIP status for each interface (IPv4)

[Syntax]

show ip rip interface [*vlan_interface*]

[Parameter]

vlan_interface	:	VLAN interface

[Input mode]

privileged EXEC mode

[Description]

Shows the RIP status for each interface.

If VLAN interface is specified, only the RIP status for the specified VLAN interface is shown.

7.15.41 Show RIPng status for each interface (IPv6)

[Syntax]

show ipv6 rip interface [*vlan_interface*]

[Parameter]

vlan_interface	:	VLAN interface

[Input mode]

privileged EXEC mode

[Description]

Shows the RIPng status for each interface.

If VLAN interface is specified, only the RIPng status for the specified VLAN interface is shown.

[Note]

This command cannot be used if the stack function is enabled.

7.15.42 Show RIP statistical information

[Syntax]

show ip rip statistics [*vlan_interface*]

[Parameter]

vlan_interface	:	VLAN interface

[Input mode]

privileged EXEC mode

[Description]

Shows RIP statistical information.

If VLAN interface is specified, the RIP statistical information for the specified VLAN interface is shown.

7.16 VRRP

7.16.1 Move to VRRP mode

[Syntax]

router vrrp *vrid ifname*
no router vrrp *vrid ifname*

[Parameter]

vrid	:	<1-255>
		Virtual router ID
ifname	:	VLAN interface name

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Transition to a mode for making VRRP settings.

If the applicable virtual router has not been generated, it will be generated.

If this command is executed with the "no" syntax, all settings related to the applicable virtual router will be deleted.

[Note]

This command cannot be used if the stack function is enabled.

[Example]

Generate virtual router #1 on VLAN #1, and transition to VRRP mode.

```
SWX3220)#configure terminal
SWX3220(config)#router vrrp 1 vlan1
SWX3220(config-router)#
```

Delete virtual router #1 of VLAN #1.

```
SWX3220)#configure terminal
SWX3220(config)#no router vrrp 1 vlan1
```

7.16.2 Move to VRRP mode(IPv6)

[Syntax]

router ipv6 vrrp *vrid ifname*

no router ipv6 vrrp *vrid ifname*

[Parameter]

vrid	:	<1-255>
		Virtual router ID
ifname	:	VLAN interface name

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Transition to a mode for making VRRP settings.

If the applicable virtual router has not been generated, it will be generated.

If this command is executed with the "no" syntax, all settings related to the applicable virtual router will be deleted.

[Note]

This command cannot be used if the stack function is enabled.

[Example]

Generate virtual router #1 on VLAN #1, and transition to VRRP mode(IPv6).

```
SWX3220)#configure terminal
SWX3220(config)#router ipv6 vrrp 1 vlan1
SWX3220(config-router)#
```

Delete virtual router #1 of VLAN #1.

```
SWX3220)#configure terminal
SWX3220(config)#no router ipv6 vrrp 1 vlan1
```

7.16.3 Set advertisement packet transmission interval

[Syntax]

advertisement-interval *interval*
no advertisement-interval

[Parameter]

interval	:	<5-4095>
		Advertisement packet transmission interval (1/100 seconds)

[Initial value]

advertisement-interval 100

[Input mode]

VRRP mode

[Description]

Sets the interval at which advertisement packets are transmitted.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be set only if the virtual router is disabled.

This command cannot be used if the stack function is enabled.

[Example]

Specify 5 seconds (500) as the interval at which advertisement packets are transmitted.

```
SWX3220(config-router)#advertisement-interval 500
```

7.16.4 Set circuit failover

[Syntax]

circuit-failover *ifname value*
no circuit-failover *ifname value*

[Parameter]

ifname : Name of VLAN interface or physical interface being monitored

value : <1-253>

Value subtracted from the priority order of the virtual router

[Initial value]

none

[Input mode]

VRRP mode

[Description]

Specifies the circuit failover setting.

If the interface being monitored goes down, the specified value is subtracted from the priority order of the virtual router.

If you specify this value so that subtracting it from the priority order of the virtual router causes it to fall below the priority order of the backup router, it will operate as the backup router when the monitored interface goes down.

If the interface being monitored recovers, the priority order of the virtual router also returns to the value prior to the subtraction.

If this command is executed with the "no" syntax, the setting is deleted.

[Note]

This command can be set only if the virtual router is disabled.

Only one monitored interface can be specified for each virtual router.

This command cannot be used if the stack function is enabled.

[Example]

Specify that when VLAN #20 goes down, its priority order is lowered by 10.

```
SWX3220(config-router)#circuit-failover vlan20 10
```

7.16.5 Enable/disable virtual router

[Syntax]

virtual-router *switch*
no virtual-router

[Parameter]

switch : Virtual router operation

Setting value	Description
enable	Enable virtual router
disable	Disable virtual router

[Initial value]

virtual-router disable

[Input mode]

VRRP mode

[Description]

Enables/disables the virtual router.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command cannot be used if the stack function is enabled.

[Example]

Enable the virtual router.

```
SWX3220(config-router)#virtual-router enable
```

7.16.6 Set preempt mode

[Syntax]

preempt-mode *switch*
no preempt-mode

[Parameter]

switch : Preempt mode setting

Setting value	Description
enable	Enable preempt mode
disable	Disable preempt mode

[Initial value]

preempt-mode enable

[Input mode]

VRRP mode

[Description]

Sets preempt mode.

If preempt mode is enabled, the higher-priority router is always the master router.

If preempt mode is disabled, and a master router already exists, the higher-priority router is the backup router even if it is a virtual router.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be set only if the virtual router is disabled.

The preempt mode settings of the master router and the backup router must be consistent.

This command cannot be used if the stack function is enabled.

[Example]

Disable preempt mode.

```
SWX3220(config-router)#preempt-mode disable
```

7.16.7 Set virtual router's priority

[Syntax]

priority *priority*
no priority

[Parameter]

priority : <1-255>

Priority

[Initial value]

priority 255 (if the **virtual-ip** command is set with the "owner" keyword)

priority 100 (if the **virtual-ip** command is not set with the "owner" keyword)

[Input mode]

VRRP mode

[Description]

Set the virtual router's priority order.

If the **virtual-ip** command is set with the "owner" keyword, this cannot be changed from the default value (255).

If the **virtual-ip** command is not set with the "owner" keyword, this can be set in the range of 1-254.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be set only if the virtual router is disabled.

This command cannot be used if the stack function is enabled.

[Example]

Set the virtual router's priority order to 150.

```
SWX3220(config-router)#priority 150
```

7.16.8 Set virtual IP address

[Syntax]

virtual-ip *ip_address* [owner]
no virtual-ip

[Keyword]

owner	:	Specify this only if setting the same IP address as the IP address of the VLAN interface specified by the router vrrp command.

[Parameter]

ip_address	:	A.B.C.D IP address

[Initial value]

no virtual-ip

[Input mode]

VRRP mode

[Description]

Set the virtual IP address.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be set only if the virtual router is disabled.

Note that if you use the same IP address as the VLAN interface, it is not possible to access the various servers that are running on this switch.

This command cannot be used if the stack function is enabled.

[Example]

Set the virtual IP address to 192.168.100.1. (if different than the IP address of the VLAN interface)

```
SWX3220(config-router)#virtual-ip 192.168.100.1
```

Set the virtual IP address to 192.168.100.1. (if the same as the IP address of the VLAN interface)

```
SWX3220(config-router)#virtual-ip 192.168.100.1 owner
```

7.16.9 Set virtual IP address(IPv6)

[Syntax]

virtual-ipv6 *ipv6_address* [owner]
no virtual-ipv6

[Keyword]

owner	:	Specify this only if setting the same IPv6 address as the IPv6 address of the VLAN interface specified by the router vrrp command.

[Parameter]

ipv6_address	:	X:X::X:X IPv6 address

[Initial value]

no virtual-ipv6

[Input mode]

VRRP mode(IPv6)

[Description]

Set the virtual IP address.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be set only if the virtual router is disabled.

Note that if you use the same IPv6 address as the VLAN interface, it is not possible to access the various servers that are running on this switch.

This command cannot be used if the stack function is enabled.

[Example]

Set the virtual IP address to fe80::10:1. (if different than the IP address of the VLAN interface)

```
SWX3220(config-router)#virtual-ipv6 fe80::10:1
```

Set the virtual IP address to fe80::10:1. (if the same as the IP address of the VLAN interface)

```
SWX3220(config-router)#virtual-ipv6 fe80::10:1 owner
```

7.16.10 Show VRRP information

[Syntax]

show vrrp [*vrid*] [*ifname*]

[Parameter]

vrid	:	<1-255> Virtual router ID
ifname	:	VLAN interface name

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the VRRP settings and status.

[Example]

Show information for virtual router #1 of VLAN #1.

```
SWX3220#show vrrp 1 vlan1
VRRP Version: 3
VMAC enabled
Backward Compatibility disabled

Address family IPv4
VRRP Id: 1 on interface: vlan1
 State: AdminUp   - Master
 Virtual IP address: 192.168.100.228 (Not-owner)
 Operational primary IP address: 192.168.100.240
```

```
 Operational master IP address: 192.168.100.240
 Priority not configured; Current priority: 100
 Advertisement interval: 100 centi sec
 Master Advertisement interval: 100 centi sec
 Skew time: 60 centi sec
 Accept mode: FALSE
 Preempt mode: TRUE
 Monitored circuit: vlan10, Priority Delta: 30, Status: UP
 Multicast membership on IPv4 interface vlan1: JOINED
 V2-Compatible: FALSE
```

7.16.11 Show VRRP information(IPv6)

[Syntax]

show vrrp ipv6 [*vrid*] [*ifname*]

[Parameter]

vrid	:	<1-255> Virtual router ID
ifname	:	VLAN interface name

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the VRRP settings and status.

[Example]

Show information for virtual router #1 of VLAN #1.

```
SWX3220#show vrrp ipv6 1 vlan1
VRRP Version: 3
VMAC enabled
Address family IPv6
VRRP Id: 1 on interface: vlan1
 State: AdminUp   - Master
 Virtual IP address: fe80::1:1 (Not-owner)
 Operational primary IP address: fe80::ae44:f2ff:fe11:1111
 Operational master IP address: fe80::ae44:f2ff:fe11:1111
 Priority is 100
 Advertisement interval: 100 centi sec
 Master Advertisement interval: 100 centi sec
 Skew time: 60 centi sec
 Accept mode: FALSE
 Preempt mode: TRUE
 Multicast membership on IPv6 interface  vlan1: JOINED
 V2-Compatible: FALSE
```

7.16.12 Show VRRP statistical information

[Syntax]

show vrrp statistics [*vrid*] [*ifname*]

[Parameter]

vrid	:	<1-255> Virtual router ID
ifname	:	VLAN interface name

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows VRRP statistical information.

[Example]

Show statistical information for virtual router #1 of VLAN #1.

```
SWX3220#show vrrp statistics 1 vlan1
VRRP Version: 3
VMAC enabled
Backward Compatibility disabled

Address family IPv4
VRRP Id: 1 on interface: vlan1
 Checksum Errors: 0
 Version Errors: 0
 VRid Errors: 0
 Master Transitions: 1
 Advertisements Rcvd: 3
 Pkts Rcvd with IP TTL Errors: 0
 Pkts Rcvd with Zero Priority: 0
 Pkts Sent with Zero Priority: 0
 Pkts Rcvd with Invalid TYPE: 0
 Pkts Rcvd with Packet Length Errors: 0
 Pkts Rcvd with IP Count Mismatch: 0
 Discontuinity Time: (0) 0:00:00.00
 Refresh Rate: 1000 ms
```

7.16.13 Show VRRP statistical information(IPv6)

[Syntax]

show vrrp ipv6 statistics [*vrid*] [*ifname*]

[Parameter]

vrid	:	<1-255> Virtual router ID
ifname	:	VLAN interface name

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows VRRP statistical information.

[Example]

Show statistical information for virtual router #1 of VLAN #1.

```
SWX3220#show vrrp ipv6 statistics 1 vlan1
VRRP Version: 3
VMAC enabled
Address family IPv6
VRRP Id: 1 on interface: vlan1
 Checksum Errors: 0
 Version Errors: 0
 VRid Errors: 0
 Master Transitions: 1
 Advertisements Rcvd: 3
 Pkts Rcvd with IP TTL Errors: 0
 Pkts Rcvd with Zero Priority: 0
 Pkts Sent with Zero Priority: 0
 Pkts Rcvd with Invalid TYPE: 0
 Pkts Rcvd with Packet Length Errors: 0
 Pkts Rcvd with IP Count Mismatch: 0
 Discontuinity Time: (0) 0:00:00.00
 Refresh Rate: 1000 ms
```

7.17 PBR

7.17.1 Generating a route map

[Syntax]

route-map *route-map-id* [*action*] [*seq_num*]
no route-map *route-map-id* [[*action seq_num*]|*seq_num*]

[Parameter]

action : Specifying operations for packets that match the application parameters

Setting value	Description
permit	Permit (execute “set” processing contents)—considered as “permit” when omitted
deny	Deny (forward using the usual routing)

route-map-id : <1-4094>

Route map ID

seq_num : <1-65535>

Entry sequence number (entry position in the route map)

[Initial value]

none

[Input mode]

global configuration mode

[Description]

If a route map does not exist for the specified ID, generate a route map and entries, and switch to route map mode.

If an existing ID or sequence number is specified, the unit will not generate them and will instead switch to edit mode using the existing route map and entries.

Up to 64 entries can be set for a route map.

To apply the generated route map, run the “ip policy route-map” (or “ipv6 policy route-map”) command in interface mode.

When “permit/deny” and thereafter is specified using the “no” syntax, entries matching all parameters will be deleted. As a result, when all entries have been deleted, the route map itself will be deleted.

When only “route-map-id” is specified using the “no” syntax, route maps for which the IDs match (and all entries) will be deleted.

[Note]

If seq_num is omitted, it will be appended to the entry. The entry sequence number generated at this time will be set to the sequencer number of the last entry plus 10. If the seq_num is omitted when the route map is generated, the sequence number will be set to “10”. Also, if the number plus 10 is greater than 65535, an error will occur.

Sequence numbers are processed in the order of packet receive time. If multiple entries exist in a single route map, they are processed in order of sequence number, and the processing ends when the parameters are met.

As an implicit “deny” entry exists in the route map, if none of the entry parameters match, forwarding is performed via the usual routing function.

Entries cannot be added or edited for route maps that have been applied to an interface, nor can they be deleted with the "no" syntax. You must clear the application before performing the operation.

[Example]

This generates a route map with ID 100, which has a permit entry with a sequence number of 10.

```
SWX3220(config)#route-map 100 permit 10
SWX3220(config-route-map)#
```

7.17.2 Set description to the route map

[Syntax]

description *line*

no description

[Parameter]

line	:	Single-byte alphanumeric characters and single-byte symbols (32characters or less) Route map description text

[Initial value]

none

[Input mode]

Route map mode

[Description]

Sets the route map description text.

If this is executed with the "no" syntax, the description is deleted from the route map.

[Note]

If a description has already been set, any succeeding descriptions will overwrite that description.

[Example]

Creates a route map and adds the “Test” description.

```
SWX3220(config)#route-map 1
SWX3220(config-route-map)#description Test
```

7.17.3 Parameter settings for application to route map entries

[Syntax]

match access-list *acl-id*
no match access-list [*acl-id*]

[Parameter]

acl-id	:	<1-4000> IPv4, MAC or IPv6 access list ID

[Initial value]

none

[Input mode]

Route map mode

[Description]

Sets the application parameters for route map entries.

If this command is executed with the "no" syntax, the application parameters are deleted from the route map entry.

[Note]

For “permit” entries, the processing contents (set) will be executed if the received packet does not match the access list.

For “deny” entries, forwarding will be performed by means of the usual routing function if the received packet does not match the access list.

If the application parameter (match) is not configured for the entry, this will be regarded as an invalid entry.

Also, only one application parameter (match) will be able to be set for the entry, and an error will occur if the command is executed in the case where application parameters are already set.

Specifying TCP flags for an IPv4 access list is not supported. A TCP flag will be ignored if it is specified.

Policy-based routing (PBR) does not support multicast or broadcast traffic. Operations cannot be guaranteed if the access list contains a multicast address or broadcast address.

[Example]

Create a route map used to forward communications from the segment of source 192.168.1.0/24 to the next hop 10.0.0.1.

```
SWX3220(config)#access-list 1 permit any 192.168.1.0 0.0.0.255 any
SWX3220(config)#route-map 100 permit 10
```

```
SWX3220(config-route-map)#match access-list 1
SWX3220(config-route-map)#set ip next-hop 10.0.0.1
SWX3220(config-route-map)#exit
```

7.17.4 Processing content (IPv4 forwarding destination) settings for route map entries

[Syntax]

set ip next-hop *ip_address*
no set ip next-hop [*ip_address*]

[Parameter]

ip_address	:	A.B.C.D IPv4 address for forwarding

[Initial value]

none

[Input mode]

Route map mode

[Description]

Sets the processing content (IPv4 forwarding destination) for route map entries.

If this command is executed with the "no" syntax, deletes the processing content (IPv4 forwarding destination) for route map entries.

[Note]

On entries with “set ip next-hop” settings, packets received that match the application parameters (match) will be forwarded to the next hop.

However, when the IPv4 address of the next hop does not exist in the ARP cache, packets are forwarded using the usual routing function.

Only one processing content (set) can be set for the entry, and an error will occur if the command is executed in the case where processing contents are already set.

If the processing content (set) is not configured for the entry, the entry will be regarded as invalid. Note that “set” may be omitted for “deny” entries.

“set ip next-hop” can also be set for “deny” entries, but the processing cannot be executed.

[Example]

This creates a route map used to forward communications from the segment of source 192.168.1.0/24 to the next hop 10.0.0.1.

```
SWX3220(config)#access-list 1 permit any 192.168.1.0 0.0.0.255 any
SWX3220(config)#route-map 100 permit 10
SWX3220(config-route-map)#match access-list 1
SWX3220(config-route-map)#set ip next-hop 10.0.0.1
SWX3220(config-route-map)#exit
```

7.17.5 Processing content (IPv6 forwarding destination) settings for route map entries

[Syntax]

set ipv6 next-hop *ipv6_address*
no set ipv6 next-hop [*ipv6_address*]

[Parameter]

ipv6_address	:	X:X::X:X IPv6 address for forwarding

[Initial value]

none

[Input mode]

Route map mode

[Description]

Sets the processing content (IPv6 forwarding destination) for route map entries.

If this command is executed with the "no" syntax, deletes the processing content (IPv6 forwarding destination) for route map entries.

[Note]

On entries with “set ipv6 next-hop” settings, packets received that match the application parameters (match) will be forwarded to the next hop.

However, when the IPv6 address of the next hop does not exist in the ARP cache, packets are forwarded using the usual routing function.

Only one processing content (set) can be set for the entry, and an error will occur if the command is executed in the case where processing contents are already set.

If the processing content (set) is not configured for the entry, the entry will be regarded as invalid. Note that “set” may be omitted for “deny” entries.

“set ipv6 next-hop” can also be set for “deny” entries, but the processing cannot be executed.

[Example]

This creates a route map used to forward communications from the segment of source 3ffe:506::/32 to the next hop 2001:db8:1::1.

```
SWX3220(config)#access-list 3001 permit 3ffe:506::/32
SWX3220(config)#route-map 100 permit 10
SWX3220(config-route-map)#match access-list 3001
SWX3220(config-route-map)#set ipv6 next-hop 2001:db8:1::1
SWX3220(config-route-map)#exit
```

7.17.6 Processing content (packet discard) settings for route map entries

[Syntax]

set interface null
no set interface [**null**]

[Input mode]

Route map mode

[Description]

Sets the processing content (packet discard) for route map entries.

If this command is executed with the "no" syntax, the processing content (packet discard) is deleted from the route map entry.

[Note]

On entries with “set interface null” settings, packets received that match the application parameters (match) will be discarded.

Only one processing content (set) can be set for the entry, and an error will occur if the command is executed in the case where processing contents are already set.

If the processing content (set) is not configured for the entry, the entry will be regarded as invalid. Note that “set” may be omitted for “deny” entries.

“set interface null” can also be set for “deny” entries, but the processing cannot be executed.

[Example]

This creates a route map used to forward communications from the segment of source 192.168.1.0/24 to the next hop 10.0.0.1, discarding everything else.

```
SWX3220(config)#access-list 1 permit any 192.168.1.0 0.0.0.255 any
SWX3220(config)#access-list 2 permit any any any
SWX3220(config)#route-map 100 permit 10
SWX3220(config-route-map)#match access-list 1
SWX3220(config-route-map)#set ip next-hop 10.0.0.1
SWX3220(config-route-map)#exit
SWX3220(config)#route-map 100 permit 20
SWX3220(config-route-map)#match access-list 2
SWX3220(config-route-map)#set interface null
SWX3220(config-route-map)#exit
```

7.17.7 Applying a route map to the interface (for IPv4)

[Syntax]

ip policy route-map *route-map-id*
no ip policy route-map [*route-map-id*]

[Parameter]

route-map-id : <1-4094>

Route map ID

[Initial value]

none

[Input mode]

interface mode

[Description]

This applies the route map for IPv4 to the interface.

If this is executed with the "no" syntax, the application of the route map is cleared from the interface.

[Note]

The types of interfaces to which this can be adapted are as follows.

- VLAN interface

Route maps that can be applied to an interface include up to one for IPv4 and IPv6 each. If a route map has already been applied, an error will occur.

An error will also occur if no valid entries exist.

The conditions for valid entries are shown below.

- “match” must be set
  - An IPv4 or MAC access list must be specified
  - At least one “permit” entry must exist in the access list
- In the case of “permit”, “set” must be set*
  - “ip next-hop” or “interface null” must be specified

*In the case of “deny”, “set” does not need to be set (it will be ignored if it has been configured)

[Example]

This applies “vlan10” to the route map used to forward communications from the segment of source 192.168.1.0/24 to the next hop 10.0.0.1.

```
SWX3220(config)#access-list 1 permit any 192.168.1.0 0.0.0.255 any
SWX3220(config)#route-map 100 permit 10
SWX3220(config-route-map)#match access-list 1
SWX3220(config-route-map)#set ip next-hop 10.0.0.1
SWX3220(config-route-map)#exit
SWX3220(config)#interface vlan10
SWX3220(config-if)#ip policy route-map 100
```

7.17.8 Applying a route map to the interface (for IPv6)

[Syntax]

ipv6 policy route-map *route-map-id*
no ipv6 policy route-map [*route-map-id*]

[Parameter]

route-map-id : <1-4094>

Route map ID

[Initial value]

none

[Input mode]

interface mode

[Description]

This applies the route map for IPv6 to the interface.

If this is executed with the "no" syntax, the application of the route map is cleared from the interface.

[Note]

The types of interfaces to which this can be adapted are as follows.

- VLAN interface

Route maps that can be applied to an interface include up to one for IPv4 and IPv6 each. If a route map has already been applied, an error will occur.

An error will also occur if no valid entries exist.

The conditions for valid entries are shown below.

- “match” must be set
  - An IPv6 access list must be specified
  - At least one “permit” entry must exist in the access list
- In the case of “permit”, “set” must be set*
  - “ipv6 next-hop” or “interface null” must be specified

*In the case of “deny”, “set” does not need to be set (it will be ignored if it has been configured)

This command cannot be used if the stack function is enabled.

[Example]

This applies “vlan10” to the route map used to forward communications from the segment of source 3ffe:506::/32 to the next hop 2001:db8:1::1.

```
SWX3220(config)#access-list 3001 permit 3ffe:506::/32
SWX3220(config)#route-map 100 permit 10
SWX3220(config-route-map)#match access-list 3001
SWX3220(config-route-map)#set ipv6 next-hop 2001:db8:1::1
SWX3220(config-route-map)#exit
SWX3220(config)#interface vlan10
SWX3220(config-if)#ipv6 policy route-map 100
```

7.17.9 Enable/disable PBR function

[Syntax]

pbr *switch*
no pbr

[Parameter]

switch : Behavior of the PBR function

Setting value	Description
enable	Enable the PBR function
disable	Disable the PBR function

[Initial value]

pbr enable

[Input mode]

global configuration mode

[Description]

Enables the PBR function.

If "disable" is specified, the PBR function is disabled.

If this command is executed with the "no" syntax, the setting returns to the default value (same as when specifying “enable”).

[Note]

Even when the function is disabled, the PBR-related settings will remain, making it possible to restore the previous state when the function is re-enabled.

[Example]

Enables the PBR function.

```
SWX3220(config)#pbr enable
```

7.17.10 Show route map information

[Syntax]

show route-map [*route-map-id*]

[Parameter]

route-map-id	:	<1-4094> Rute map ID

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows information for the registered route map.

When “route-map-id” has been omitted, information for all route maps will be displayed.

[Example]

Shows information for all route maps.

```
SWX3220#show route-map
Route Map 100
  Description:
  10 permit
    Match clauses:
      access-list 1
    Set clauses:
      ip next-hop 10.0.0.1
  20 permit
    Match clauses:
      access-list 2
    Set clauses:
      interface null
Route Map 200
  Description: PBR_IPV6
  10 deny
    Match clauses:
      access-list 3001
    Set clauses:
```

7.17.11 Show IPv4 PBR information

[Syntax]

show ip route pbr

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Displays the route map information to be applied as IPv4 for each interface.

[Note]

Displays all entries of the applied route map (including invalid entries and entries for which the next hop does not exist in the ARP cache).

[Example]

Displays the route map information to be applied as IPv4 for each interface.

```
SWX3220#show ip route pbr
Policy Routing
vlan10
  Route Map 100, PBR1
    10 permit
      match access-list 1
      set ip next-hop 10.0.0.1
    20 permit
      match access-list 2
      set interface null
vlan20
  Route Map 200
    10 deny
      match access-list 2001
```

7.17.12 Show IPv6 PBR information

[Syntax]

show ipv6 route pbr

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Displays the route map information to be applied as IPv6 for each interface.

[Note]

Displays all entries of the applied route map (including invalid entries and entries for which the next hop does not exist in the ARP cache).

This command cannot be used if the stack function is enabled.

[Example]

Displays the route map information to be applied as IPv6 for each interface.

```
SWX3220#show ipv6 route pbr
Policy Routing
vlan10
  Route Map 100, PBR1
    10 permit
      match access-list 3001
      set ip next-hop 2001:db8:1::1
    20 permit
      match access-list 3002
      set interface null
vlan20
  Route Map 200
    10 deny
      match access-list 3003
```

Chapter 8

IP multicast control

8.1 IP multicast basic settings

8.1.1 Set IP multicast routing

[Syntax]

ip multicast-routing
no ip multicast-routing

[Initial value]

no ip multicast-routing

[Input mode]

global configuration mode

[Description]

Enables IP multicast routing.

If this command is executed with the "no" syntax, the IP multicast routing is disabled.

[Example]

Enable the IP multicast routing.

```
SWX3220(config)#ip multicast-routing
```

8.1.2 Set IP multicast routing (physical port)

[Syntax]

multicast *type*
no multicast

[Parameter]

type : Multicast routing operations

Setting value	Description
disable	Disables multicast routing for the applicable port.
enable	Enables multicast routing for the applicable port.

[Initial value]

multicast enable

[Input mode]

interface mode

[Description]

Disables IP multicast routing (L3 multicast packet forwarding) for the applicable physical port.

If this command is executed with the "no" syntax, or when enable is specified, IP multicast routing is enabled for the applicable physical port (default operation).

[Example]

Disable IP multicast routing on port 1.1.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#multicast disable
```

8.1.3 Set RFP check unicast routing information

[Syntax]

ip mroute *source*/*mask* [*protocol*] *rpfneighbor* [*distance*]
no ip mroute *source*/*mask* [*protocol*]

[Parameter]

source : IPv4 address of multicast sender (A.B.C.D)

mask : <0-32>

Number of mask bits

protocol : Unicast routing protocol

Setting value	Description
rip	Specifies RIP for the unicast routing protocol
ospf	Specifies OSPF for the unicast routing protocol

rpfneighbor : RPF address (A.B.C.D)

distance : <1-255>

Management distance (priority order)

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Registers the unicast routing information statically, which is used by the multicast routing protocol during RPF (Reverse Path Forwarding) checks.

If this command is executed with the "no" syntax, deletes the unicast routing information that was statically registered.

[Example]

Set the RPF neighbor for the multicast sender 10.10.10.50/24 to 10.10.10.20.

```
SWX3220(config)#ip mroute 10.10.10.50/24 10.10.10.20
```

8.1.4 Set maximum number of entries for IP multicast routing

[Syntax]

ip multicast route-limit *routelimit* [*warnlimit*]
no ip multicast route-limit

[Parameter]

routelimit : <1-2147483647>

Maximum number of IP multicast routing entries

warnlimit : <1-2147483647>

Threshold value used for warnings when the number of IP multicast routing entries have been exceeded

[Initial value]

no ip multicast route-limit

[Input mode]

global configuration mode

[Description]

Sets the maximum number of entries for IP multicast routing that can be registered in the routing information base.

If the threshold value for a warning has been set, a warning message will be output when the threshold value has been exceeded.

Set the threshold value for warnings to a value equal to or lower than the maximum number of entries for IP multicast routing.

If this command is executed with the "no" syntax, the maximum number and threshold value are both 2147483647.

[Example]

Limit the maximum number of entries for IP multicast routing to 100, and set the threshold for warning to 80.

```
SWX3220(config)#ip multicast route-limit 100 80
```

8.1.5 Show IP multicast routing information base

[Syntax]

show ip mroute [*group* [*source*] | *source* [*group*]] [*entry*] [*type*]

[Parameter]

group : Specifies the multicast group address. (A.B.C.D)

source : Specifies the IPv4 address for the multicast sender. (A.B.C.D)

entry : Sets the entries to be shown. When this is omitted, information for all entries is shown.

Setting value	Description
dense	Shows information only for entries originating from PIM-DM.
sparse	Shows information only for entries originating from PIM-SM.

type : Sets information to be shown. When this is omitted, information for each entry is shown.

Setting value	Description
count	Shows statistical information.
summary	Shows summary information.

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the IP multicast routing information base.

[Example]

Show the IP multicast routing information base.

```
SWX3220#show ip mroute

IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)

(192.168.100.2, 239.1.1.5), uptime 00:01:49, stat expires 00:01:41
Owner PIM-DM, Flags: TF
  Incoming interface: vlan1
  Outgoing interface list:
    vlan2 (1)

(192.168.100.2, 239.255.255.250), uptime 00:02:53, stat expires 00:03:09
Owner PIM-DM, Flags: TF
  Incoming interface: vlan1
  Outgoing interface list:
    vlan2 (1)

(192.168.200.2, 239.255.255.250), uptime 00:02:41, stat expires 00:03:09
Owner PIM-DM, Flags: TF
```

```
  Incoming interface: vlan2
  Outgoing interface list:
    vlan1 (1)

SWX3220#show ip mroute 239.1.1.5

IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)

(192.168.100.2, 239.1.1.5), uptime 00:02:26, stat expires 00:01:04
Owner PIM-DM, Flags: TF
  Incoming interface: vlan1
  Outgoing interface list:
    vlan2 (1)

SWX3220#show ip mroute 239.1.1.5 192.168.100.2

IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)

(192.168.100.2, 239.1.1.5), uptime 00:03:03, stat expires 00:00:27
Owner PIM-DM, Flags: TF
  Incoming interface: vlan1
  Outgoing interface list:
    vlan2 (1)

SWX3220#show ip mroute 239.1.1.5 count

IP Multicast Statistics
Total 3 routes using 372 bytes memory
Route limit/Route threshold: 2048/2048
Total NOCACHE/WRONGVIF/WHOLEPKT recv from fwd: 116/0/0
Total NOCACHE/WRONGVIF/WHOLEPKT sent to clients: 116/0/0
Immediate/Timed stat updates sent to clients: 0/69
Reg ACK recv/Reg NACK recv/Reg pkt sent: 0/0/0
Next stats poll: 00:00:27

Forwarding Counts: Pkt count/Byte count, Other Counts: Wrong If pkts
Fwd msg counts: WRONGVIF/WHOLEPKT recv
Client msg counts: WRONGVIF/WHOLEPKT/Imm Stat/Timed Stat sent
Reg pkt counts: Reg ACK recv/Reg NACK recv/Reg pkt sent

(192.168.100.2, 239.1.1.5), Forwarding: 2/1, Other: 0
  Fwd msg: 0/0, Client msg: 0/0/0/0, Reg: 0/0/0

SWX3220#show ip mroute 239.1.1.5 summary

IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)

(192.168.100.2, 239.1.1.5), 00:04:28/00:02:10, PIM-DM, Flags: TF
```

8.1.6 Show information for virtual interfaces used for IP multicasts

[Syntax]

show ip mvif *ifname*

[Parameter]

ifname	:	Interface name

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the information for virtual interfaces used for IP multicasts.

[Example]

Show the information for virtual interfaces used for IP multicasts.

```
SWX3220#show ip mvif
Interface Vif Owner TTL Local Remote Uptime
          Idx Module Address Address
          vlan1 1 PIM-DM 1 192.168.100.100 0.0.0.0 00:00:05
          vlan2 2 PIM-DM 1 192.168.200.100 0.0.0.0 00:38:25

SWX3220#show ip mvif vlan1
Interface Vif Owner TTL Local Remote Uptime
          Idx Module Address Address
vlan1     1 PIM-DM 1 192.168.100.100 0.0.0.0 00:00:44
```

8.1.7 Show RPF information

[Syntax]

show ip rpf *source*

[Parameter]

source	:	IPv4 address of multicast sender (A.B.C.D)

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows information for IPv4 address RPF (Reverse Path Forwarding) for the specified multicast sender.

[Example]

Show information for RPF (Reverse Path Forwarding) for the multicast sender of IPv4 address 192.168.100.2.

```
SWX3220#show ip rpf 192.168.100.2
  RPF information for 192.168.100.2
  RPF interface: vlan1
  RPF neighbor: 0.0.0.0
  RPF route: 192.168.100.0/24
  RPF type: unicast (connected)
  RPF recursion count: 0
  Doing distance-preferred lookups across tables
  Distance: 0
  Metric: 0
```

8.1.8 Delete entries from the IP multicast routing information base

[Syntax]

clear ip mroute *group* [*source*]
clear ip mroute statistics *group* [*source*]

[Keyword]

statistics	:	Deletes statistical information regarding the multicast routing.

[Parameter]

group	:	Multicast group address (A.B.C.D) "*" indicates all entries
source	:	IPv4 address of multicast sender (A.B.C.D)

[Input mode]

privileged EXEC mode

[Description]

Deletes specified entries from the IP multicast routing information base.

[Example]

Delete multicast group 225.1.1.1 from the IP multicast routing information base.

```
SWX3220# clear ip mroute 225.1.1.1
```

8.1.9 Set processing method for unknown multicast frames

[Syntax]

l2-unknown-mcast *mode*

[Parameter]

mode : Sets the processing method for multicast frames

Setting value	Description
discard	Discard
flood	Flood

[Initial value]

l2-unknown-mcast flood

[Input mode]

global configuration mode

[Description]

Specifies the processing method for multicast frames that are not registered in the MAC address table.

[Example]

Discard unknown multicast.

```
SWX3220(config)#l2-unknown-mcast discard
```

8.1.10 Setting the processing method for unknown multicast frames (interface)

[Syntax]

l2-unknown-mcast *mode* [**except-routing**]
no l2-unknown-mcast

[Keyword]

except-routing : Targets unknown multicast frames for routing.

[Parameter]

mode : Sets the processing method for multicast frames

Setting value	Description
discard	Discard
flood	Flood

[Initial value]

None

[Input mode]

interface mode

[Description]

Sets the processing method for multicast frames received by the VLAN interface, which are not registered in the MAC address table.

When the "discard" and "except-routing" keywords are not specified for the method of processing multicast frames

- Unknown multicast frames within the 224.0.0.0/4 range are discarded, and are not targeted for multicast routing by IGMP/PIM.
- When l2-unknown-mcast forward link-local is configured at the system level, multicast frames with addresses in the link-local range (224.0.0.0/24) are forwarded rather than discarded.

- When the l2-mcast flood command is used on a VLAN interface, frames for individual multicast addresses can be forwarded instead of being discarded.

When the "discard" and "except-routing" keywords are specified for the method of processing multicast frames

- Unknown multicast frames within the 224.0.0.0/4 range are discarded, and are targeted for multicast routing by IGMP/PIM.
- Even if l2-unknown-mcast forward link-local is configured at the system level, multicast frames with addresses in the link-local range (224.0.0.0/24) cannot be forwarded.
- When the l2-mcast flood command is used on a VLAN interface, frames for individual multicast addresses can be forwarded instead of being discarded.

If this command is executed with the "no" syntax, the setting returns to its default value, the system-wide processing method for unknown multicast frames is used.

[Note]

This command can be specified only for VLAN interfaces.

This command is prioritized over the settings for the system-wide processing method for unknown multicast frames.

The "except-routing" keyword can only be specified when the method for multicast frame processing is "discard".

The "except-routing" keyword can only be specified on models that support IGMP/PIM multicast routing.

[Example]

Discards unknown multicast frames on VLAN #1, but forwards frames for multicast link-local addresses.

```
SWX3220(config)# l2-unknown-mcast forward link-local
SWX3220(config)# interface vlan1
SWX3220(config-if)# l2-unknown-mcast discard
```

Discards unknown multicast frames on VLAN2, but IGMP/PIM multicast routing frames are targeted. Also, mDNS(224.0.0.251) and Dante(224.0.0.230-233) frames are forwarded for VLAN2

```
SWX3220(config)# interface vlan2
SWX3220(config-if)# l2-unknown-mcast discard except-routing
SWX3220(config-if)# l2-mcast flood 224.0.0.251
SWX3220(config-if)# l2-mcast flood 224.0.0.230
SWX3220(config-if)# l2-mcast flood 224.0.0.231
SWX3220(config-if)# l2-mcast flood 224.0.0.232
SWX3220(config-if)# l2-mcast flood 224.0.0.233
```

8.1.11 Forwarding setting for link local multicast frames

[Syntax]

l2-unknown-mcast forward link-local
no l2-unknown-mcast forward link-local

[Initial value]

None

[Input mode]

global configuration mode

[Description]

When l2-unknown-mcast discard is set, the frame for the link local multicast address is forwarded without being discarded.

If this command is executed with the "no" syntax, the specified setting is deleted.

[Note]

The link local multicast address for this command falls within the ranges shown below.

- IPv4: 224.0.0.0/24
- IPv6: ff02::/112

The format for specifying the IPv4 multicast address has been discontinued. When you load a config that includes this format, the config is automatically replaced with the **l2-mcast flood** command.

[Example]

This forwards frames for the link local multicast address as unknown multicasts without discarding them.

```
SWX3220(config)#l2-unknown-mcast discard
SWX3220(config)#l2-unknown-mcast forward link-local
```

8.1.12 Forwarding setting for multicast frames

[Syntax]

l2-mcast flood *ipv4_addr*
no l2-mcast flood *ipv4_addr*

[Parameter]

ipv4_addr	:	A.B.C.D IPv4 multicast address

[Initial value]

None

[Input mode]

interface mode

[Description]

Floods the frames with the IPv4 multicast address specified by the destination in multicast traffic received by the VLAN interface.

Up to 100 instances of this command can be set system-wide.

If this command is executed with the "no" syntax, the specified IPv4 multicast address settings are deleted.

If no IPv4 multicast address is specified, all settings are deleted.

[Note]

This command can be specified only for VLAN interfaces.

The IPv4 multicast address specified by this command is excluded from IGMP snooping.

[Example]

Floods the frame 239.0.0.251 with the destination IPv4 address received by VLAN #1.

```
SWX3220(config)#interface vlan1
SWX3220(config-if)#l2-mcast flood 239.0.0.251
```

8.1.13 Enable/disable function to transmit IGMP/MLD query when topology changes

[Syntax]

l2-mcast snooping tcn-query enable *time*
l2-mcast snooping tcn-query disable
no l2-mcast snooping tcn-query

[Parameter]

time	:	<1-30> Wait time for transmitting IGMP/MLD query (seconds)

[Initial value]

l2-mcast snooping tcn-query disable

[Input mode]

global configuration mode

[Description]

Specifies operation of the function that transmits an IGMP/MLD query when the topology changes due to spanning tree.

If this command is executed with the "no" syntax, the setting returns to the default.

When both IGMP/MLD snooping and spanning tree are used together, multicast communication might stop temporarily due to a change in topology, but that interval can be shortened by using this function.

If this is enabled, when a change in topology is detected, an IGMP/MLD query is transmitted after waiting the specified time.

If this is disabled, an IGMP/MLD query is not transmitted even if the topology changes.

[Example]

Enable transmission of an IGMP/MLD query when topology changes, and set the wait time to 5 seconds.

```
SWX3220(config)#l2-mcast snooping tcn-query enable 5
```

Disable transmission of an IGMP/MLD query when topology changes.

```
SWX3220(config)#l2-mcast snooping tcn-query disable
```

8.2 IGMP snooping

8.2.1 Set enable/disable IGMP snooping

[Syntax]

ip igmp snooping *switch*
no ip igmp snooping

[Parameter]

switch : IGMP snooping operations

Setting value	Description
enable	Enable IGMP snooping
disable	Disable IGMP snooping

[Initial value]

ip igmp snooping enable

[Input mode]

interface mode

[Description]

Enables the IGMP snooping setting of the interface.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be specified only for VLAN interface.

[Example]

Enable IGMP snooping for VLAN #2.

```
SWX3220#configure terminal
SWX3220(config)#interface vlan2
SWX3220(config-if)#ip igmp snooping enable
```

Disable IGMP snooping for VLAN #2.

```
SWX3220#configure terminal
SWX3220(config)#interface vlan2
SWX3220(config-if)#ip igmp snooping disable
```

8.2.2 Set IGMP snooping fast-leave

[Syntax]

ip igmp snooping fast-leave [auto-assignment]
no ip igmp snooping fast-leave

[Keyword]

auto-assignment : If the switch is connected to and controlled by the LAN/SFP port, the fast-leave function is disabled.

[Initial value]

none

[Input mode]

interface mode

[Description]

Enables IGMP snooping fast-leave for the interface.

If this is executed with the "no" syntax, IGMP snooping fast-leave is disabled.

If the Yamaha switch is connected to and controlled by the LAN/SFP port when the auto-assignment option is specified, the fast-leave function is automatically disabled only for that port.

The determination that a Yamaha switch is connected to and controlled by the LAN/SFP port is made by checking the LLDP frames received by the port in question and checking whether all of the following conditions are fulfilled.

- The OUI of the Chassis ID (MAC address) for the required TLV must be a Yamaha product
- "Bridge" must be included in the Enabled Capabilities of the basic management TLV

For this reason, when using the auto-assignment option, LLDP transmission/reception must be enabled on this product and on the opposing switch, and the basic management TLV must be appended to the transmitted frames.

[Note]

This command can be specified only for VLAN interface.

On a VLAN interface for which multiple hosts are connected to the LAN/SFP port, use this command to either enable the auto-assignment option or disable the fast-leave function altogether.

[Example]

Enable IGMP snooping fast-leave for VLAN #2.

```
SWX3220#configure terminal
SWX3220(config)#interface vlan2
SWX3220(config-if)#ip igmp snooping fast-leave
```

Disable IGMP snooping fast-leave for VLAN #2.

```
SWX3220#configure terminal
SWX3220(config)#interface vlan2
SWX3220(config-if)#no ip igmp snooping fast-leave
```

8.2.3 Set multicast router connection destination

[Syntax]

ip igmp snooping mrouter interface *ifname*
no ip igmp snooping mrouter interface *ifname*

[Parameter]

ifname	:	LAN/SFP port interface name Interface to set

[Initial value]

none

[Input mode]

interface mode

[Description]

Statically sets the LAN/SFP port to which the multicast router is connected.

If this command is executed with the "no" syntax, the setting is discarded.

[Note]

This command can be specified only for VLAN interface.

The multicast router must be connected to the specified LAN/SFP port. If an IGMP report is received from the receiver, it is forwarded to the specified LAN/SFP port.

[Example]

Specify LAN port #8 as a connection destination of the multicast router.

```
SWX3220#configure terminal
SWX3220(config)#interface vlan2
SWX3220(config-if)#ip igmp snooping mrouter interface port1.8
```

Remove LAN port #8 as a connection destination of the multicast router.

```
SWX3220#configure terminal
SWX3220(config)#interface vlan2
SWX3220(config-if)#no ip igmp snooping mrouter interface port1.8
```

8.2.4 Set query transmission function

[Syntax]

ip igmp snooping querier
no ip igmp snooping querier

[Initial value]

none

[Input mode]

interface mode

[Description]

Enables the IGMP query transmission function.

If this is executed with the "no" syntax, the IGMP query transmission function is disabled.

[Note]

This command can be specified only for VLAN interface.

Note that if you change the IP address while leaving this command enabled, queries will no longer be sent with the correct IP address following the change.

[Example]

Enable the transmission function for VLAN #2.

```
SWX3220#configure terminal
SWX3220(config)#interface vlan2
SWX3220(config-if)#ip igmp snooping querier
```

Disable the transmission function for VLAN #2.

```
SWX3220#configure terminal
SWX3220(config)#interface vlan2
SWX3220(config-if)#no ip igmp snooping querier
```

8.2.5 Set IGMP query transmission interval

[Syntax]

ip igmp snooping query-interval *interval*
no ip igmp snooping query-interval

[Parameter]

interval	:	<20-18000>
		Query transmission interval (seconds)

[Initial value]

ip igmp snooping query-interval 125

[Input mode]

interface mode

[Description]

Sets the transmission interval for IGMP queries.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be specified only for VLAN interface.

[Example]

Set the VLAN #2 query transmission interval to 30 seconds.

```
SWX3220#configure terminal
SWX3220(config)#interface vlan2
SWX3220(config-if)#ip igmp snooping query-interval 30
```

Return the VLAN #2 query transmission interval to the default setting.

```
SWX3220#configure terminal
SWX3220(config)#interface vlan2
SWX3220(config-if)#no ip igmp snooping query-interval
```

8.2.6 Set TTL value verification function for IGMP packets

[Syntax]

ip igmp snooping check ttl *switch*
no ip igmp snooping check ttl

[Parameter]

switch : TTL value verification function for IGMP packets

Setting value	Description
enable	Enable
disable	Disable

[Initial value]

ip igmp snooping check ttl enable

[Input mode]

interface mode

[Description]

Sets the TTL value verification function for IGMP packets.

If this command is executed with the "no" syntax, the setting returns to the default.

When this is enabled, IGMP packets with illegal TTL values in the IP header (besides 1) will be discarded.

When disabled, the relevant packet will be discarded, and the TTL value will be corrected to 1 and forwarded.

[Note]

This command can be specified only for VLAN interface.

[Example]

Enable the TTL value verification function of IGMP packets for VLAN #2.

```
SWX3220#configure terminal
SWX3220(config)#interface vlan2
SWX3220(config-if)#ip igmp snooping check ttl enable
```

Disnable the TTL value verification function of IGMP packets for VLAN #2.

```
SWX3220#configure terminal
SWX3220(config)#interface vlan2
SWX3220(config-if)#ip igmp snooping check ttl disable
```

8.2.7 Set RA verification function for IGMP packets

[Syntax]

ip igmp snooping check ra *switch*
no ip igmp snooping check ra

[Parameter]

switch : RA verification function for IGMP packets

Setting value	Description
enable	Enable
disable	Disable

[Initial value]

ip igmp snooping check ra disable

[Input mode]

interface mode

[Description]

Configures the RA verification function for IGMPv2/IGMPv3 packets.

If this command is executed with the "no" syntax, the setting returns to the default.

If this is enabled, IGMPv2/IGMPv3 packets whose IP headers do not include an RA (Router Alert) option are discarded.

When disabled, the relevant packet is not discarded; instead, an RA option is added to the IP header and the packet is forwarded.

[Note]

This command can only be specified for VLAN interface.

[Example]

This enables the RA verification function of IGMP packets for VLAN #2.

```
SWX3220#configure terminal
SWX3220(config)#interface vlan2
SWX3220(config-if)#ip igmp snooping check ra enable
```

This disables the RA verification function of IGMP packets for VLAN #2.

```
SWX3220#configure terminal
SWX3220(config)#interface vlan2
SWX3220(config-if)#ip igmp snooping check ra disable
```

8.2.8 Set ToS verification function for IGMP packets

[Syntax]

ip igmp snooping check tos *switch*
no ip igmp snooping check tos

[Parameter]

switch : ToS verification function for IGMP packets

Setting value	Description
enable	Enable
disable	Disable

[Initial value]

ip igmp snooping check tos disable

[Input mode]

interface mode

[Description]

Configures the ToS verification function for IGMP packets.

If this command is executed with the "no" syntax, the setting returns to the default.

When this is enabled, IGMPv3 packets with illegal ToS IP Precedence values (3 bits) in the IP header (besides B'110) will be discarded. For all other packets, the ToS is rewritten to 0xc0 and forwarded.

When disabled, the IGMP packet is not discarded; instead, the ToS will be corrected to 0xc0 and the packet is forwarded.

[Note]

This command can only be specified for VLAN interface.

[Example]

This enables the ToS verification function of IGMP packets for VLAN #2.

```
SWX3220#configure terminal
SWX3220(config)#interface vlan2
SWX3220(config-if)#ip igmp snooping check tos enable
```

This disables the ToS verification function of IGMP packets for VLAN #2.

```
SWX3220#configure terminal
SWX3220(config)#interface vlan2
SWX3220(config-if)#ip igmp snooping check tos disable
```

8.2.9 Set IGMP version

[Syntax]

ip igmp snooping version *version*

no ip igmp snooping version

[Parameter]

version : <2-3>
IGMP version

[Initial value]

ip igmp snooping version 3

[Input mode]

interface mode

[Description]

Sets the IGMP version.

If this command is executed with the "no" syntax, the IGMP version returns to the default setting (V3).

[Note]

This command can be specified only for VLAN interface.

If an IGMP packet of a different version than this setting is received, the following action occurs.

- When set to V2
  - If a V3 query is received, it is forwarded as a V2 query
  - If a V3 report is received, it is discarded
- When set to V3
  - If a V2 query is received, it is forwarded as a V2 query
  - If a V2 report is received, it is forwarded as a V3 report

[Example]

On VLAN #2, set the IGMP version to 2.

```
SWX3220#configure terminal
SWX3220(config)#interface vlan2
SWX3220(config-if)#ip igmp snooping version 2
```

On VLAN #2, return the IGMP version to the default setting.

```
SWX3220#configure terminal
SWX3220(config)#interface vlan2
SWX3220(config-if)#no ip igmp snooping version
```

8.2.10 Settings for IGMP Report Suppression

[Syntax]

ip igmp snooping report-suppression *switch*
no ip igmp snooping report-suppression

[Parameter]

switch : IGMP report suppression

Setting value	Description
enable	Enable
disable	Disable

[Initial value]

ip igmp snooping report-suppression enable

[Input mode]

interface mode

[Description]

Configures IGMP report suppression.

If this command is executed with the "no" syntax, the setting returns to the default.

When enabled, the minimum number of messages will be sent to the multicast router ports based on the information obtained from the received Report messages and Leave messages.

When disabled, the received Report messages and Leave messages will be sequentially transmitted to the multicast router ports.

[Note]

This command can only be specified for VLAN interface.

[Example]

Enables IGMP report suppression at VLAN #2.

```
SWX3220#configure terminal
SWX3220(config)#interface vlan2
SWX3220(config-if)#ip igmp snooping report-suppression enable
```

Disables IGMP report suppression at VLAN #2.

```
SWX3220#configure terminal
SWX3220(config)#interface vlan2
SWX3220(config-if)#ip igmp snooping report-suppression disable
```

8.2.11 Set the IGMP report forwarding function

[Syntax]

ip igmp snooping report-forward *switch*
no ip igmp snooping report-forward

[Parameter]

switch : IGMP report forwarding function

Setting value	Description
enable	Enable
disable	Disable

[Initial value]

ip igmp snooping report-forward disable

[Input mode]

interface mode

[Description]

This configures the IGMP report forwarding function.

If this command is executed with the "no" syntax, the setting returns to the default.

When this is enabled and a Yamaha switch is connected to and controlled by LAN/SFP port, an IGMP Report message or a Leave message is forwarded to that port, as well as to the multicast router port.

When disabled, the IGMP Report messages and Leave messages will be forwarded only to the multicast router port.

The determination that a Yamaha switch is connected to and controlled by the LAN/SFP port is made by checking the LLDP frames received by the port in question and checking whether all of the following conditions are fulfilled.

- The OUI of the Chassis ID (MAC address) for the required TLV must be a Yamaha product
- "Bridge" must be included in the Enabled Capabilities of the basic management TLV

For this reason, when using this function, LLDP transmission/reception must be enabled on this product and on the opposing switch, and the basic management TLV must be appended to the transmitted frames.

[Note]

This command can only be specified for VLAN interface.

When this function is enabled, disable the IGMP report suppression function.

[Example]

Enables the IGMP report forwarding function for VLAN #2.

```
SWX3220#configure terminal
SWX3220(config)#interface vlan2
SWX3220(config-if)#ip igmp snooping report-forward enable
```

Disables the IGMP report forwarding function for VLAN #2.

```
SWX3220#configure terminal
SWX3220(config)#interface vlan2
SWX3220(config-if)#ip igmp snooping report-forward disable
```

8.2.12 Settings for Suppression of Data Transmission to Multicast Router Ports

[Syntax]

ip igmp snooping mrouter-port data-suppression *switch*
no ip igmp snooping mrouter-port data-suppression

[Parameter]

switch : Suppression of data transmission to multicast router ports

Setting value	Description
enable	Enable
disable	Disable

[Initial value]

ip igmp snooping mrouter-port data-suppression disable

[Input mode]

interface mode

[Description]

Configures suppression of data transmission to multicast router ports.

If this command is executed with the "no" syntax, the setting returns to the default.

When enabled, the relevant data will be transmitted to the multicast router ports only when Report messages are received by the multicast router ports.

When disabled, the relevant data will be transmitted to the multicast router ports when Report messages are received by any of the multicast router ports.

[Note]

This command can only be specified for VLAN interface.

[Example]

Enables suppression of data transmission to multicast router ports at VLAN #2.

```
SWX3220#configure terminal
SWX3220(config)#interface vlan2
SWX3220(config-if)#ip igmp snooping mrouter-port data-suppression enable
```

Disables suppression of data transmission to multicast router ports in VLAN #2.

```
SWX3220#configure terminal
SWX3220(config)#interface vlan2
SWX3220(config-if)#ip igmp snooping mrouter-port data-suppression disable
```

8.2.13 Show multicast router connection port information

[Syntax]

show ip igmp snooping mrouter *ifname*

[Parameter]

ifname : VLAN interface name

Interface to show

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the multicast router connection port information that was dynamically learned or statically set.

[Example]

Show multicast router connection port information for VLAN #2.

```
SWX3220#show ip igmp snooping mrouter vlan2
VLAN    Interface             IP-address    Expires
2       port1.8(dynamic)          192.168.100.216        00:00:49
```

8.2.14 Show IGMP group membership information

[Syntax]

show ip igmp snooping groups [detail]
show ip igmp snooping groups *A.B.C.D* [detail]
show ip igmp snooping groups *ifname* [detail]

[Keyword]

detail	:	Detailed information

[Parameter]

A.B.C.D	:	Multicast group address
ifname	:	VLAN interface name Interface to show

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows IGMP group membership information.

[Example]

Show IGMP group membership information.

```
SWX3220#show ip igmp snooping groups
IGMP Snooping Group Membership
Group source list: (R - Remote, S - Static)
Vlan   Group/Source Address    Interface      Flags   Uptime     Expires  Last
Reporter   Version
1      239.255.255.250          port1.5        R      01:06:02   00:03:45
192.168.100.11    V3
```

Show detailed IGMP group membership information.

```
SWX3220#show ip igmp snooping groups detail
IGMP Snooping Group Membership Details
Flags: (R - Remote, S - Static)

Interface:      port1.5
Group:          239.255.255.250
Flags:          R
Uptime:         01:07:10
Group mode:     Exclude (Expires: 00:04:13)
Last reporter:  192.168.100.11
Source list is empty
```

8.2.15 Show an interface's IGMP-related information

[Syntax]

show ip igmp snooping interface *ifname*

[Parameter]

ifname	:	VLAN interface name Interface to show

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows IGMP-related information for a VLAN interface.

[Example]

Show IGMP-related information for VLAN #1.

```
SWX3220#show ip igmp snooping interface vlan1

IGMP Snooping information for vlan1
 IGMP Snooping enabled
 Snooping Querier none
 IGMP Snooping other querier timeout is 255 seconds
 Group Membership interval is 260 seconds
 IGMPv2/v3 fast-leave is enabled
 IGMPv1/v2 Report suppression enabled
 IGMPv2/v3 fast-leave auto-assignment is enabled
 IGMPv3 Report suppression enabled
 IGMPv1/v2/v3 Report forwarding enabled
 IGMP Snooping check TTL is enabled
 IGMP Snooping check RA is enabled
 IGMP Snooping check ToS is enabled
 IGMP Snooping Mrouter-port Data suppression disabled
 Router port detection using IGMP Queries
 Number of router-ports: 1
 Number of Groups: 1
 Number of v1-reports: 0
 Number of v2-reports: 6
 Number of v2-leaves: 0
 Number of v3-reports: 127
 Active Ports:
  port1.1 (F,R)
  port1.2

  F - Fast-leave auto-assignment is enabled
  R - Report forwarding is enabled
```

8.2.16 Clear IGMP group membership entries

[Syntax]

clear ip igmp snooping
clear ip igmp snooping group *A.B.C.D*
clear ip igmp snooping interface *ifname*

[Keyword]

group	:	Specifies the multicast group address to be cleared
interface	:	Specifies the VLAN interface to be cleared

[Parameter]

A.B.C.D	:	Multicast group address "*" indicates all entries
ifname	:	VLAN interface name Interface to clear

[Input mode]

privileged EXEC mode

[Description]

Clears IGMP group membership entries.

[Example]

Clear IGMP group membership entries for VLAN #1.

```
SWX3220#clear ip igmp snooping interface vlan1
```

8.3 MLD snooping

8.3.1 Enable/disable MLD snooping

[Syntax]

ipv6 mld snooping *switch*
no ipv6 mld snooping

[Parameter]

switch : MLD snooping operations

Setting value	Description
enable	Enable MLD snooping
disable	Disable MLD snooping

[Initial value]

ipv6 mld snooping enable

[Input mode]

interface mode

[Description]

Configures the operations of the MLD snooping setting of the interface.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This command can be specified only for VLAN interfaces.

[Example]

Enable MLD snooping for VLAN #2.

```
SWX3220#configure terminal
SWX3220(config)#interface vlan2
SWX3220(config-if)#ipv6 mld snooping enable
```

Disnable MLD snooping for VLAN #2.

```
SWX3220#configure terminal
SWX3220(config)#interface vlan2
SWX3220(config-if)#ipv6 mld snooping disable
```

8.3.2 Set MLD snooping fast-leave

[Syntax]

ipv6 mld snooping fast-leave
no ipv6 mld snooping fast-leave

[Initial value]

none

[Input mode]

interface mode

[Description]

Enables MLD snooping fast-leave for the interface.

If this is executed with the "no" syntax, MLD snooping fast-leave is disabled.

[Note]

This command can be specified only for VLAN interfaces. Also, this can be specified only if MLD snooping is enabled.

Do not enable this command on a VLAN interface for which multiple hosts are connected to the LAN/SFP port.

[Example]

Enable MLD snooping fast-leave for VLAN #2.

```
SWX3220#configure terminal
SWX3220(config)#interface vlan2
SWX3220(config-if)#ipv6 mld snooping fast-leave
```

Disable MLD snooping fast-leave for VLAN #2.

```
SWX3220#configure terminal
SWX3220(config)#interface vlan2
SWX3220(config-if)#no ipv6 mld snooping fast-leave
```

8.3.3 Set multicast router connection destination

[Syntax]

ipv6 mld snooping mrouter interface *ifname*
no ipv6 mld snooping mrouter interface *ifname*

[Parameter]

ifname	:	Interface name of LAN/SFP port Interface to set

[Initial value]

none

[Input mode]

interface mode

[Description]

Statically sets the LAN/SFP port to which the multicast router is connected.

If this command is executed with the "no" syntax, the setting is discarded.

[Note]

This command can be specified only for VLAN interfaces. Also, this can be specified only if MLD snooping is enabled.

The multicast router must be connected to the specified LAN/SFP port. If an MLD report is received from the receiver, it is forwarded to the specified LAN/SFP port.

[Example]

Specify LAN port #8 as a connection destination of the multicast router.

```
SWX3220#configure terminal
SWX3220(config)#interface vlan2
SWX3220(config-if)#ipv6 mld snooping mrouter interface port1.8
```

Remove LAN port #8 as a connection destination of the multicast router.

```
SWX3220#configure terminal
SWX3220(config)#interface vlan2
SWX3220(config-if)#no ipv6 mld snooping mrouter interface port1.8
```

8.3.4 Set query transmission function

[Syntax]

ipv6 mld snooping querier
no ipv6 mld snooping querier

[Initial value]

none

[Input mode]

interface mode

[Description]

Enables the MLD query transmission function.

If this command is executed with the "no" syntax, the MLD query transmission function is disabled.

[Note]

This command can be specified only forVLAN interfaces. Also, this can be specified only if MLD snooping is enabled.

When using this command, you must specify the **ipv6 enable** command for one of the VLAN interfaces. Note that if the **ipv6 enable** command has not been specified, MLD query is not transmitted.

[Example]

Enable the MLD query transmission function for VLAN #2.

```
SWX3220#configure terminal
SWX3220(config)#interface vlan2
SWX3220(config-if)#ipv6 mld snooping querier
```

Disable the MLD query transmission function for VLAN #2.

```
SWX3220#configure terminal
SWX3220(config)#interface vlan2
SWX3220(config-if)#no ipv6 mld snooping querier
```

8.3.5 Set MLD query transmission interval

[Syntax]

ipv6 mld snooping query-interval *interval*
no ipv6 mld snooping query-interval

[Parameter]

interval	:	<20-18000>
		Query transmission interval (seconds)

[Initial value]

ipv6 mld snooping query-interval 125

[Input mode]

interface mode

[Description]

Sets the transmission interval for MLD queries.

If this command is executed with the "no" syntax, the MLD query transmission interval is returned to the default setting.

[Note]

This command can be specified only for VLAN interfaces. Also, this can be specified only if MLD snooping is enabled.

[Example]

Set the VLAN #2 query transmission interval to 30 seconds.

```
SWX3220#configure terminal
SWX3220(config)#interface vlan2
SWX3220(config-if)#ipv6 mld snooping query-interval 30
```

Return the VLAN #2 query transmission interval to the default setting.

```
SWX3220#configure terminal
SWX3220(config)#interface vlan2
SWX3220(config-if)#no ipv6 mld snooping query-interval
```

8.3.6 Set MLD version

[Syntax]

ipv6 mld snooping version *version*
no ipv6 mld snooping version

[Parameter]

version	:	<1-2>
		MLD version

[Initial value]

ipv6 mld snooping version 2

[Input mode]

interface mode

[Description]

Sets the MLD version.

If this command is executed with the "no" syntax, the MLD version returns to the default setting (V2).

[Note]

This command can be specified only for VLAN interfaces. Also, this can be specified only if MLD snooping is enabled.

If an MLD packet of a different version than this setting is received, the following action occurs.

- If V1 is specified

  - If a V2 query is received, it is forwarded as a V1 query
  - If a V2 report is received, it is discarded
- If V2 is specified
  - If a V1 query is received, it is forwarded as a V1 query
  - If a V1 report is received, it is forwarded as a V2 report

[Example]

On VLAN #2, set the MLD version to 1.

```
SWX3220#configure terminal
SWX3220(config)#interface vlan2
SWX3220(config-if)#ipv6 mld snooping version 1
```

On VLAN #2, return the MLD version to the default setting.

```
SWX3220#configure terminal
SWX3220(config)#interface vlan2
SWX3220(config-if)#no ipv6 mld snooping version
```

8.3.7 Settings for MLD Report Suppression

[Syntax]

ipv6 mld snooping report-suppression *switch*
no ipv6 mld snooping report-suppression

[Parameter]

switch : MLD report suppression

Setting value	Description
enable	Enable
disable	Disable

[Initial value]

ipv6 mld snooping report-suppression enable

[Input mode]

interface mode

[Description]

Configures MLD report suppression.

If this command is executed with the "no" syntax, the setting returns to the default.

When enabled, the minimum number of messages will be sent to the multicast router ports based on the information obtained from the received Report messages and Leave messages.

When disabled, the received Report messages and Leave messages will be sequentially transmitted to the multicast router ports.

[Note]

This command can only be specified for VLAN interface.

[Example]

Enables MLD report suppression at VLAN #2.

```
SWX3220#configure terminal
SWX3220(config)#interface vlan2
SWX3220(config-if)#ipv6 mld snooping report-suppression enable
```

Disables MLD report suppression at VLAN #2.

```
SWX3220#configure terminal
SWX3220(config)#interface vlan2
SWX3220(config-if)#ipv6 mld snooping report-suppression disable
```

8.3.8 Show multicast router connection port information

[Syntax]

show ipv6 mld snooping mrouter *ifname*

[Parameter]

ifname	:	VLAN interface name Interface to show

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the multicast router connection port information that was dynamically learned or statically set.

[Example]

Show multicast router connection port information for VLAN #2.

```
SWX3220#show ipv6 mld snooping mrouter vlan2
VLAN    Interface             IP-address    Expires
2       port1.11(dynamic)         fe80::ae44:f2ff:fe30:291        00:01:04
```

8.3.9 Show MLD group membership information

[Syntax]

show ipv6 mld snooping groups [detail]
show ipv6 mld snooping groups *X*:*X*::*X*:*X* [detail]
show ipv6 mld snooping groups *ifname* [detail]

[Keyword]

detail	:	Detailed information

[Parameter]

X:*X*::*X*:*X*	:	Multicast group address
ifname	:	VLAN interface name Interface to show

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows MLD group membership information.

[Example]

Show MLD group membership information.

```
SWX3220#show ipv6 mld snooping groups
MLD Connected Group Membership
Group Address                           Interface            Uptime   Expires  Last
Reporter
ff15::1                                 port1.3              00:00:44 00:01:07
fe80::a00:27ff:fe8b:87e3
```

Show detailed MLD group membership information.

```
SWX3220#show ipv6 mld snooping groups detail
MLD Snooping Group Membership Details
Flags: (R - Remote, S - Static)

Interface:      port1.3
Group:          ff15::1
Uptime:         00:00:03
Group mode:     Include ()
Last reporter:  fe80::a00:27ff:fe8b:87e3
Group source list: (R - Remote, M - SSM Mapping, S - Static )
    Source Address                          Uptime    v2 Exp    Fwd  Flags
    fe80::221:70ff:fef9:8a39               00:00:03  00:01:06  Yes  R
```

8.3.10 Show an interface's MLD-related information

[Syntax]

show ipv6 mld snooping interface *ifname*

[Parameter]

ifname	:	VLAN interface name Interface to show

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Show a VLAN interface's MLD-related information.

[Example]

Show MLD-related information for VLAN #1.

```
SWX3220#show ipv6 mld snooping interface vlan1

MLD Snooping information for vlan1
 MLD Snooping enabled
 Snooping Querier none
 MLD Snooping other querier timeout is 255 seconds
 Group Membership interval is 260 seconds
 MLDv1 fast-leave is disabled
 MLDv1 Report suppression enabled
 MLDv2 Report suppression enabled
 Router port detection using MLD Queries
 Number of router-ports: 0
 Number of Groups: 0
 Number of v1-reports: 0
 Number of v1-leaves: 0
 Number of v2-reports: 127
 Number of v1-query-warnings: 0
 Number of v2-query-warnings: 0
 Active Ports:
  port1.1
  port1.2
```

8.3.11 Clear MLD group membership entries

[Syntax]

clear ipv6 mld snooping
clear ipv6 mld snooping group *X*:*X*::*X*:*X*
clear ipv6 mld snooping interface *ifname*

[Keyword]

group	:	Specifies the multicast group address to be cleared
interface	:	Specifies the VLAN interface to clear

[Parameter]

X:*X*::*X*:*X*	:	Multicast group address "*" indicates all entries
ifname	:	VLAN interface name Interface to clear

[Input mode]

privileged EXEC mode

[Description]

Clears MLD group membership entries.

[Example]

Clear MLD group membership entries for VLAN #1.

```
SWX3220#clear ipv6 mld snooping interface vlan1
```

8.4 PIM

8.4.1 Set PIM operation mode

[Syntax]

ip pim *mode* [passive]
no ip pim *mode* [passive]

[Keyword]

passive : Specifies the applicable interface as a passive interface.

[Parameter]

mode : PIM operation mode

Setting value	Description
dense-mode	Enables PIM-DM.
sparse-mode	Enables PIM-SM.

[Initial value]

none

[Input mode]

interface mode

[Description]

When dense-mode is specified, this enables PIM-DM; and when sparse-mode is specified, this enables PIM-SM for the applicable interface.

If this command is executed with the "no" syntax, the function is disabled.

The same operation mode must be used on all VLAN interfaces.

When specifying a passive interface, multicast packets will be forwarded, but PIM messages will not be transmitted or received.

[Note]

When PIM-DM and PIM-SM are enabled, use the **ip multicast-routing** command to enable multicast routing. Also, using this command will automatically enable IGMP, but we recommend explicitly enabling the IGMP and IGMP snooping functions.

[Example]

Enable PIM-DM on VLAN #2.

```
SWX3220(config)#interface vlan2
SWX3220(config-if)# ip pim dense-mode
SWX3220(config-if)# ip igmp
```

Enable PIM-SM on VLAN #2.

```
SWX3220(config)#interface vlan2
SWX3220(config-if)# ip pim sparse-mode
SWX3220(config-if)# ip igmp
```

8.4.2 Set Hello message interval

[Syntax]

ip pim hello-interval *interval*
no ip pim hello-interval

[Parameter]

interval : <1-18724>

PIM Hello message send interval (seconds)

[Initial value]

ip pim hello-interval 30

[Input mode]

interface mode

[Description]

Sets the Hello Period value (the Hello message transmission interval) for applicable interfaces on which PIM-SM and PIM-DM are enabled.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

If there are no Hello Holdtime settings for the Hello message time to live according to the **ip pim hello-holdtime** command, Hello Holdtime is set to (Hello Period x 3.5) seconds.

If Hello Holdtime is less than Hello Period as a result of the Hello Period setting value being changed with this command, Hello Holdtime will be updated to (Hello Period x 3.5) seconds.

[Example]

This sets the Hello message transmission interval to 20 seconds.

```
SWX3220(config)#interface vlan2
SWX3220(config-if)#ip pim hello-interval 20
```

8.4.3 Set Hello message timeout

[Syntax]

ip pim hello-holdtime *time*
no ip pim hello-holdtime

[Parameter]

time	:	<1-65535> (seconds)

[Initial value]

none

[Input mode]

interface mode

[Description]

Sets the timeout interval for Hello messages received on applicable interfaces where PIM-SM and PIM-DM are enabled.

If this command is executed with the "no" syntax, the setting returns to the default.

The default value is (Hello Period x 3.5). When the Hello Period Is at the default value of 30 seconds, the Hello Holdtime default value will be 105 seconds.

[Note]

The Hello Period value can be changed using the **ip pim hello-interval** command.

When the Hello Holdtime is less than the Hello Period due to having changed the Hello Period setting, this will be updated to (Hello Period x 3.5).

[Example]

Set the Hello message timeout period to 120 seconds.

```
SWX3220(config)#interface vlan2
SWX3220(config-if)#ip pim hello-holdtime 120
```

8.4.4 Set PIM neighbor filter

[Syntax]

ip pim_neighbor-filter *listnum*
no ip_pim_neighbor-filter *listnum*

[Parameter]

listnum	:	<1-2000>
		ID of IPv4 access list

[Initial value]

none

[Input mode]

interface mode

[Description]

By applying the IPv4 access list on an applicable interface where PIM-SM and PIM-DM are enabled, this prevents a neighboring relationship to be formed with a specific PIM router.

If this command is executed with the "no" syntax, the PIM neighbor filter setting is deleted.

[Note]

For the IPv4 access list, specify permit to form a neighboring relationship with PIM neighbors, and deny to prevent forming a neighboring relationship.

[Example]

Prevent a neighboring relationship to be formed with a PIM router that has an IP address of 192.168.1.10.

```
SWX3220(config)#interface vlan1
SWX3220(config-if)#ip pim neighbor-filter 10
SWX3220(config-if)#exit
SWX3220(config)#access-list 10 deny any 192.168.1.10 0.0.0.0 any
SWX3220(config)#access-list 10 permit any any any
```

8.4.5 Set Generation ID

[Syntax]

ip pim exclude-genid
no ip pim exclude-genid

[Initial value]

none

[Input mode]

interface mode

[Description]

Configures the Hello message not to include the GenID (Generation ID).

If this command is executed with the "no" syntax, includes the GenID in the PIM Hello message.

[Example]

Configure the Hello message not to include the GenID.

```
SWX3220(config)#interface vlan2
SWX3220(config-if)#ip pim exclude-genid
```

8.4.6 Set DR priority order

[Syntax]

ip pim dr-priority *priority*
no ip pim dr-priority [*priority*]

[Parameter]

priority	:	<0-4294967294>
		DR priority order

[Initial value]

ip pim dr-priority 1

[Input mode]

interface mode

[Description]

Sets the DR (Designated Router) priority for the applicable interface.

If multiple PIM-SM routers exist on the same LAN, the PIM-SM router with the highest DR priority will be the designated router (DR).

If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

Set the DR priority to 2.

```
SWX3220(config)#interface vlan2
SWX3220(config-if)#ip pim dr-priority 2
```

8.4.7 Set static RP

[Syntax]

ip pim rp-address *address* [*listnum*]
no ip pim rp-address *address* [*listnum*]

[Parameter]

address	:	RP IP address (A.B.C.D)
listnum	:	<1-2000> ID of IPv4 access list

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Statically sets the rendezvous point (RP).

If this command is executed with the "no" syntax, deletes static RP information.

[Note]

Multiple static RPs can be registered. Also, both static RP and Bootstrap Router (BSR) mechanisms can be used together.

If both the RP that was learned by the BSR and the static RP exist simultaneously, the RP that was learned by the BSR is given priority for use. If there are multiple RPs that were learned by the BSR, the RP is selected using the RP priority and hash function.

If multiple static RPs exist, the RP with the largest IP address is selected as the RP.

If the group range specified by the IPv4 access list does not exist, or if "any" is specified, the group range will be 224.0.0.0/4 (all multicast group addresses).

When a group range is specified in the IPv4 access list, this should be set to "permit" for the multicast group that is managed by the RP.

[Example]

Specify 10.0.0.1 as the static RP.

```
SWX3220(config)#ip pim rp-address 10.0.0.1
```

8.4.8 Set RP candidate

[Syntax]

ip pim rp-candidate *ifname* [group-list *listnum*] [interval *interval*] [priority *priority*]
no ip pim rp-candidate [*ifname*]

[Keyword]

group-list	:	Specifies the IPv4 access list and targets a specific multicast group.
interval	:	Specifies the transmission interval for the Candidate-RP-Advertisement message.
priority	:	Specifies the priority when the RP is selected. The smaller one will be given priority for RP selection.

[Parameter]

ifname	:	Name of interface on which the IP address that is reported as a rendezvous point candidate is set
listnum	:	<1-2000> IPv4 access list
interval	:	<1-16383> Candidate-RP-Advertisement message transmission interval (seconds)
priority	:	<0-255> Priority for RP selection

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Sets the interface that will operate as a candidate rendezvous point (C-RP).

If this command is executed with the "no" syntax, disables operations as a C-RP.

[Note]

If both the RP that was learned by the BSR and the static RP exist simultaneously, the RP that was learned by the BSR is given priority for use. If there are multiple RPs that were learned by the BSR, the RP is selected using the RP priority and hash function.

If multiple static RPs exist, the RP with the largest IP address is selected as the RP.

If the group range specified by the IPv4 access list does not exist, or if "any" is specified, the group range will be 224.0.0.0/4 (all multicast group addresses).

When a group range is specified in the IPv4 access list, this should be set to "permit" for the multicast group that is managed by the RP.

[Example]

Specify VLAN #2 as a candidate RP for all multicast group addresses 224.0.0.0/4.

```
SWX3220(config)#ip pim rp-candidate vlan2
```

8.4.9 Set Candidate-RP-Advertisement message

[Syntax]

ip pim crp-fixed-prefix
no ip pim crp-fixed-prefix

[Initial value]

none

[Input mode]

global configuration mode

[Description]

If nothing is specified for the multicast group range on the rendezvous point (C-RP), this sets Prefix Count = 1, and configures the Candidate-RP-Advertisement to be transmitted for Group = 224.0.0.0/4 (all multicast groups).

If this command is executed with the "no" syntax, returns to the operations set by default.

If nothing is specified for the multicast group range using the **ip pim rp-candidate** command by default, this sets Prefix Count = 0, and transmits the Candidate-RP-Advertisement message without Group information.

[Example]

If nothing is specified for the multicast group range in the C-RP settings, this sets Prefix Count = 1, and transmits the Candidate-RP-Advertisement message for Group = 224.0.0.0/4.

```
SWX3220(config)#ip pim crp-fixed-prefix
```

8.4.10 Set BSR candidate

[Syntax]

ip pim bsr candidate *ifname* [*mask* [*priority*]]
no ip pim bsr-candidate [*ifname*]

[Parameter]

ifname	:	Interface name Specified interface
mask	:	<0-32> Hash mask length when RP is selected
priority	:	<0-255> BSR priority order

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Enables operations as a candidate bootstrap router (C-BSR), using the IP address configured for the interface.

The BSR performs mapping of the multicast group and rendezvous point (RP). The higher the BSR priority, the greater the likelihood of selection as a BSR.

If this command is executed with the "no" syntax, disables operations as a C-BSR.

[Example]

Use the IP address of VLAN #2 to configure this switch to operate as a C-BSR on a PIM-SM network.

```
SWX3220(config)#ip pim bsr-candidate vlan2
```

8.4.11 Set BSR message transmit/receive

[Syntax]

ip pim bsr-border
no ip pim bsr-border

[Initial value]

none

[Input mode]

interface mode

[Description]

Stops transmit/receive of bootstrap router (BSR) messages on applicable interfaces where PIM-SM is enabled.

If this command is executed with the "no" syntax, transmitting and receiving BSR messages will be allowed.

[Example]

Stop transmit and receive of BSR messages on the VLAN #2.

```
SWX3220(config)#interface vlan2
SWX3220(config-if)#ip pim bsr-border
```

8.4.12 Set RP priority usage

[Syntax]

ip pim ignore-rp-set-priority
no ip pim ignore-rp-set-priority

[Initial value]

none

[Input mode]

global configuration mode

[Description]

When RP is selected from the candidate rendezvous point (C-RP), this ignores the RP priority and uses only the hash function.

If this command is executed with the "no" syntax, the RP priority and hash function are used to select the RP.

[Example]

Select the RP using only the hash function without RP priority.

```
SWX3220(config)#ip pim ignore-rp-set-priority
```

8.4.13 Set source IP address for Register messages

[Syntax]

ip pim register-source *address*
ip pim register-source *ifname*
no ip pim register-source

[Parameter]

address	:	Register message source IP address (A.B.C.D)
ifname	:	Interface name. The IP address of the specified interface will be used as the source IP address for Register messages.

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Explicitly specifies the source IP address for Register messages. When specifying, the IP address of the default RPF interface will be overwritten.

If this command is executed with the "no" syntax, uses the IP address of the closest RPF interface to the multicast sender.

[Note]

You must set an IP address that can be reached from the rendezvous point (RP).

[Example]

Set the source IP address for Register messages to 192.168.100.100.

```
SWX3220(config)#ip pim register-source 192.168.100.100
```

8.4.14 Set register message filtering

[Syntax]

ip pim accept-register list *listnum*
no ip pim accept-register

[Parameter]

listnum	:	<1-2000> ID of IPv4 access list

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Filters Register messages at the rendezvous point (RP).

If this command is executed with the "no" syntax, deletes the filtering settings.

[Note]

Since only the source IP address of the multicast IP address is used for filtering, the destination IP address settings will be ignored.

To allow receiving Register messages, use permit; and to block Register messages, use deny.

[Example]

Block Register messages from source address 10.0.0.1 at the RP.

```
SWX3220(config)#access-list 120 deny any 10.0.0.1 0.0.0.0 any
SWX3220(config)#access-list 120 permit any any any
SWX3220(config)#ip pim accept-register list 120
```

8.4.15 Set upper limit value of the Register message transmission rate

[Syntax]

ip pim register-rate-limit *limit*
no ip pim register-rate-limit

[Parameter]

limit : <1-65535>

The upper limit for the number of packets that can be transmitted within 1 second.

[Initial value]

none

[Input mode]

global configuration mode

[Description]

For interfaces on which PIM-SM is enabled, this specifies the upper limit for the number of Register message packets that can be transmitted within 1 second.

If this command is executed with the "no" syntax, cancels the limitation.

[Note]

The transmission rate limit is applied as a (S, G) per-group upper limit, not as a system-wide limit.

[Example]

Set the limitation for the maximum number of Register message packets that can be transmitted within 1 second to 3000.

```
SWX3220(config)#ip pim register-rate-limit 3000
```

8.4.16 Set calculation method for Register message checksums

[Syntax]

ip pim register-checksum all [group-list *listnum*]
no ip pim register-checksum all [group-list *listnum*]

[Keyword]

group-list : Specifies the IPv4 access list and targets a specific multicast group.

[Parameter]

listnum : <1-2000>

ID of IPv4 access list

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Configures the entire packet for PIM messages as a target for calculation when calculating checksums for Register messages.

If this command is executed with the "no" syntax, calculates the checksum by using only the header.

[Example]

This calculates the checksum by using the entire PIM message, when calculating the checksum from Register messages received from multicast group 224.0.1.1.

```
SWX3220(config)#ip pim register-checksum all group-list 20
SWX3220(config)#access-list 20 permit any 224.0.1.1 0.0.0.0 any
```

8.4.17 Set Register message transmission standby time

[Syntax]

ip pim register-suppression *time*
no ip pim register-suppression

[Parameter]

time : <1-65535>

Register message transmission standby time (seconds.)

[Initial value]

ip pim register-suppression 60

[Input mode]

global configuration mode

[Description]

Sets the Register Suppression Timeout time before resending a Register message after receiving a Register-Stop message.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

If the RP Keepalive Timer (KAT) settings made with the **ip pim rp-register-kat** command do not exist, the KAT is automatically determined by using the Register Suppression Timeout value.

[Example]

Set the time before resending a Register message after receiving a Register-Stop message to 500 seconds.

```
SWX3220(config)#ip pim register-suppression 500
```

8.4.18 Set Join/Prune message transmission interval

[Syntax]

ip pim jp-timer *time*
no ip pim jp-timer [*time*]

[Parameter]

time : <1-65535>

Join/Prune message transmission interval (seconds)

[Initial value]

ip pim jp-timer 60

[Input mode]

global configuration mode

[Description]

Sets the transmission interval for Join/Prune messages (Join/Prune Period) on the interface where PIM-SM is enabled.

If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

Sets the Join/Prune message transmission interval to 120 seconds.

```
SWX3220(config)#ip pim jp-timer 120
```

8.4.19 Set RP Keepalive Timer

[Syntax]

ip pim rp-register-kat *time*
no ip pim rp-register-kat

[Parameter]

time	:	<1-65535> (seconds) Keepalive Timer value for (S, G) entry

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Sets the (S, G) entry Keepalive Timer (KAT) on the rendezvous point (RP).

When the number of seconds on the KAT have elapsed after data traffic has stopped, the Join status on the (S, G) entries is deleted.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

If the Register Suppression Timeout is set using the **ip pim register-suppression** command without configuring this command, the KAT will automatically be changed based on the Register Suppression Timeout.

[Example]

Sets the (S, G) entry Keepalive Timer to 3000 seconds.

```
SWX3220(config)#ip pim rp-register-kat 3000
```

8.4.20 Set SPT move operation

[Syntax]

ip pim spt-disable [group-list *listnum*]
no ip pim spt-disable [group-list *listnum*]

[Keyword]

group-list	:	Specifies the IPv4 access list and targets a specific multicast group.

[Parameter]

listnum	:	<1-2000> ID of IPv4 access list

[Initial value]

none

[Input mode]

global configuration mode

[Description]

When this unit is operating as a last hop router, the shortest path tree (SPT) is not used. Instead, the rendezvous point tree (RPT) is used for multicast routing.

If this command is executed with the "no" syntax, SPT is used to find the shortest route for multicast routing.

[Note]

The IPv4 access list should be set to allow (permit) the multicast group in question.

[Example]

Use RPT to perform multicast routing on multicast group 224.0.1.3.

```
SWX3220(config)#ip pim spt-disable group-list 10
SWX3220(config)#access-list 10 permit any 224.0.1.3 0.0.0.0 any
```

8.4.21 Set PIM-SSM

[Syntax]

ip pim ssm default
ip pim ssm range [*listnum*]
no ip pim ssm

[Parameter]

listnum	:	<1-2000>
		ID of IPv4 access list

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Enables the PIM-SSM (Source Specific Multicast).

When "default" is specified, 232.0.0.0/8 is used for the SSM range, and the standard IPv4 access list can be used to specify the desired SSM range.

If this command is executed with the "no" syntax, disables PIM-SSM and deletes the settings for the SSM range.

[Note]

To make multicast receivers in the SSM range join the multicast group, you must specify an IGMPv3 multicast sender.

For IGMPv2, you must enable the SSM mapping function using the **ip igmp ssm-map enable** command, and statically associate the multicast group and multicast sender using the **ip igmp ssm-map static** command.

[Example]

Enable PIM-SSM and uses 232.0.0.0/8 for the SSM range.

```
SWX3220(config)#ip pim ssm default
```

8.4.22 Set State Refresh message transmission interval

[Syntax]

ip pim state-refresh origination-interval *interval*
no ip pim state-refresh rigination-interval

[Parameter]

interval	:	<1-100>
		State Refresh message transmission interval (seconds)

[Initial value]

ip pim state-refresh origination-interval 60

[Input mode]

interface mode

[Description]

Sets the transmission interval for State Refresh messages (State Refresh Interval) on the interface where PIM-DM is enabled.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

These settings must be made on a VLAN to which the multicast sender is connected.

[Example]

Set the State Refresh message transmission interval to 180 seconds.

```
SWX3220(config)#interface vlan2
SWX3220(config-if)# ip pim state-refresh origination-interval 180
```

8.4.23 Set Graft message maximum resend count

[Syntax]

ip pim graft-retransmit *count*
no ip pim graft-retransmit

[Parameter]

count	:	<1-65535>
		Graft message maximum resend count

[Initial value]

none

[Input mode]

interface mode

[Description]

Sets the Graft message maximum resend count for applicable interfaces on which PIM-DM is enabled.

If this command is executed with the "no" syntax, messages continue to be resent until a Graft Ack message is received.

[Example]

Set the Graft message maximum resend count to 5.

```
SWX3220(config)# interface vlan2
SWX3220(config-if)# ip pim graft-retransmit 5
```

8.4.24 Set forward delay time for PIM messages

[Syntax]

ip pim propagation-delay *time*
no ip pim propagation-delay

[Parameter]

time	:	<0-32767>
		Forward delay time for PIM messages (milli seconds)

[Initial value]

ip pim propagation-delay 500

[Input mode]

interface mode

[Description]

Sets the Propagation Delay estimated forward delay time for PIM messages for applicable interfaces on which PIM-DM is enabled.

If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

Set Propagation Delay for PIM messages to 1000 ms.

```
SWX3220(config)#interface vlan2
SWX3220(config-if)#ip pim propagation-delay 1000
```

8.4.25 Set unicast BSM send/receive

[Syntax]

ip pim unicast-bsm
no ip pim unicast-bsm

[Initial value]

none

[Input mode]

interface mode

[Description]

Enables transmit/receive of unicast bootstrap messages (BSM) on applicable interfaces where PIM-SM is enabled.

If this command is executed with the "no" syntax, disables unicast BSM send/receive.

[Example]

Enable unicast BSM send/receive.

```
SWX3220(config)#ip pim unicast-bsm
```

8.4.26 Set confirmation for RP-reachability messages

[Syntax]

ip pim register-rp-reachability
no ip pim register-rp-reachability

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Enables checking of RP-reachability messages.

If this command is executed with the "no" syntax, RP-reachability messages will not be checked.

[Example]

Enable checking of RP-reachability messages.

```
SWX3220(config)#ip pim register-rp-reachability
```

8.4.27 Show PIM interface information

[Syntax]

show ip pim interface [detail]

[Keyword]

detail	:	Also show detailed information

[Initial value]

none

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows information for interfaces on which PIM is enabled.

[Example]

Show information for interfaces on which PIM-DM is enabled.

```
SWX3220#show ip pim interface
Total interfaces: 3
Address          Interface   VIFindex   Ver/   Nbr    DR         DR
                                        Mode   Count  Prior
192.168.20.1     vlan20      1          v2/D   0      1
192.168.110.2    vlan110     0          v2/D   1      1
192.168.130.1    vlan130     2          v2/D   0      1
```

Show detailed information for interfaces on which PIM-DM is enabled.

```
SWX3220#show ip pim interface detail
vlan20 (vif 1):
  Address 192.168.20.1, Mode: Dense
  DR N/A
  Hello period 30 seconds, Next Hello in 9 seconds
  Triggered Hello period 5 seconds
  PIM GenID sent in Hellos: 3924591a
  Graft retransmissions: infinite
  State refresh origination interval is 5 seconds
  Propagation delay is 500 milli-seconds
  Neighbors:
  PIM neighbor count: 0
  PIM configured DR priority: 1
  PIM border interface: no
  PIM Neighbor policy: not configured

vlan110 (vif 0):
  Address 192.168.110.2, Mode: Dense
  DR N/A
  Hello period 30 seconds, Next Hello in 4 seconds
  Triggered Hello period 5 seconds
  PIM GenID sent in Hellos: 68e2d99a
  Graft retransmissions: infinite
  State refresh origination interval is 3 seconds
  Propagation delay is 500 milli-seconds
  Neighbors:
   192.168.110.1
  PIM neighbor count: 1
  PIM configured DR priority: 1
  PIM border interface: no
  PIM Neighbor policy: not configured

vlan130 (vif 2):
  Address 192.168.130.1, Mode: Dense
  DR N/A
  Hello period 30 seconds, Next Hello in 21 seconds
  Triggered Hello period 5 seconds
  PIM GenID sent in Hellos: 18eec518
  Graft retransmissions: infinite
  State refresh origination interval is 60 seconds
  Propagation delay is 500 milli-seconds
  Neighbors:
  PIM neighbor count: 0
  PIM configured DR priority: 1
  PIM border interface: no
  PIM Neighbor policy: not configured
```

Show information for interfaces on which PIM-SM is enabled.

```
SWX3220#show ip pim interface
Total interfaces: 3
Address          Interface   VIFindex   Ver/   Nbr    DR         DR
                                        Mode   Count  Prior
192.168.20.1     vlan20      2          v2/S   0      1          192.168.20.1
192.168.110.2    vlan110     0          v2/S   1      1          192.168.110.2
```

Show detailed information for interfaces on which PIM-SM is enabled.

```
SWX3220#show ip pim interface detail
vlan20 (vif 2):
  Address 192.168.20.1, Mode: Sparse
  DR 192.168.20.1, DR's priority: 1
  Hello period 30 seconds, Next Hello in 2 seconds
  Triggered Hello period 5 seconds
  PIM GenID sent in Hellos: 61d3c50d
  Interface ID: Router-ID:192.168.110.2 Local-ID 320
  Neighbors:
  PIM neighbor count: 0
  PIM configured DR priority: 1
  PIM border interface: no
  PIM Neighbor policy: not configured

vlan110 (vif 0):
  Address 192.168.110.2, Mode: Sparse
  DR 192.168.110.2, DR's priority: 1
  Hello period 30 seconds, Next Hello in 5 seconds
  Triggered Hello period 5 seconds
  PIM GenID sent in Hellos: 7c30c40a
  Interface ID: Router-ID:192.168.110.2 Local-ID 410
  Neighbors:
   192.168.110.1
  PIM neighbor count: 1
  PIM neighbor holdtime: 105
  PIM configured DR priority: 1
  PIM border interface: no
  PIM Neighbor policy: not configured
```

8.4.28 Show IP multicast routing information base

[Syntax]

show ip pim mroute [*group*] [*source*] [detail]

[Keyword]

detail	:	Shows detailed information

[Parameter]

group	:	Multicast group address (A.B.C.D; only when PIM-SM is used)
source	:	Source IPv4 address (A.B.C.D; only when PIM-SM is used)

[Initial value]

none

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the IP multicast routing information base.

[Example]

Show the IP multicast routing information base when PIM-DM is in operation.

```
SWX3220#show ip pim mroute
PIM-DM Multicast Routing Table
(192.168.30.100, 239.0.0.1)
  RPF Neighbor: 192.168.110.1, Nexthop: 192.168.110.1
  Upstream IF: vlan110
    Upstream State: Forwarding
    Upstream Prune Limit Timer Expiry: 0 secs
    Assert State: NoInfo
  Source Active Timer Expiry: 180 secs
  State Refresh Timer Expiry: 0 secs
  Downstream IF List:
    vlan130:, not in 'olist'
      Downstream State: NoInfo
```

```
      Assert State: NoInfo
    vlan20:, in 'olist'
      Downstream State: NoInfo
      Assert State: NoInfo
```

Show the IP multicast routing information base when PIM-SM is in operation.

```
SWX3220#show ip pim mroute
IP Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 2
(S,G) Entries: 2
(S,G,rpt) Entries: 2
FCR Entries: 0

(*, 239.0.0.1)
RP: 192.168.120.1
RPF nbr: 192.168.110.1
RPF idx: vlan110
Upstream State: JOINED
 Local     ..i.............................
 Joined    ................................
 Asserted  ................................
FCR:

(192.168.30.100, 239.0.0.1)
RPF nbr: 192.168.110.1
RPF idx: vlan110
SPT bit: 1
Upstream State: JOINED
 Local     ................................
 Joined    ................................
 Asserted  ................................
 Outgoing  ..o.............................

(192.168.30.100, 239.0.0.1, rpt)
RP: 192.168.120.1
RPF nbr: 192.168.110.1
RPF idx: vlan110
Upstream State: NOT PRUNED
 Local     ................................
 Pruned    ................................
 Outgoing  ..o.............................
```

Show detailed information for the IP multicast routing information base when PIM-SM is in operation.

```
SWX3220#show ip pim mroute 239.0.0.1 detail
(*, 239.0.0.1) Uptime: 00:13:40
RP: 192.168.120.1, RPF nbr: 192.168.110.1, RPF idx: vlan110
  Upstream:
   State: JOINED, SPT Switch: Enabled, JT Expiry: 40 secs
   Macro state: Join Desired,
  Downstream:
   vlan20:
     State: NO INFO, ET: off, PPT: off
     Assert State: NO INFO, AT: off
      Winner: 0.0.0.0, Metric: 4294967295, Pref: 4294967295, RPT bit: on
     Macro state: Could Assert, Assert Track
  Local Olist:
   vlan20

(192.168.30.100, 239.0.0.1) Uptime: 00:09:20
  RPF nbr: 192.168.110.1, RPF idx: vlan110
  Upstream:
   State: JOINED, SPT Bit: on, JT Expiry: 41 secs, KAT Expiry: 70 secs
   Macro state: Join Desired,
  Downstream:
  Inherited Olist:
   vlan20

(192.168.30.100, 239.0.0.1, rpt) Uptime: 00:09:20
RP: 192.168.120.1RPF nbr: 192.168.110.1, RPF idx: vlan110
  Upstream:
```

```
   State: NOT PRUNED, OT: off
   Macro state: RPT Join,
  Downstream:
  Inherited Olist:
   vlan20
```

8.4.29 Show PIM neighbor information

[Syntax]

show ip pim neighbor [*ifname*] [*address*] [detail]

[Keyword]

detail	:	Shows detailed information

[Parameter]

ifname	:	Interface name
address	:	IP address of neighbor interface

[Initial value]

none

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the PIM neighbor information.

[Example]

Show the PIM neighbor information when PIM-DM is in operation.

```
SWX3220#show ip pim neighbor
Neighbor        Interface          Uptime/Expires            Ver     DR
Address                                                            Priority/Mode
192.168.110.1   vlan110            02:14:48/00:01:28         v2    N /
192.168.130.2   vlan130            00:37:50/00:01:27         v2    N /
```

Show the detailed PIM neighbor information when PIM-DM is in operation.

```
SWX3220#show ip pim neighbor detail
Nbr 192.168.110.1 (vlan110)
 Expires in 88 seconds, uptime 02:15:48

Nbr 192.168.130.2 (vlan130)
 Expires in 87 seconds, uptime 00:38:50
```

Show the PIM neighbor information when PIM-SM is in operation.

```
SWX3220#show ip pim neighbor
Neighbor        Interface          Uptime/Expires            Ver     DR
Address                                                            Priority/Mode
192.168.110.1   vlan110            00:19:30/00:01:40         v2    1 /
```

Show the detailed PIM neighbor information when PIM-SM is in operation.

```
Nbr 192.168.110.1 (vlan110)
 Expires in 81 seconds, uptime 00:19:19
 Holdtime: 105 secs, DR priority: 1, Gen ID: 277507370,
 Interface ID: Router-ID: 192.168.120.1 Local-ID: 410,
```

8.4.30 Show necthop information

[Syntax]

show ip pim nexthop

[Initial value]

none

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows next hop information.

[Example]

Shows next hop information when PIM-DM is in operation.

```
SWX3220#show ip pim nexthop
Flags: N = New, R = RP, S = Source, U = Unreachable
Destination     Type  Nexthop   Nexthop         Nexthop  Nexthop Metric Pref  Refcnt
                        Num     Addr            Ifindex  Name
_____________________________________________________________________________________
192.168.20.100  ..S.   1         0.0.0.0         320      vlan20  3      1     1
192.168.30.100  ..S.   1         192.168.110.1   410      vlan110 20     110   2
```

Shows next hop information when PIM-SM is in operation.

```
SWX3220#show ip pim nexthop
Flags: N = New, R = RP, S = Source, U = Unreachable
Destination     Type  Nexthop   Nexthop         Nexthop  Nexthop Metric Pref  Refcnt
                        Num     Addr            Ifindex  Name
_____________________________________________________________________________________
192.168.20.100  ..S.   1         0.0.0.0         320      vlan20  3      1     3
192.168.30.100  ..S.   1         192.168.110.1   410      vlan110 20     110   3
192.168.110.1   ..S.   1         0.0.0.0         410      vlan110 3      1     1
192.168.120.1   .RS.   1         192.168.110.1   410      vlan110 20     110   8
192.168.130.1   .R..   1         0.0.0.0         430      vlan130 3      1     1
192.168.130.2   N..U   0         0.0.0.0         -1               -1     255   1
```

8.4.31 Show RP information

[Syntax]

show ip pim rp mapping

[Initial value]

none

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the rendezvous point (RP) information.

[Example]

Shows the static rendezvous point (RP) information.

```
SWX3220#show ip pim rp mapping
PIM Group-to-RP Mappings
Group(s): 238.0.0.0/8, Static
    RP: 172.17.10.1
         Uptime: 00:00:13
Group(s): 239.0.0.0/8, Static
    RP: 172.17.10.2
         Uptime: 00:00:23
```

Shows the dynamic rendezvous point (RP) information.

```
SWX3220#show ip pim rp mapping
PIM Group-to-RP Mappings
Group(s): 224.0.0.0/4
  RP: 192.168.120.1
    Info source: 192.168.120.1, via bootstrap, priority 190
         Uptime: 00:00:42, expires: 00:01:48
```

8.4.32 Show RP selection candidate

[Syntax]

show ip pim rp-hash *group*

[Parameter]

group	:	Multicast group address (A.B.C.D)

[Initial value]

none

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the rendezvous point (RP) selection candidate for the specified multicast group.

[Example]

Show the rendezvous point (RP) selection candidate for multicast group 224.0.1.3 (static RP settings only).

```
SWX3220#show ip pim rp-hash 224.0.1.3
    RP: 192.168.40.1
```

Show the rendezvous point (RP) selection candidate for multicast group 224.0.1.3 (dynamic settings only).

```
SWX3220#show ip pim rp-hash 224.0.1.3
    RP: 192.168.30.254
    Info source: 192.168.30.254, via bootstrap
```

8.4.33 Show BSR information

[Syntax]

show ip pim bsr-router

[Initial value]

none

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the bootstrap router (BSR) information.

[Example]

Show the BSR information (during non-BSR operations).

```
SWX3220#show ip pim bsr-router
PIMv2 Bootstrap information
  BSR address: 192.168.120.1
  Uptime:      00:20:37, BSR Priority: 70, Hash mask length: 0
  Expires:     00:01:33
  Role: Non-candidate BSR
  State: Accept Preferred
```

Show the BSR information (during BSR operations).

```
SWX3220#show ip pim bsr-router
PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
  BSR address: 192.168.120.1
  Uptime:      00:29:03, BSR Priority: 70, Hash mask length: 0
  Next bootstrap message in 00:00:04
  Role: Candidate BSR
  State: Elected BSR

  Candidate RP: 192.168.120.1(vlan120)
```

```
    Advertisement interval 60 seconds
    Next C-RP advertisement in 00:00:03
```

8.4.34 Clear RP information

[Syntax]

clear ip pim sparse-mode bsr rp-set *

[Initial value]

none

[Input mode]

privileged EXEC mode

[Description]

Clears the rendezvous point (RP) information learned from the bootstrap router (BSR).

[Example]

Clear all RP information.

```
SWX3220#clear ip pim sparse-mode bsr rp-set *
```

8.5 IGMP

8.5.1 Set IGMP

[Syntax]

ip igmp *type*
no ip igmp

[Parameter]

type : Specifies the action for the IGMP

Setting value	Description
enable	Enable the IGMP
disable	Disable the IGMP

[Initial value]

ip igmp disable

[Input mode]

interface mode

[Description]

Enables IGMP on the applicable interface, even when multicast routing protocols such as PIM are not in effect. When multicast routing protocols are in effect, IGMP will be enabled regardless of the settings for this command.

If this command is executed with the "no" syntax or "disable" is set as a parameter, all IGMP-related settings will be initialized (including IGMP proxy settings), and IGMP will be disabled when the multicast routing protocol is not in effect.

[Note]

When a multicast routing protocol is enabled for the applicable interface, this command should be enabled. When a multicast routing protocol is disabled, we recommend that this command should be disabled.

[Example]

Enable IGMP for VLAN2.

```
SWX3220(config)#interface vlan2
SWX3220(config-if)#ip igmp enable
```

8.5.2 Set IGMP version

[Syntax]

ip igmp version *version*

no ip igmp version

[Parameter]

version : <2-3>

IGMP version

[Initial value]

none

[Input mode]

interface mode

[Description]

Sets the IGMP version on the applicable interface.

If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

On VLAN #2, set the IGMP version to 2.

```
SWX3220(config)#interface vlan2
SWX3220(config-if)#ip igmp version 2
```

8.5.3 Set Query Interval

[Syntax]

ip igmp query-interval *time*
no ip igmp query-interval

[Parameter]

time : <1-18000>

General Membership Query transmission interval (second)

[Initial value]

ip igmp query-interval 125

[Input mode]

interface mode

[Description]

Sets the transmission interval for General Membership Query (Query Interval) on the applicable interface.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

This should be set to a greater value than the setting in the **ip igmp query-max-response-time** command.

[Example]

Set the transmission interval for the General Membership Query to 120 seconds.

```
SWX3220(config)#interface vlan2
SWX3220(config-if)#ip igmp query-interval 120
```

8.5.4 Set General Membership Query maximum reply time

[Syntax]

ip igmp query-max-response-time *time*
no ip igmp query-max-response-time

[Parameter]

time : <1-240>

Maximum reply time for a General Membership Query (seconds)

[Initial value]

ip igmp query-max-response-time 10

[Input mode]

interface mode

[Description]

Sets the maximum reply time (Max Response Time) for the IGMP General Membership Query on the applicable interface.

If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

Set the maximum reply time for General Membership Query to 8 seconds.

```
SWX3220(config)#interface vlan2
SWX3220(config-if)#ip igmp query-max-response-time 8
```

8.5.5 Set Last Member Query Interval

[Syntax]

ip igmp last-member-query-interval *interval*
no ip igmp last-member-query-interval

[Parameter]

interval	:	<1000-25500>(millisecond) Transmission interval for Group-Specific Membership Queries that are sent after a Leave Group message is received on the applicable interface.

[Initial value]

ip igmp last-member-query-interval 1000

[Input mode]

interface mode

[Description]

Sets the interval for transmitting Group-Specific Membership Queries (Last Member Query Interval) on the applicable interface, after receiving a Leave Group message.

If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

Set the interval between sending transmit Group-Specific Membership Queries after receiving a Leave Group message to 2 seconds.

```
SWX3220(config)#interface vlan2
SWX3220(config-if)#ip igmp last-member-query-interval 2000
```

8.5.6 Set Last Member Query Count

[Syntax]

ip igmp last-member-query-count *count*
no ip igmp last-member-query-count

[Parameter]

count	:	<2-7> Number of times to transmit group-specific queries on the applicable interface, after receiving a Leave Group message.

[Initial value]

ip igmp last-member-query-count 2

[Input mode]

interface mode

[Description]

Sets the number of times to transmit group-specific queries (Last Member Query Count) on the applicable interface, after receiving a Leave Group message.

If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

Set the number of times to transmit group-specific queries after receiving a Leave Group message to 3.

```
SWX3220(config)#interface vlan2
SWX3220(config-if)#ip igmp last-member-query-count 3
```

8.5.7 Set Other Querier Present Interval

[Syntax]

ip igmp querier-timeout *time*
no ip igmp querier-timeout

[Parameter]

time : <60-300>

Time after which no other queriers are determined to exist. (seconds)

[Initial value]

none

[Input mode]

interface mode

[Description]

Sets the standby time on the applicable interface after which other queriers stop query transmission and inherit querier operations (Other Querier Present Interval).

If this command is executed with the "no" syntax, the setting returns to the default.

The default setting is Other Querier Present Interval = (Robustness Variable x Query Interval) + (Query Response Time x 0.5). When all parameters are at their default value, this would be (2 x 125) + (10 x 0.5) = 255 seconds.

[Example]

Wait for 120 seconds before determining that no other queriers exist.

```
SWX3220(config)#interface vlan2
SWX3220(config-if)#ip igmp querier-timeout 120
```

8.5.8 Set Robustness Variable

[Syntax]

ip igmp robustness-variable *variable*
no ip igmp robustness-variable

[Parameter]

variable : <2-7>

Parameter that indicates robustness against packet loss.

[Initial value]

ip igmp robustness-variable 2

[Input mode]

interface mode

[Description]

Sets the Robustness Variable of the IGMP operating parameter for the applicable interface.

The greater the Robustness Variable, the greater the robustness against packet loss will be.

If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

Set the Robustness Variable to 3.

```
SWX3220(config)#interface vlan2
SWX3220(config-if)#ip igmp robustness-variable 3
```

8.5.9 Set IGMP immediate-leave

[Syntax]

ip igmp immediate-leave group-list *listnum*
no ip igmp immediate-leave

[Parameter]

listnum : <1-2000>
ID of IPv4 access list

[Initial value]

none

[Input mode]

interface mode

[Description]

Enables IGMP fast-leave for the applicable interface.

If this command is executed with the "no" syntax, disables IGMP fast-leave.

[Note]

When fast-leave is enabled, the entry for IGMP group membership are deleted immediately after the IGMPv2 Leave Group message is received.

If there are multiple multicast receivers on the VLAN, fast-leave should not be enabled.

[Example]

Enable fast-leave for multicast groups on VLAN #2 within the range of 225.192.20.0 to 225.192.20.255.

```
SWX3220(config)#interface vlan2
SWX3220(config-if)#ip igmp immediate-leave group-list 1
SWX3220(config-if)#exit
SWX3220(config)#access-list 1 permit any 225.192.20.0 0.0.0.255 any
```

8.5.10 Set source address check for IGMP packets

[Syntax]

ip igmp check source-address *type*
no ip igmp check source-address

[Parameter]

type : Address check operations

Setting value	Description
disable	Disables source address checking
enable	Enables source address checking

[Input mode]

interface mode

[Description]

If disable is specified, this disables IGMP packet (Report/Leave message) source address checking for the applicable interface.

If this command is executed using the "no" syntax or when enable is specified, source address checking is enabled.

Default setting is enabled.

When source address checking is enabled, this checks the source IP address for IGMP packets; and if the address falls outside of the subnet address range to which the receiving interface belongs, the IGMP packet is discarded.

[Note]

Address checks will not be performed on IGMP packets with a source IP address of 0.0.0.0.

[Example]

Disable source address checking for IGMP.

```
SWX3220(config)# interface vlan2
SWX3220(config-if)# ip igmp check source-address disable
```

8.5.11 Set limit multicast group membership

[Syntax]

ip igmp access-group *listnum*
no ip igmp access-group

[Parameter]

listnum	:	<1-2000> ID of IPv4 access list

[Initial value]

none

[Input mode]

interface mode

[Description]

Applies the IPv4 access list to the applicable interface, and limits membership to which multicast receivers may join.

If this command is executed with the "no" syntax, cancels the limitations on a multicast group.

[Note]

The IPv4 access list should be set to allow (permit) the multicast group that will be added.

[Example]

Limit the range of multicast groups that can join within 225.2.0.0 to 225.2.255.255.

```
SWX3220(config)#access-list 1 permit any 225.2.0.0 0.0.0.255 any
SWX3220(config)#interface vlan2
SWX3220(config-if)#ip igmp access-group 1
```

8.5.12 Set maximum number of registerable groups for IGMP group membership

[Syntax]

ip igmp limit *number* [except *listnum*]
no ip igmp limit

[Keyword]

except	:	Specifies a multicast group for which the number of registrants is not limited

[Parameter]

number	:	<1-2097152> Maximum number of group membership entries
listnum	:	<1-2000> ID of IPv4 access list

[Initial value]

none

[Input mode]

global configuration mode, interface mode

[Description]

Sets the maximum number of registrants for IGMP group membership.

This sets the maximum number system-wide in global configuration mode, and the maximum number for the interface in interface mode.

Applying the IPv4 access list will allow for specific multicast groups to be excluded from the maximum number limitation.

If this command is executed with the "no" syntax, deletes the maximum number of registrants.

[Note]

The IPv4 access list should be set to allow (permit) the multicast group that will be excluded.

[Example]

This sets the maximum number of registrants for IGMP group membership to 100, and excludes multicast group 239.0.0.1 from the limitations.

```
SWX3220(config)#access-list 1 permit any 239.0.0.1 0.0.0.0 any
SWX3220(config)#ip igmp limit 100 except 1
```

8.5.13 Set IGMP group membership static entry

[Syntax]

ip igmp static-group *group* [source *source*]
no ip igmp static-group

[Keyword]

source	:	Specifies the IP address of the multicast sender

[Parameter]

group	:	Multicast group address (A.B.C.D)
source	:	IPv4 address of a multicast sender (A.B.C.D)

[Initial value]

none

[Input mode]

interface mode

[Description]

Registers IGMP group membership static entries for the applicable interface.

If this command is executed with the "no" syntax, delete entries.

[Note]

The IP address of the multicast sender can be specified only when using IGMPv3.

Setting this command will determine that a multicast receiver statically exists on the applicable interface, and the multicast traffic will be forwarded. However, this unit will not receive multicast traffic, and an IGMP report will not be transmitted.

[Example]

Add a static IGMP group member (multicast group: 226.1.2.4; multicast sender: 10.0.0.1).

```
SWX3220(config)#interface vlan2
SWX3220(config-if)#ip igmp static-group 226.1.2.4 source 10.0.0.1
```

8.5.14 Set SSM mapping function

[Syntax]

ip igmp ssm-map *type*
no ip igmp ssm-map

[Parameter]

type	:	SSM mapping function operations

Setting value	Description
disable	Disables SSM mapping.
enable	Enables SSM mapping.

[Initial value]

ip igmp ssm-map enable

[Input mode]

global configuration mode

[Description]

Disables the IGMP SSM (Source Specific Multicast) mapping function.

If this command is executed using the "no" syntax or if enable is specified, the SSM mapping function will be enabled.

[Note]

Enables mapping for the multicast group address and multicast sender(s). This will allow multicast receivers that are compatible only with IGMPv2 to use PIM-SSM.

The entire multicast group can be specified as an SSM range by default, not just the standard SSM range.

[Example]

Disable the SSM mapping function.

```
SWX3220(config)#ip igmp ssm-map disable
```

8.5.15 Set SSM mapping static entry

[Syntax]

ip igmp ssm-map static *listnum source*
no ip igmp ssm-map static *listnum source*

[Parameter]

listnum	:	<1-2000> ID of IPv4 access list
source	:	The IPv4 address of a multicast sender (A.B.C.D)

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Sets the static entries for IGMP SSM mapping.

The IPv4 address of a multicast sender can be associated with the multicast group specified in the IPv4 access list.

This will cause the requests for membership to the relevant IGMPv2 group to be processed as requests for membership, with which the associated source address is specified.

If this command is executed with the "no" syntax, deletes the specified static entry.

[Note]

The IPv4 access list must be set to allow (permit) the multicast group that is associated with the IPv4 address of the multicast sender.

The entire multicast group can be specified as an SSM range by default, not just the standard SSM range.

[Example]

Associate multicast sender IPv4 address 192.168.100.100 with multicast group 224.1.1.0 through 224.1.1.255.

```
SWX3220(config)# ip igmp ssm-map static 1 192.168.100.100
SWX3220(config)# access-list 1 permit any 224.1.1.0 0.0.0.255 any
```

8.5.16 Set downstream interface for the IGMP proxy

[Syntax]

ip igmp mroute-proxy *ifname*
no ip igmp mroute-proxy

[Parameter]

ifname	:	Downstream interfaces for the IGMP proxy (multicast router side)

[Initial value]

none

[Input mode]

interface mode

[Description]

Sets the applicable interface to a downstream interface for the IGMP proxy (on the multicast receiver side), and specifies the upstream interface (multicast router side).

If this command is executed with the "no" syntax, disables the operations of the IGMP proxy as a downstream interface.

[Note]

When using the IGMP proxy function, the following settings should be made.

- Enable the multicast routing function using the **ip multicast-routing** command.
- Enable IGMP using the **ip igmp** command on both upstream and downstream interfaces.
- Set the **ip igmp proxy-service** command beforehand on the specified upstream interface.

Disable the multicast routing protocol on the interfaces that will use the IGMP proxy function.

Multiple downstream interfaces can be specified for a single upstream interface.

[Example]

Set VLAN #2 as an IGMP proxy downstream interface, and set VLAN #3 as an IGMP upstream interface.

```
SWX3220(config)#interface vlan2
SWX3220(config-if)#ip igmp mroute-proxy vlan3
```

8.5.17 Set IGMP proxy upstream interface

[Syntax]

ip igmp proxy-service
no ip igmp proxy-service

[Initial value]

none

[Input mode]

interface mode

[Description]

Set the applicable interface as an IGMP proxy upstream interface (multicast router side).

If this command is executed with the "no" syntax, disables the operations of the IGMP proxy as a upstream interface.

[Note]

When using the IGMP proxy function, the following settings should be made.

- Enable the multicast routing function using the **ip multicast-routing** command.
- Enable IGMP using the **ip igmp** command on both upstream and downstream interfaces.
- Make sure to configure using this command before setting the downstream interfaces using the **ip igmp mroute-proxy** command.

Disable the multicast routing protocol on the interfaces that will use the IGMP proxy function.

Multiple downstream interfaces can be specified for a single upstream interface.

[Example]

Set VLAN #3 as an IGMP proxy upstream interface.

```
SWX3220(config)#interface vlan3
SWX3220(config-if)#ip igmp proxy-service
```

8.5.18 Show multicast group information

[Syntax]

show ip igmp groups [*ifname*] [*group*] [detail]

[Keyword]

detail	:	Detailed information

[Parameter]

ifname	:	Interface name
group	:	Multicast group address (A.B.C.D)

[Initial value]

none

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the multicast group learned by the IGMP.

[Example]

Show the multicast group information for all interfaces.

```
SWX3220#show ip igmp groups detail
IGMP Connected Group Membership Details
Flags: (M - SSM Mapping, R - Remote, L - Local,
SG - Static Group, SS - Static Source)
Interface:    vlan1
Group:         224.1.1.1
Flags:         L
Uptime:    00:00:04
Group mode:     Exclude (Expires: 00:04:15, Static)
Last reporter:     3.3.3.3
Group source list: (R - Remote, M - SSM Mapping, S - Static, L - Local)
Include Source List :

 Source Address Uptime v3 Exp Fwd Flags
 2.2.2.2 00:00:04 stopped Yes L
```

8.5.19 Show IGMP interface information

[Syntax]

show ip igmp interface [*ifname*]

[Parameter]

ifname	:	Interface name

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows IGMP-related information for a specified interface or for all interfaces.

[Example]

Show IGMP-related information for all interfaces on which IGMP is enabled.

```
SWX3220#show ip igmp interface
Interface vlan1 (Index 301)
 IGMP Enabled, Active, Querier, Version 3 (default)
```

```
Internet address is 192.168.100.240
IGMP interface has 0 group-record states
IGMP Interface statistics:
v1-reports: 0
v2-reports: 0, v2-leaves: 0
v3-reports: 0
IGMP robustness variable is 2
IGMP query interval is 125 seconds
IGMP querier timeout is 255 seconds
IGMP max query response time is 10 seconds
Group Membership interval is 260 seconds
IGMP Last member query count is 2
Last member query response interval is 1000 milliseconds
Source Address checking is enabled
```

8.5.20 Show IGMP SSM map information

[Syntax]

show ip igmp ssm-map [*group*]

[Parameter]

group	:	Multicast group address (A.B.C.D)

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the IGMP SSM map information.

[Example]

Show the IGMP SSM map information.

```
SWX3220#show ip igmp ssm-mapping
SSM Mapping: Enabled
Database: Static mappings configured
```

Show IGMP SSM map information for multicast group 232.1.1.4.

```
SWX3220#show ip igmp ssm-map 232.1.1.4
Group address: 232.1.1.4
Database : Static
Source list : 172.16.8.5
            : 172.16.8.6
```

8.5.21 Show IGMP proxy interface information

[Syntax]

show ip igmp proxy [groups [*ifname*] [*groups*] [detail]]

[Keyword]

groups	:	Shows the IGMP proxy group information.
detail	:	Detailed information

[Parameter]

groups	:	Multicast group address (A.B.C.D)
ifname	:	VLAN interface name

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows IGMP-related information for interfaces on which the IGMP proxy is enabled.

[Example]

Show IGMP-related information for all interfaces on which the IGMP proxy is enabled.

```
SWX3220#show ip igmp proxy groups
IGMP Connected Proxy Group Membership
Group Address    Interface            State     Member state
239.0.0.1        vlan2                Active    Delay

SWX3220#show ip igmp proxy groups detail
Interface:      vlan2
Group:          239.0.0.1
Group mode:     Exclude
State:          Active
Member state:   Delay
Source list is empty
```

8.5.22 Clear IGMP group membership

[Syntax]

clear ip igmp [*entry*]

[Parameter]

entry : Entries to clear

Setting value	Description
group *group* [*ifname*]	Specifies the multicast group entries to be cleared
interface *ifname*	Specifies the interface entries to be cleared

group : Multicast group address (A.B.C.D)

"*" indicates all entries

ifname : Interface name

[Input mode]

privileged EXEC mode

[Description]

Clears IGMP group membership entry

[Note]

IGMP group membership that was statically registered will not be deleted.

[Example]

Delete the IGMP group membership entries for multicast group 224.1.1.1.

```
SWX3220#clear ip igmp group 224.1.1.1
```

Chapter 9

Traffic control

9.1 ACL

9.1.1 Generate IPv4 access list

[Syntax]

access-list *ipv4-acl-id* [*seq_num*] *action protocol src-info* [*src-port*] *dst-info* [*dst-port*] [**ack**] [**fin**] [**psh**] [**rst**] [**syn**] [**urg**]
no access-list *ipv4-acl-id* [*seq_num*] [*action protocol src-info* [*src-port*] *dst-info* [*dst-port*] [**ack**] [**fin**] [**psh**] [**rst**] [**syn**] [**urg**]]

[Keyword]

ack : If tcp is specified as the protocol, the ACK flag of the TCP header is specified as a condition.

fin : If tcp is specified as the protocol, the FIN flag of the TCP header is specified as a condition.

psh : If tcp is specified as the protocol, the PSH flag of the TCP header is specified as a condition.

rst : If tcp is specified as the protocol, the RST flag of the TCP header is specified as a condition.

syn : If tcp is specified as the protocol, the SYN flag of the TCP header is specified as a condition.

urg : If tcp is specified as the protocol, the URG flag of the TCP header is specified as a condition.

[Parameter]

ipv4-acl-id : <1-2000>

ID of IPv4 access list

seq_num : <1-65535>

Sequence number. Specifies the position of the entry within the applicable access list.

If the sequence number is omitted, the entry is added to the end of the list. At this time, the new entry is automatically given a number that is 10 greater than the last existing entry. (If an entry is initially added without a sequence number, its entry number will be 10.)

action : Specifies the action for the access condition

Setting value	Description
deny	"Deny" the condition
permit	"Permit" the condition

protocol : Specifies the applicable protocol type

Setting value	Description
<0-255>	Protocol number of the IP header
any	All IPv4 packets
tcp	TCP packets
udp	UDP packets

src-info : Specifies the transmission-source IPv4 address that is the condition

Setting value	Description
A.B.C.D E.F.G.H	Specifies an IPv4 address (A.B.C.D) with wildcard bits (E.F.G.H)
A.B.C.D/M	Specifies an IPv4 address (A.B.C.D) with subnet mask length (Mbit)
host A.B.C.D	Specifies a single IPv4 address (A.B.C.D)
any	Applies to all IPv4 addresses

src-port : <0-65535>

If protocol is specified as tcp or udp, this specifies the transmission source port number <0-65535> that is the condition. This can also be omitted.

Method of specifying	Description
eq X	Specify port number (X)
range X Y	Specify port numbers (X) through (Y)

dst-info : Specifies the destination IPv4 address information that is the condition

Setting value	Description
A.B.C.D E.F.G.H	Specifies an IPv4 address (A.B.C.D) with wildcard bits (E.F.G.H)
A.B.C.D/M	Specifies an IPv4 address (A.B.C.D) with subnet mask length (Mbit)
host A.B.C.D	Specifies a single IPv4 address (A.B.C.D)
any	Applies to all IPv4 addresses

dst-port : <0-65535>

If protocol is specified as tcp or udp, this specifies the destination port number <0-65535> that is the condition. This can also be omitted.

Method of specifying	Description
eq X	Specify port number (X)
range X Y	Specify port numbers (X) through (Y)

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Generates an IPv4 access list.

Multiple conditions (maximum 768) can be specified for the generated access list.

To apply the generated access list, use the **access-group** command of interface mode.

If the "no" syntax is used to specify "action" and following, the IPv4 access list that matches all conditions is deleted.

If the "no" syntax is used without specifying "action" and following, the IPv4 access list of the matching ID of access list is deleted.

[Note]

An access list that is applied to LAN/SFP port and logical interface cannot be deleted using the "no" syntax. You must first cancel the application, and then delete the access list.

For both src-port and dst-port, you can use "range" to specify a range; however, for the entire system, only one IPv4 access list that specifies a range in this way can be applied system-wide by using the **access-group** or **vlan filter** commands.

[Example]

Create access list #1 that denies communication from the source segment 192.168.1.0/24 to the destination 172.16.1.1.

```
SWX3220(config)#access-list 1 deny any 192.168.1.0 0.0.0.255 host 172.16.1.1
```

Delete IPv4 access list #1.

```
SWX3220(config)#no access-list 1
```

9.1.2 Adding a description for IPv4 access list

[Syntax]

access-list *ipv4-acl-id* **description** *line*
no access-list *ipv4-acl-id* **description**

[Parameter]

ipv4-acl-id : <1-2000>
ID of the IPv4 access list to which to add a description

line : Description to add. Can be up to 32 ASCII characters

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Add a description to the generated IPv4 access list.

If this command is executed with the "no" syntax, the IPv4 description is cleared.

[Note]

A description can be added with this command even after applying an access list to LAN/SFP port and logical interface. (The later description will overwrite it)

[Example]

Create IPv4 access list #1 that denies communication from the 192.168.1.0/24 sending source segment to 172.16.1.1, and add the description of "Test".

```
SWX3220(config)#access-list 1 deny any 192.168.1.0 0.0.0.255 host 172.16.1.1
SWX3220(config)#access-list 1 description Test
```

9.1.3 Apply IPv4 access list

[Syntax]

access-group *ipv4-acl-id direction*
no access-group *ipv4-acl-id direction*

[Parameter]

ipv4-acl-id : <1-2000>
ID of IPv4 access list to apply

direction : Specifies the direction of applicable frames

Setting value	Description
in	Apply to received frames
out	Apply to transmitted frames

[Initial value]

none

[Input mode]

interface mode

[Description]

Applies an IPv4 access list to both LAN/SFP port and logical interface.

If the received/transmitted frame matches the conditions in the access list, the action in the access list will be the action (permit, deny) for the corresponding frame.

If this command is executed with the "no" syntax, the applied access list is deleted from both LAN/SFP port and logical interface.

[Note]

Only one access list for each direction can be registered for incoming frames (in) and for outgoing frames (out) on the same interface.

The access list for transmitted frames can only be applied to LAN/SFP port.

Only one IPv4 access list for which the port number range (range X Y) is specified can be applied for the entire system, and it cannot be applied to outgoing frames (out).

An LAN/SFP port for which an incoming frames access list is specified cannot be associated to an logical interface.

An incoming frames access list cannot be applied to an LAN/SFP port that is associated with an logical interface. However, if an access list setting for incoming frames is specified for an LAN/SFP port that is associated with an logical interface in the startup config, then the setting for the lowest-numbered port is applied to the logical interface.

[Example]

Apply extended IPv4 access list #1 to received frames of LAN port #1.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#access-group 1 in
```

9.1.4 Generate IPv6 access list

[Syntax]

access-list *ipv6-acl-id* [*seq_num*] *action src-info*
no access-list *ipv6-acl-id* [*seq_num*] [*action src-info*]

[Parameter]

ipv6-acl-id : <3001-4000>

ID of IPv6 access list

seq_num : <1-65535>

Sequence number. Specifies the position of the entry within the applicable access list.

If the sequence number is omitted, the entry is added to the end of the list. At this time, the new entry is automatically given a number that is 10 greater than the last existing entry. (If an entry is initially added without a sequence number, its entry number will be 10.)

action : Specifies the action for the access condition

Setting value	Description
deny	"Deny" the condition
permit	"Permit" the condition

src-info : Specifies the transmission-source IPv6 address that is the condition

Setting value	Description
X:X::X:X/M	Specifies an IPv6 address (X:X::X:X) with subnet mask length (Mbit)
any	Applies to all IPv6 addresses

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Generates an IPv6 access list.

Multiple conditions (maximum 768) can be specified for the generated access list.

To apply the generated access list, use the **access-group** command of interface mode.

If the "no" syntax is used to specify "action" and following, the IPv6 access list that matches all conditions is deleted.

If the "no" syntax is used without specifying "action" and following, the IPv6 access list of the matching ID of access list is deleted.

[Note]

An access list that is applied to LAN/SFP port and logical interface cannot be deleted using the "no" syntax. Before you can delete the access list, you must rescind the application of that list.

This command cannot be used if the stack function is enabled.

[Example]

Create IPv6 access list #3002 which will deny frames from 3ffe:506::/32.

```
SWX3220(config)#access-list 3002 deny 3ffe:506::/32
```

Delete IPv6 access list #3002.

```
SWX3220(config)#no access-list 3002
```

9.1.5 Adding a description for IPv6 access list

[Syntax]

access-list *ipv6-acl-id* **description** *line*
no access-list *ipv6-acl-id* **description**

[Parameter]

ipv6-acl-id	:	<3001-4000> ID of the IPv6 access list to which to add a description
line	:	Description to add. Can be up to 32 ASCII characters

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Add a description to the generated IPv6 access list.

If this command is executed with the "no" syntax, the IPv6 descriptive text is cleared.

[Note]

A description can be added with this command even after applying an access list to LAN/SFP port and logical interface. (It will be overwritten with the later description)

This command cannot be used if the stack function is enabled.

[Example]

Create IPv6 access list #3002 that denies packets from 3ffe:506::/32, and add the description of "Test".

```
SWX3220(config)#access-list 3002 deny 3ffe:506::/32
SWX3220(config)#access-list 3002 description Test
```

9.1.6 Apply IPv6 access list

[Syntax]

access-group *ipv6-acl-id direction*

no access-group *ipv6-acl-id direction*

[Parameter]

ipv6-acl-id : <3001-4000>

ID of IPv6 access list to apply

direction : Specifies the direction of applicable frames

Setting value	Description
in	Apply to received frames
out	Apply to transmitted frames

[Initial value]

none

[Input mode]

interface mode

[Description]

Applies an IPv6 access list to both LAN/SFP port and logical interface.

If the received/transmitted frame matches the conditions in the access list, the action in the access list will be the action (permit, deny) for the corresponding frame.

If this command is executed with the "no" syntax, the applied access list is deleted from both LAN/SFP port and logical interface.

[Note]

Only one access list for each direction can be registered for incoming frames (in) and for outgoing frames (out) on the same interface.

The access list for transmitted frames can only be applied to LAN/SFP port.

The following restrictions apply.

An LAN/SFP port for which an incoming frames access list is specified cannot be associated to an logical interface.

An incoming frames access list cannot be applied to an LAN/SFP port that is associated with an logical interface. However, if an access list setting for incoming frames is specified for an LAN/SFP port that is associated with an logical interface in the startup config, then the setting for the lowest-numbered port is applied to the logical interface.

This command cannot be used if the stack function is enabled.

[Example]

Apply IPv6 access list #3002 to received frames of LAN port #1.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#access-group 3002 in
```

9.1.7 Generate MAC access list

[Syntax]

access-list *mac-acl-id* [*seq_num*] *action src-info dst-info*
no access-list *mac-acl-id* [*seq_num*] [*action src-info dst-info*]

[Parameter]

mac-acl-id : <2001-3000>

ID of MAC access list

seq_num : <1-65535>

Sequence number. Specifies the position of the entry within the applicable access list.

If the sequence number is omitted, the entry is added to the end of the list. At this time, the new entry is automatically given a number that is 10 greater than the last existing entry. (If an entry is initially added without a sequence number, its entry number will be 10.)

action : Specifies the action for the access condition

Setting value	Description
deny	"Deny" the condition
permit	"Permit" the condition

src-info : Specifies the transmission-source MAC address information that is the condition

Setting value	Description
HHHH.HHHH.HHHH WWWW.WWWW.WWWW	Specifies the MAC address (HHHH.HHHH.HHHH) with wildcard bits (WWWW.WWWW.WWWW)
host HHHH.HHHH.HHHH	Specifies an individual MAC address (HHHH.HHHH.HHHH)
any	Applies to all MAC addresses

dst-info : Specifies the destination MAC address information that is the condition

Setting value	Description
HHHH.HHHH.HHHH WWWW.WWWW.WWWW	Specifies the MAC address (HHHH.HHHH.HHHH) with wildcard bits (WWWW.WWWW.WWWW)
host HHHH.HHHH.HHHH	Specifies an individual MAC address (HHHH.HHHH.HHHH)
any	Applies to all MAC addresses

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Generates a MAC access list.

Multiple conditions (maximum 768) can be specified for the generated access list.

To apply the generated access list, execute the **access-group** command in interface mode.

If the "no" syntax is used to specify "action" and following, the MAC access list that matches all conditions is deleted.

If the "no" syntax is used without specifying "action" and following, the MAC access list of the matching ID of access list is deleted.

[Note]

An access list that is applied to LAN/SFP port and logical interface cannot be deleted using the "no" syntax. You must first cancel the application, and then delete the access list.

"W" and "H" represent a single character from the range 0-9, a-f, and A-F.

[Example]

Create MAC access list #2001 which denies frames from MAC address 00-A0-DE-12-34-56.

```
SWX3220(config)#access-list 2001 deny 00A0.DE12.3456 0000.0000.0000 any
```

Delete MAC access list #2001.

```
SWX3220(config)#no access-list 2001
```

9.1.8 Adding a description for MAC access lists

[Syntax]

access-list *mac-acl-id* **description** *line*
no access-list *mac-acl-id* **description**

[Parameter]

mac-acl-id : <2001-3000>

ID of the MAC access list to which to add a description

line : Description to add. Can be up to 32 ASCII characters

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Add a description to the generated MAC access list.

If this command is executed with the "no" syntax, the MAC description is cleared.

[Note]

A description can be added with this command even after applying an access list to LAN/SFP port and logical interface. (The later description will overwrite it)

[Example]

Create MAC access list #2001 that denies frames from MAC address 00-A0-DE-12-34-56, and add the description of "Test".

```
SWX3220(config)#access-list 2001 deny 00A0.DE12.3456 0000.0000.0000 any
SWX3220(config)#access-list 2001 description Test
```

9.1.9 Apply MAC access list

[Syntax]

access-group *mac-acl-id direction*
no access-group *mac-acl-id direction*

[Parameter]

mac-acl-id : <2001-3000>

ID of MAC access list to apply

direction : Specifies the direction of applicable frames

Setting value	Description
in	Apply to received frames

[Initial value]

none

[Input mode]

interface mode

[Description]

Applies a MAC access list to both LAN/SFP port and logical interface.

If the received frame matches the conditions in the access list, the action in the access list will be the action (permit, deny) for the corresponding frame.

If this is executed with the "no" syntax, the applied access list is deleted from both LAN/SFP port and logical interface.

[Note]

It is not possible to register multiple access lists for a single interface.

The following restrictions apply.

An LAN/SFP port for which an incoming frames access list is specified cannot be associated to an logical interface.

An incoming frames access list cannot be applied to an LAN/SFP port that is associated with an logical interface. However, if an access list setting for incoming frames is specified for an LAN/SFP port that is associated with an logical interface in the startup config, then the setting for the lowest-numbered port is applied to the logical interface.

[Example]

Apply access list #2001 to received frames of LAN port #1.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#access-group 2001 in
```

9.1.10 Show generated access list

[Syntax]

show access-list [*acl_id*]

[Parameter]

acl-id	:	<1-2000>, <2001-3000>, <3001-4000> ID of access list

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the registered access list.

If acl-id is omitted, all access lists are shown.

If an access list is applied to an interface, and one or more frames that match the conditions are received or forwarded, the total number (match) of those frames is also shown.

[Note]

The total number (match) of frames that match the traffic category (QoS) conditions is also incremented.

The statistical number (match) of frames that conforms to the conditions of the route map (PBR) is not counted up.

[Example]

Show a list.

```
SWX3220>show access-list
IPv4 access list 1
    10 deny any 192.168.1.0/24 host 172.16.1.1 [match= 62]
MAC access list 2001
    10 deny host 00A0.DE12.3456 any [match= 123]
IPv6 access list 3002
    10 deny 3ffe:506::/32
```

9.1.11 Clear counters

[Syntax]

clear access-list counters [*acl_id*]

[Parameter]

acl-id	:	<1-2000>, <2001-3000>, <3001-4000> ID of access list

[Input mode]

privileged EXEC mode

[Description]

Clears the counters (match) that are shown by the "show access-list" command.

[Example]

Clear counters.

```
SWX3220>clear access-list counters
```

9.1.12 Show access list applied to interface

[Syntax]

show access-group

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

For each interface, shows the ID of all access lists that are applied.

[Example]

Show a list.

```
SWX3220>show access-group
Interface port1.1 : IPv4 access group 1 in
Interface port1.7 : IPv6 access group 3002 in
Interface port1.8 : MAC access group 2001 in
```

9.1.13 Set VLAN access map and move to VLAN access map mode

[Syntax]

vlan access-map *access-map-name*
no vlan access-map *access-map-name*

[Parameter]

access-map-name	:	Single-byte alphanumeric characters and single-byte symbols(256 characters or less) Access map name

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Create a VLAN access map with the name specified by *access-map-name*, and then move to VLAN access map mode in order to make VLAN access map settings.

If this command is executed with the "no" syntax, the specified VLAN access map is deleted.

[Note]

To return from VLAN access map mode mode to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

[Example]

Create a VLAN access map named "VAM001", and move to VLAN access map mode.

```
SWX3220(config)#vlan access-map VAM001
SWX3220(config-vlan-access-map)#
```

9.1.14 Set access list for VLAN access map

[Syntax]

match access-list *list-id*
no match access-list *list-id*

[Parameter]

list-id	:	<1-2000>, <2001-3000>, <3001-4000> Access list number specified by the access-list command

[Initial value]

none

[Input mode]

VLAN access map mode

[Description]

Sets the access list that is applied to the corresponding VLAN access map.

If this command is executed with the "no" syntax, the specified access list is deleted from the corresponding VLAN access map.

[Note]

Only one access list can be specified for one VLAN access map.

You can use the **show vlan access-map** command to view the setting.

[Example]

Create a VLAN access map named "VAM001", and specify an access list that denies packets from 192.168.0.1.

```
SWX3220(config)#access-list 2 deny any 192.168.0.1/32 any
SWX3220(config)#vlan access-map VAM001
SWX3220(config-vlan-access-map)#match access-list 2
```

9.1.15 Set VLAN access map filter

[Syntax]

vlan filter *access-map-name vlan-id* [*direction*]
no vlan filter *access-map-name vlan-id* [*direction*]

[Parameter]

access-map-name : Single-byte alphanumeric characters and single-byte symbols(256 characters or less)

Access map name specified by the vlan access-map command

vlan-id : <1-4094>

VLAN ID set to the "enable" status by the vlan command

direction : Specifies the direction of applicable frames. Applied to incoming frames when omitted

Setting value	Description
in	Apply to received frames
out	Apply to transmitted frames

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Sets the VLAN access map filter for the specified VLAN.

If this command is executed with the "no" syntax, the VLAN access map filter for the specified VLAN is deleted.

[Note]

It is not possible to specify this command for a VLAN ID that is set to the "disable" state.

Only one VLAN access map for each direction can be registered for incoming frames (in) and for outgoing frames (out) on the same interface.

VLAN access maps for which the MAC access list is set cannot be applied to outgoing frames (out).

Only one IPv4 access list for which the port number range (range X Y) is specified can be applied for the entire system, and it cannot be applied to outgoing frames (out).

[Example]

Creates a VLAN access map named VAM001, specifies an access list that denies packets beginning from 192.168.0.1, and then applies VAM001 to incoming frames of VLAN #1000.

```
SWX3220(config)#vlan database
SWX3220(config-vlan)#vlan 1000
SWX3220(config-vlan)#exit
SWX3220(config)#access-list 2 deny any 192.168.0.1/32 any
SWX3220(config)#vlan access-map VAM001
SWX3220(config-vlan-access-map)#match access-list 2
SWX3220(config-vlan-access-map)#exit
SWX3220(config)#vlan filter VAM001 1000 in
```

9.1.16 Show VLAN access map

[Syntax]

show vlan access-map

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the registered VLAN access map.

The following items are shown.

- Name of the VLAN access map
- Access list applied to VLAN access map

[Example]

Show VLAN access map information.

```
SWX3220>show vlan access-map
Vlan access-map VAM001
    match ipv4 access-list 2
```

9.1.17 Show VLAN access map filter

[Syntax]

show vlan filter

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Show VLAN access map filter application information.

The following items are shown.

- Name of the VLAN access map
- VLAN ID applied to VLAN access map
- Frame direction (in/out) for which a VLAN access map is applied

[Example]

Show VLAN access map filter information.

```
SWX3220>show vlan filter
Vlan Filter VAM001 is applied to vlan 1000 in
Vlan Filter VAM001 is applied to vlan 1001 out
Vlan Filter VAM002 is applied to vlan 2000-2001 in
```

9.2 QoS (Quality of Service)

9.2.1 Enable/disable QoS

[Syntax]

qos *action*
qos_disable

[Parameter]

action : Operation for Qos

Setting value	Description
enable	Qos is enabled
disable	Qos is disabled

[Initial value]

no qos

[Input mode]

global configuration mode

[Description]

Enables QoS.

If this is executed with the "no" syntax, QoS is disabled. At this time, the related QoS settings are also deleted.

[Note]

If the flow control system setting is enabled, it is not possible to enable QoS.

Many of the commands related to QoS cannot be executed unless QoS is left enabled.

[Example]

Enable QoS.

```
SWX3220(config)#qos enable
```

Disable QoS.

```
SWX3220(config)#qos disable
```

9.2.2 Set default CoS

[Syntax]

qos cos *value*
no qos cos

[Parameter]

value	:	<0-7>
		Default CoS value

[Initial value]

qos cos 0

[Input mode]

interface mode

[Description]

Sets the default CoS of LAN/SFP port and logical interface.

If this is executed with the "no" syntax, the default value (CoS=0) is specified.

The default CoS is used if untagged frames are received when the interface's trust mode is set to CoS. (Since CoS is not specified for the frame)

[Note]

In order to execute this command, QoS must be enabled.

If this is executed for an interface whose trust mode is CoS, the command results in an execution error.

An LAN/SFP port whose default CoS differs cannot be aggregated as an logical interface.

If the interface for which this is executed is an LAN/SFP port that is associated with an logical interface, then this command produces an execution error. However, in the case of settings for an LAN/SFP port that is associated with an logical interface in the startup config, the setting for the lowest-numbered port is applied to the logical interface.

[Example]

Set the default CoS value to 2.

```
SWX3220(config-if)#qos cos 2
```

Return the default CoS value to the default value.

```
SWX3220(config-if)#no qos cos
```

9.2.3 Set trust mode

[Syntax]

qos trust *mode*
no qos trust

[Parameter]

mode : Trust mode

Setting value	Description
cos	Determines the egress queue based on the CoS value
dscp	Determines the egress queue based on the DSCP value
port-priority	Applies the specified priority to the receiving port

[Initial value]

qos trust cos

[Input mode]

interface mode

[Description]

Specifies the trust mode of LAN/SFP port and logical interface.

If this is executed with the "no" syntax, the default value (CoS trust mode) is specified.

In the case of "CoS" trust mode, the CoS value of incoming frames is used to determine the egress queue. In the case of "DSCP," the DSCP value of incoming frames is used to determine the egress queue. In the case of "port priority," the priority specified for the receiving interface is used to determine the egress queue.

The CoS value and DSCP value, and the egress queue that is associated with the receiving port, can be changed by using the following commands.

Trust mode	Setting value used for egress queue determination	Corresponding command
CoS	CoS - egress queue ID conversion table	**qos cos-queue**
DSCP	DSCP - egress queue ID conversion table	**qos dscp-queue**
Port Priority	Priority specified for each receiving port	**qos port-priority-queue**

Within the various QoS processes, there are four types of timing that determine (change) the egress queue.

1. When assigning the egress queue
2. Specifying the egress queue by class map
3. Specifying pre-marking by class map
4. Specifying remarking by class map

Types 2, 3, and 4 can be specified whether the trust mode is "CoS" or "DSCP"; in either case, the egress queue is assigned by referencing the "egress queue ID conversion table" that corresponds to its own trust mode.

[Note]

In order to execute this command, QoS must be enabled.

If a policy map is applied to LAN/SFP port and logical interface, the trust mode cannot be changed.

An LAN/SFP port whose trust mode differs cannot be aggregated as an logical interface.

The trust mode cannot be changed for an LAN/SFP port that is associated with an logical interface. However, in the case of settings for an LAN/SFP port that is associated with an logical interface in the startup config, the setting for the lowest-numbered port is applied to the logical interface.

Some QoS functions have limitations on execution depending on the trust mode, or may show different results.

[Example]

Set the trust mode of LAN/SFP port and logical interface to DSCP.

```
SWX3220(config-if)#qos trust dscp
```

Set the trust mode of LAN/SFP port and logical interface to the default setting (CoS).

```
SWX3220(config-if)#no qos trust
```

9.2.4 Show status of QoS function setting

[Syntax]

show qos

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the enabled (Enable) or disabled (Disable) status of the QoS function.

[Example]

Show the status of the system's QoS setting.

```
SWX3220#show qos
  Enable
```

9.2.5 Show QoS information for interface

[Syntax]

show qos interface [*ifname*]

[Parameter]

ifname : Name of the LAN/SFP port or logical interface. If this is omitted, the command applies to all ports.

Interface to show

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows QoS settings for the specified interface. The following content is shown.

Item	Description
Port Trust Mode	Trust mode of interface (CoS/DSCP/Port-Priority)
Input Policy-Map Name	Name of policy map already applied to the interface class map information (note 1)
Port Default CoS Priority	Default CoS value (note 2)
Port-Priority-Queue	Port priority order (note 3)
Egress Traffic Shaping	Traffic shaping (individual port)
Egress Traffic Queue Shaping	Traffic shaping (individual queue)
Queue Scheduling	Egress queue scheduling format and weight
CoS (Queue)	CoS - egress queue ID conversion table (note 2)
DSCP (Queue)	DSCP - egress queue ID conversion table (note 4)
Special Queue Assignment: Sent From CPU	Specify the egress queue of the frames transmitted from the CPU

Note 1) Not shown if no policy map is applied. For details on class map information, refer to the **show class-map** command.

Note 2) Shown only for CoS trust mode.

Note 3) Shown only if the trust mode is "port priority."

Note 4) Shown only for DSCP trust mode.

[Note]

In order to execute this command, QoS must be enabled.

[Example]

Show the QoS settings of LAN port #1. (trust mode CoS)

```
SWX3220#show qos interface port1.1

  Port Trust Mode: CoS
```

```
  Port Default CoS Priority: 0

  Egress Traffic Shaping: Rate 30016 Kbps, Burst 1876 KByte

  Queue Scheduling:
  Queue0 : Weight  1 ( 5.3%)
  Queue1 : Weight  1 ( 5.3%)
  Queue2 : Weight  2 (10.5%)
  Queue3 : Weight  5 (26.3%)
  Queue4 : Weight  5 (26.3%)
  Queue5 : Weight  5 (26.3%)
  Queue6 : SP
  Queue7 : SP

  Cos (Queue): 0(2), 1(0), 2(1), 3(3), 4(4), 5(5), 6(6), 7(7)

  Special Queue Assignment:
    Sent From CPU: Queue7
```

Show the QoS settings of LAN port #1. (trust mode DSCP)

```
SWX3220#show qos interface port1.1

  Port Trust Mode: DSCP

  Egress Traffic Shaping: Not Configured

  Queue Scheduling:
  Queue0 : SP
  Queue1 : SP
  Queue2 : SP
  Queue3 : SP
  Queue4 : SP
  Queue5 : SP
  Queue6 : SP
  Queue7 : SP

  DSCP (Queue):  0(2),  1(2),  2(2),  3(2),  4(2),  5(2),  6(2),  7(2)
                 8(0),  9(0), 10(0), 11(0), 12(0), 13(0), 14(0), 15(0)
                16(1), 17(1), 18(1), 19(1), 20(1), 21(1), 22(1), 23(1)
                24(3), 25(3), 26(3), 27(3), 28(3), 29(3), 30(3), 31(3)
                32(4), 33(4), 34(4), 35(4), 36(4), 37(4), 38(4), 39(4)
                40(5), 41(5), 42(5), 43(5), 44(5), 45(5), 46(5), 47(5)
                48(6), 49(6), 50(6), 51(6), 52(6), 53(6), 54(6), 55(6)
                56(7), 57(7), 58(7), 59(7), 60(7), 61(7), 62(7), 63(7)

  Special Queue Assignment:
    Sent From CPU: Queue7
```

9.2.6 Show egress queue usage ratio

[Syntax]

show qos queue-counters [*ifname*]

[Parameter]

ifname	:	Name of the LAN/SFP port. If this is omitted, the command applies to all ports. Interface to show

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the usage ratio for each egress queue of the specified LAN/SFP port. The queue usage ratio is calculated as follows.

(queue usage ratio) = (number of buffers held in the queue) / (maximum length of the queue)

[Note]

This command can be used regardless of the QoS status (enabled/disabled).

[Example]

Show the queue usage ratio of LAN port #1.

```
SWX3220#show qos queue-counters port1.1
QoS: Enable
Interface port1.1 Queue Counters:
  Queue 0         59.4 %
  Queue 1         15.0 %
  Queue 2          0.0 %
  Queue 3          0.0 %
  Queue 4          0.0 %
  Queue 5          3.6 %
  Queue 6          0.0 %
  Queue 7          0.1 %
```

9.2.7 Set CoS - egress queue ID conversion table

[Syntax]

qos cos-queue *cos-value queue-id*
no qos cos-queue *cos-value*

[Parameter]

cos-value : <0-7>

CoS value of conversion source

queue-id : <0-7>

Egress queue ID corresponding to CoS value

[Initial value]

See [Note]

[Input mode]

global configuration mode

[Description]

Specifies the values of the CoS - egress queue ID conversion table that is used to determine the egress queue.

If this is executed with the "no" syntax, the egress queue ID for the specified CoS value is returned to the default setting.

The CoS - egress queue ID conversion table is used when the trust mode is set to CoS.

[Note]

In order to execute this command, QoS must be enabled.

The following table shows the default settings of the CoS - egress queue ID conversion table.

CoS value	Egress queue
0	2
1	0
2	1
3	3
4	4
5	5
6	6
7	7

[Example]

Assign egress queue #4 to CoS value "0".

```
SWX3220(config)#qos cos-queue 0 4
```

Return the egress queue ID of CoS value "0" to the default value.

```
SWX3220(config)#no qos cos-queue 0
```

9.2.8 Set DSCP - egress queue ID conversion tabl

[Syntax]

qos dscp-queue *dscp-value queue-id*
no qos dscp-queue *dscp-value*

[Parameter]

dscp-value : <0-63>

DSCP value of the conversion source

queue-id : <0-7>

Egress queue ID corresponding to DSCP value

[Initial value]

See [Note]

[Input mode]

global configuration mode

[Description]

Specifies the values of the DSCP - egress queue ID conversion table that is used to determine the egress queue.
If this is executed with the "no" syntax, the egress queue ID for the specified DSCP value is returned to the default setting.
The DSCP - egress queue ID conversion table is used when the trust mode is set to DSCP.

[Note]

In order to execute this command, QoS must be enabled.
The following table shows the default settings of the DSCP - egress queue ID conversion table.

DSCP value	Egress queue
0-7	2
8-15	0
16-23	1
24-31	3
32-39	4
40-47	5
48-55	6
56-63	7

[Example]

Assign egress queue #4 to DSCP value "0."

```
SWX3220(config)#qos dscp-queue 0 4
```

Return the egress queue ID of DSCP value "23" to the default value.

```
SWX3220(config)#no qos dscp-queue 23
```

9.2.9 Set port priority order

[Syntax]

qos port-priority-queue *queue-id*
no qos port-priority-queue

[Parameter]

queue-id : <0-7>

Egress queue ID assigned to LAN/SFP port

[Initial value]

qos port-priority-queue 2

[Input mode]

interface mode

[Description]

Specifies the priority (egress queue ID) for the receiving interface to LAN/SFP port and logical interface.

If this is executed with the "no" syntax, the egress queue ID for the specified interface is returned to the default setting (2).

The port priority is used to determine the egress queue when the trust mode is set to "port priority."

[Note]

In order to execute this command, QoS must be enabled.

If this is executed for an interface whose trust mode is not "port priority," the command results in an execution error.

An LAN/SFP port whose port priority differs cannot be aggregated as an logical interface.

If the interface for which this is executed is an LAN/SFP port that is associated with an logical interface, then this command produces an execution error. However, in the case of settings for an LAN/SFP port that is associated with an logical interface in the startup config, the setting for the lowest-numbered port is applied to the logical interface.

[Example]

Assign egress queue ID #4 as the port priority for LAN port #1.

```
SWX3220#interface port1.1
SWX3220(config-if)#qos port-priority-queue 4
```

9.2.10 Specify egress queue of frames transmitted from the switch itself

[Syntax]

qos queue sent-from-cpu *queue-id*
no qos queue sent-from-cpu

[Parameter]

queue-id	:	<0-7> Egress queue ID

[Initial value]

qos queue sent-from-cpu 7

[Input mode]

global configuration mode

[Description]

Specifies the egress queue for the storage destination of frames sent to each LAN/SFP port from the switch itself (CPU).

If this is executed with the "no" syntax, the default value is specified.

[Note]

In order to execute this command, QoS must be enabled.

If the priority order of frames sent from the CPU is lowered, transmission from a higher-priority queue takes priority; this means that under conditions of high load, functions such as L2MS or loop detection might stop working. For this reason, we recommend that you set this setting to as high a value (priority) as possible.

When the stack function is enabled, the storage-destination transmission queue ID for frames sent from the CPU is "6" by default.

[Example]

Specify #5 as the storage destination egress queue for frames sent from the CPU.

```
SWX3220(config)#qos queue sent-from-cpu 5
```

9.2.11 Generate class map (traffic category conditions)

[Syntax]

class-map *name*
no class-map *name*

[Parameter]

name	:	Name of class map (maximum 20 characters; uppercase and lowercase are distinguished)

[Input mode]

global configuration mode

[Description]

Generates a class map.

A class map defines the conditions used to classify received frames into traffic classes, and consists of conditions defined by the **match** command and the corresponding action (permit/deny).Class map actions are handled as follows. Class map actions are handled as follows.

- If an access list (ACL) is specified (execute the **match access-group** command)

  The class map action will be the action for the ACL.
- If other than an access list (ACL) is specified

  Permit.

After generating the class map, move to class map mode to specify its content.

If this command is executed with the "no" syntax, the specified class map is deleted.

[Note]

In order to execute this command, QoS must be enabled.

If the specified class map has already been generated, the change is applied to the previous settings. However, if a policy map has been applied to LAN/SFP port and logical interface, then the class map that is associated with the policy map cannot be edited or deleted.

[Example]

Create class map "class1."

```
SWX3220(config)#class-map class1
SWX3220(config-cmap)#
```

9.2.12 Associate class map

[Syntax]

class *name*
no class *name*

[Parameter]

name	:	Class map name

[Input mode]

policy map mode

[Description]

Associates a class map to a policy map.

When the class map association succeeds, move to policy map class mode. In policy map class mode, you can make the following settings for each traffic class.

- Pre-marking or specifying the egress queue
- Metering
- Policing
- Remarking

If this command is executed with the "no" syntax, the association of the class map to the policy map is canceled.

For LAN/SFP port and logical interface to which a policy map is applied, received frames are classified into traffic classes according to the conditions of the associated class map. If the action in the class map is "permit," the QoS processing specified by the user for that traffic class is performed.

Up to eight class maps can be associated to one policy map.

[Note]

In order to execute this command, QoS must be enabled.

It is meaningless to specify QoS processing settings for a traffic class for which the action is "deny."

[Example]

Make the following settings for received frames to LAN port #1.

- Permit traffic from the 10.1.0.0 network
- Categorize bandwidth classes as CIR:48kbps, CBS:12kbyte, and EBS:12kbyte
- Green: forward, Yellow: rewrite DSCP value to 10, Red: discard

[Traffic class definition]

```
SWX3220(config)#access-list 1 permit any 10.1.0.0 0.0.255.255 any
SWX3220(config)#class-map class1
SWX3220(config-cmap)#match access-list 1
SWX3220(config-cmap)#exit
```

[Policy settings]

```
SWX3220(config)#policy-map policy1
SWX3220(config-pmap)#class class1
SWX3220(config-pmap-c)#police 48 12 12 yellow-action remark red-action drop
SWX3220(config-pmap-c)#remark-map yellow ip-dscp 10
SWX3220(config-pmap-c)#exit
SWX3220(config-pmap)#exit
SWX3220(config)#interface port1.1
SWX3220(config-if)#service-policy input policy1
```

9.2.13 Set traffic classification conditions (access-list)

[Syntax]

match access-list *acl-id*
no match access-list *acl-id*

[Parameter]

acl-id : <1 - 2000>

IPv4 access list ID

: <2001 - 3000>

MAC access list ID

: <3001 - 4000>

IPv6 access list ID

[Input mode]

class map mode

[Description]

Uses the access list as the conditions to classify the traffic class.

If the received frame matches the conditions in the access list, the action in the access list will be the action (permit, deny) for the traffic class.

If this is executed with the "no" syntax, the condition settings of the access list are deleted.

[Note]

In order to execute this command, QoS must be enabled.

A maximum of 39 conditions can be specified for traffic categorization in an access list.

[Example]

Specify access list #1 as the classification conditions for class map "class1."

```
SWX3220(config)#class-map class1
SWX3220(config-cmap)#match access-list 1
```

9.2.14 Set traffic classification conditions (CoS)

[Syntax]

match cos *cos-list*
no match cos

[Parameter]

cos-list : <0 - 7>

CoS value used as classification condition. Up to eight can be registered.

[Input mode]

class map mode

[Description]

Uses the CoS value of the VLAN tag header as the condition to classify the traffic class.

If this is executed with the "no" syntax, the CoS condition setting is deleted.

The setting can be repeated up to the maximum number (eight) of registrations.

[Note]

In order to execute this command, QoS must be enabled.

[Example]

Specify CoS values "1" and "2" as the classification conditions for class map "class1."

```
SWX3220(config)#class-map class1
SWX3220(config-cmap)#match cos 1 2
```

9.2.15 Set traffic classification conditions (TOS precedence)

[Syntax]

match ip-precedence *tos-list*
no match ip-precedence

[Parameter]

tos-list : <0 - 7>

Value of the IP header's TOS precedence field used as a classification condition. Up to eight can be registered.

[Input mode]

class map mode

[Description]

Uses the value of the IP header's TOS precedence field as a condition to classify the traffic class.

If this is executed with the "no" syntax, the classification conditions using TOS precedence are deleted.

The setting can be repeated up to the maximum number (eight) of registrations.

[Note]

In order to execute this command, QoS must be enabled.

[Example]

Specify TOS precedence values "3" and "4" as the classification conditions for class map "class1".

```
SWX3220(config)#class-map class1
SWX3220(config-cmap)#match ip-precedence 3 4
```

9.2.16 Set traffic classification conditions (DSCP)

[Syntax]

match ip-dscp *dscp-list*
no match ip-dscp

[Parameter]

dscp-list : <0 - 63>

Value of the IP header's DSCP (DiffServ Code Point) field used as a classification condition. Up to eight can be registered.

[Input mode]

class map mode

[Description]

Uses the value of the IP header's DSCP (DiffServ Code Point) field as a condition to classify the traffic class.

If this is executed with the "no" syntax, the classification conditions using DSCP precedence are deleted.

The setting can be repeated up to the maximum number (eight) of registrations.

[Note]

In order to execute this command, QoS must be enabled.

[Example]

Specify DSCP values "48" and "56" as the classification conditions for class map "class1."

```
SWX3220(config)#class-map class1
SWX3220(config-cmap)#match ip-dscp 48 56
```

9.2.17 Set traffic classification conditions (Ethernet Type)

[Syntax]

match ethertype *type*
match ethertype *type* tagged
match ethertype *type* untagged
no match ethertype

[Keyword]

tagged : Set conditional VLAN tagging

untagged : Set conditional VLAN untagging

[Parameter]

type :

Specifies the type of the Ethernet frame.

Setting value	Description
0xXXXX	Hexadecimal expression of type value
any	All frame

[Input mode]

class map mode

[Description]

Uses the Ethernet frame's type value and the presence of a VLAN tag as the conditions to classify the traffic class.

If this command is executed with the "no" syntax, deletes conditional settings based on the Ethernet frame's type value and the presence of a VLAN tag.

If this setting has already been made by the **match ethertype** command, the content of the setting is changed.

[Note]

In order to execute this command, QoS must be enabled.

If applied to an access port, the "tagged" specification is invalid (because tagged frames are not handled by an access port).

[Example]

Set Ethernet frame type value "0x0800" as the classification condition for class map "class1."

```
SWX3220(config)#class-map class1
SWX3220(config-cmap)#match ethertype 0x0800
```

9.2.18 13.2.22 Set traffic classification conditions (VLAN ID)

[Syntax]

match vlan *id*
no match vlan

[Parameter]

id : <1 - 4094>

VLAN ID used as classification condition

[Input mode]

class map mode

[Description]

Uses the VLAN ID as the condition to classify the traffic class.

If this is executed with the "no" syntax, the classification conditions using VLAN ID are deleted.

The setting can be repeated up to the maximum number (30) of registrations.

[Note]

In order to execute this command, QoS must be enabled.

[Example]

Specify VLAN #20 as the classification conditions for class map "class1".

```
SWX3220(config)#class-map class1
SWX3220(config-cmap)#match vlan 20
```

9.2.19 Set traffic classification conditions (VLAN ID range)

[Syntax]

match vlan-range *id-start* **to** *id-end*

[Parameter]

id-start	:	<1 - 4094> Starting VLAN ID value used as classification condition.
id-end	:	<1 - 4094> Ending VLAN ID value used as classification condition. The range from the specified starting value to the ending value can be a maximum of 30.

[Input mode]

class map mode

[Description]

Uses the VLAN ID as the condition to classify the traffic class.

To delete the classification condition, use the **no match vlan** command.

This can be used in conjunction with the setting of the **match vlan** command.

The **match vlan** command or **match vlan-range** command settings can be repeated up to the maximum number that can be registered (30).

[Note]

In order to execute this command, QoS must be enabled.

[Example]

Specify VLAN #20 through #30 as the classification conditions for class map "class1".

```
SWX3220(config)#class-map class1
SWX3220(config-cmap)#match vlan-range 20 to 30
```

9.2.20 Show class map information

[Syntax]

show class-map [*name*]

[Parameter]

name	:	Class map name. If this is omitted, all class map information is shown.

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows information for the specified class map. The following information is shown for each class map.

Section	Item	Description
Classification conditions (match)	Match Access-List	Access list ID
	Match ethertype	Ethernet Type
	Match vlan	VLAN ID
	Match vlan-range	
	Match CoS	CoS value
	Match IP precedence	TOS precedence
	Match IP DSCP	DSCP value

- The classification condition is shown only once for each type that is specified.
- A classification condition for which a corresponding command (match) is not set will not be shown.

[Note]

In order to execute this command, QoS must be enabled.

[Example]

Show information for class map "class1".

```
SWX3220#show class-map class1

    Class-Map Name: class1
      Match vlan 10
```

9.2.21 Generate policy map for received frames

[Syntax]

policy-map *name*
no policy-map *name*

[Parameter]

name : Name of policy map (maximum 32 characters; uppercase and lowercase are distinguished)

[Input mode]

global configuration mode

[Description]

Generates a policy map. The policy map combines the following processing for received frames, for each traffic class.

- Traffic classification
- Pre-marking
- Metering
- Policing
- Remarking

The policy map generated by this command can be applied to LAN/SFP port and logical interface by the **service-policy input** command. This classifies received frames into traffic classes according to each class map in the policy map, and applies the QoS process specified by the user to each class of traffic.

After generating the policy map, move to policy map mode to specify its content.

If this is executed with the "no" syntax, the specified policy map is deleted.

[Note]

In order to execute this command, QoS must be enabled.

If the specified policy map has already been generated, the change is applied to the previous settings. However, if the policy map is already applied to LAN/SFP port and logical interface, it cannot be edited or deleted.

[Example]

Make the following settings for received frames to LAN port #1.

- Permit traffic from the 10.1.0.0 network
- Categorize bandwidth classes as CIR:48kbps, CBS:12kbyte, and EBS:12kbyte
- Green: forward, Yellow: rewrite DSCP value to 10, Red: discard

[Traffic class definition]

```
SWX3220(config)#access-list 1 permit any 10.1.0.0 0.0.255.255 any
SWX3220(config)#class-map class1
SWX3220(config-cmap)#match access-list 1
SWX3220(config-cmap)#exit
```

[Policy settings]

```
SWX3220(config)#policy-map policy1
SWX3220(config-pmap)#class class1
SWX3220(config-pmap-c)#police 48 12 12 yellow-action remark red-action drop
SWX3220(config-pmap-c)#remark-map yellow ip-dscp 10
SWX3220(config-pmap-c)#exit
SWX3220(config-pmap)#exit
SWX3220(config)#interface port1.1
SWX3220(config-if)#service-policy input policy1
```

9.2.22 Apply policy map for received frames

[Syntax]

service-policy input *name*
no service-policy *name*

[Parameter]

name : Name of policy map to apply

[Input mode]

interface mode

[Description]

Applies the policy map to the corresponding LAN/SFP port and logical interface.

If this is executed with the "no" syntax, the policy map is deleted from the LAN/SFP port and logical interface.

[Note]

In order to execute this command, QoS must be enabled.

If a policy map has already been applied to the LAN/SFP port and logical interface, an error occurs.

For a class map that is associated with a policy map, an error occurs if there is not even one setting that corresponds to the trust mode of the LAN/SFP port and logical interface. Of the class map settings, the following commands are limited in their applicability by the trust mode.

Trust mode	Command	Restrictions
CoS	**set ip-dscp-queue**	Cannot be used
DSCP	**set cos-queue**	Cannot be used
Port Priority	**set cos**	Cannot be used
	set ip-precedence	
	set ip-dscp	
	set cos-queue	
	set ip-dscp-queue	
	police, remark-map	Cannot use a combination for which remarking is enabled (*1)

*1) A combination for which remarking is enabled refers to when the yellow-action or red-action of the **police** command is set to "remark" and the **remark-map** of the corresponding color is specified.

An LAN/SFP port to which a policy map is applied cannot be associated with an logical interface.

A policy map cannot be applied to an LAN/SFP port that is associated with an logical interface. However, in the case of settings for an LAN/SFP port that is associated with an logical interface in the startup config, the setting for the lowest-numbered port is applied to the logical interface.

Metering cannot be performed on the following logical interfaces. A policy map that includes metering (policer) settings (police-type commands) must not be applied.

- On the SWX3200-52GT, logical interfaces that group ports 1 - 24, 49, 50 with ports 25 - 48, 51, 52
- Logical interfaces that are grouped across member switches constituting a stack

[Example]

Apply policy map "policy1" to LAN port #1.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#service-policy input policy1
```

Remove policy map "policy1" from LAN port #1.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#no service-policy input policy1
```

9.2.23 Set pre-marking (CoS)

[Syntax]

set cos *value*
no set cos

[Parameter]

value : <0 - 7>

CoS value set by pre-marking

[Input mode]

policy map class mode

[Description]

Changes the CoS value of the classified traffic class to the specified CoS value. In addition, reassign the egress queue according to the egress queue ID table that corresponds to the trust mode.

If this is executed with the "no" syntax, pre-marking processing of the CoS value corresponding to the traffic class is removed.

[Note]

In order to execute this command, QoS must be enabled.

Pre-marking cannot be used in conjunction with the set egress queue function.

[Example]

Make the following settings for received frames of LAN port #1

- Permit traffic from the 10.1.0.0 network
- Change the classified traffic class to the CoS value "2"

[Traffic class definition]

```
SWX3220(config)#access-list 1 permit any 10.1.0.0 0.0.255.255 any
SWX3220(config)#class-map class1
SWX3220(config-cmap)#match access-list 1
SWX3220(config-cmap)#exit
```

[Policy settings]

```
SWX3220(config)#policy-map policy1
SWX3220(config-pmap)#class class1
SWX3220(config-pmap-c)#set cos 2
SWX3220(config-pmap-c)#exit
SWX3220(config-pmap)#exit
SWX3220(config)#interface port1.1
SWX3220(config-if)#service-policy input policy1
```

9.2.24 Set pre-marking (TOS precedence)

[Syntax]

set ip-precedence *value*
no set ip-precedence

[Parameter]

value : <0 - 7>

TOS precedence to specify by pre-marking

[Input mode]

policy map class mode

[Description]

Changes the value of the IP header's TOS precedence field of the classified traffic class to the specified TOS value. In addition, reassign the egress queue according to the egress queue ID table that corresponds to the trust mode.

If this is executed with the "no" syntax, pre-marking processing of the TOS precedence corresponding to the traffic class is removed.

[Note]

In order to execute this command, QoS must be enabled.

Pre-marking cannot be used in conjunction with the set egress queue function.

[Example]

Make the following settings for received frames of LAN port #1

- Permit traffic from the 10.1.0.0 network
- Change the classified traffic class to TOS precedence "5".

[Traffic class definition]

```
SWX3220(config)#access-list 1 permit any 10.1.0.0 0.0.255.255 any
SWX3220(config)#class-map class1
SWX3220(config-cmap)#match access-list 1
SWX3220(config-cmap)#exit
```

[Policy settings]

```
SWX3220(config)#policy-map policy1
SWX3220(config-pmap)#class class1
SWX3220(config-pmap-c)#set ip-precedence 5
SWX3220(config-pmap-c)#exit
SWX3220(config-pmap)#exit
SWX3220(config)#interface port1.1
SWX3220(config-if)#service-policy input policy1
```

9.2.25 Set pre-marking (DSCP)

[Syntax]

set ip-dscp *value*
no set dscp

[Parameter]

value : <0 - 63>

DSCP value specified by pre-marking

[Input mode]

policy map class mode

[Description]

Changes the DSCP value of the classified traffic class to the specified DSCP value. In addition, reassign the egress queue according to the egress queue ID table that corresponds to the trust mode.

If this is executed with the "no" syntax, pre-marking processing of the DSCP value corresponding to the traffic class is removed.

[Note]

In order to execute this command, QoS must be enabled.

Pre-marking cannot be used in conjunction with the set egress queue function.

Up to four values may be used for pre-marking/remarking to a DSCP value not recommended in the RFC. The following table shows the DSCP values that are recommended in the RFC.

PHB	DSCP value	RFC
default	0	2474
Class Selector	0, 8, 16, 24, 32, 40, 48, 56	2474
Assured Forwarding	10, 12, 14, 18, 20, 22, 26, 28, 30, 34, 36, 38	2597
Expedited Forwarding(EF)	46	2598

[Example]

Make the following settings for received frames of LAN port #1

- Permit traffic from the 10.1.0.0 network
- Change the classified traffic class to the DSCP value "10."

[Traffic class definition]

```
SWX3220(config)#access-list 1 permit any 10.1.0.0 0.0.255.255 any
SWX3220(config)#class-map class1
SWX3220(config-cmap)#match access-list 1
SWX3220(config-cmap)#exit
```

[Policy settings]

```
SWX3220(config)#policy-map policy1
SWX3220(config-pmap)#class class1
SWX3220(config-pmap-c)#set ip-dscp 10
SWX3220(config-pmap-c)#exit
SWX3220(config-pmap)#exit
SWX3220(config)#interface port1.1
SWX3220(config-if)#service-policy input policy1
```

9.2.26 Set individual policers (single rate)

[Syntax]

police [single-rate] *CIR CBS EBS* **yellow-action** *action* **red-action** *action*
no police

[Keyword]

single-rate	:	Use single-rate policer

[Parameter]

CIR	:	<1 - 102300000> Traffic rate (kbps)
CBS	:	<11 - 2097120> Burst size of conformant token bucket (kbyte)
EBS	:	<11 - 2097120> Burst size of excess token bucket (kbyte)
action	:	Operation for packets categorized by bandwidth class

Setting value	Operation
transmit	Forward
drop	Discard
remark	Remarking (CoS/TOS/DSCP)

[Input mode]

policy map class mode

[Description]

Specifies individual policers (single rate) for the categorized traffic classes.

If the setting was already made by the **police** command, its content is changed.

Metering on the SWX3220 is implemented as a single-rate three-color marker (RFC2697), and the following processing can be specified for the categorized bandwidth classes.

- Green : Only forward (cannot be specified)
- Yellow : Choose forward, discard, or remark
- Red : Choose discard or remark

  However, remarking can be specified for either Yellow or Red, not both.

Detailed remarking settings are made using the **remark-map** command (policy map class mode). Regardless of whether *action* is set to "remark," remarking is disabled if there are no detailed remarking settings for that bandwidth class. In this case, the default settings (Yellow: forward, Red: discard) are applied.

If this is executed with the "no" syntax, metering/policing/remarking processing is deleted.

This cannot be used in conjunction with the aggregate policer (**police-aggregate** command).

[Note]

In order to execute this command, QoS must be enabled.

Metering cannot be performed on the following logical interfaces. A policy map that includes metering (policer) settings (police-type commands) must not be applied.

- On the SWX3200-52GT, logical interfaces that group ports 1 - 24, 49, 50 with ports 25 - 48, 51, 52
- Logical interfaces that are grouped across member switches constituting a stack

[Example]

Make the following settings for received frames of LAN port #1

- Permit traffic from the 10.1.0.0 network
- Categorize bandwidth classes as CIR:48kbps, CBS:12kbyte, and EBS:12kbyte
- Green: forward, Yellow: rewrite DSCP value to 10, Red: discard

[Traffic class definition]

```
SWX3220(config)#access-list 1 permit any 10.1.0.0 0.0.255.255 any
SWX3220(config)#class-map class1
SWX3220(config-cmap)#match access-list 1
SWX3220(config-cmap)#exit
```

[Policy settings]

```
SWX3220(config)#policy-map policy1
SWX3220(config-pmap)#class class1
SWX3220(config-pmap-c)#police 48 12 12 yellow-action remark red-action drop
SWX3220(config-pmap-c)#remark-map yellow ip-dscp 10
SWX3220(config-pmap-c)#exit
SWX3220(config-pmap)#exit
SWX3220(config)#interface port1.1
SWX3220(config-if)#service-policy input policy1
```

9.2.27 Set individual policers (twin rate)

[Syntax]

police twin-rate *CIR PIR CBS PBS* **yellow-action** *action* **red-action** *action*
no police

[Keyword]

twin-rate : Use twin rate policers

[Parameter]

CIR : <1 - 102300000>

Traffic rate (kbps)

PIR : <1 - 102300000>

Peak traffic rate (kbps). A value less than CIR cannot be specified.

CBS : <11 - 2097120>

Burst size of conformant token bucket (kbyte)

PBS : <11 - 2097120>

Burst size of peak token bucket (kbyte)

action : Operation for packets categorized by bandwidth class

Setting value	Operation
transmit	Forward
drop	Discard
remark	Remarking (CoS/TOS/DSCP)

[Input mode]

policy map class mode

[Description]

Specifies individual policers (twin rate) for the categorized traffic classes.

If the setting was already made by the **police** command, its content is changed.

Metering on the SWX3220 is implemented as a single-rate three-color marker (RFC2697), and the following processing can be specified for the categorized bandwidth classes.

- Green : Only forward (cannot be specified)
- Yellow : Choose forward, discard, or remark
- Red : Choose discard or remark

  However, remarking can be specified for either Yellow or Red, not both.

Detailed remarking settings are made using the **remark-map** command (policy map class mode). Regardless of whether *action* is set to "remark," remarking is disabled if there are no detailed remarking settings for that bandwidth class. In this case, the default settings (Yellow: forward, Red: discard) are applied.

If this is executed with the "no" syntax, metering/policing/remarking processing is deleted.

This cannot be used in conjunction with the aggregate policer (**police-aggregate** command).

[Note]

In order to execute this command, QoS must be enabled.

Metering cannot be performed on the following logical interfaces. A policy map that includes metering (policer) settings (police-type commands) must not be applied.

- On the SWX3200-52GT, logical interfaces that group ports 1 - 24, 49, 50 with ports 25 - 48, 51, 52
- Logical interfaces that are grouped across member switches constituting a stack

[Example]

Make the following settings for received frames of LAN port #1

- Permit traffic from the 10.1.0.0 network
- Categorize bandwidth classes as CIR:48kbps, PIR:96kbps, CBS:12kbyte, and PBS:12kbyte
- Green: forward, Yellow: rewrite DSCP value to 10, Red: discard

[Traffic class definition]

```
SWX3220(config)#ip-access-list 1 permit 10.1.0.0 0.0.255.255
SWX3220(config)#class-map class1
SWX3220(config-cmap)#match access-group 1
SWX3220(config-cmap)#exit
```

[Policy settings]

```
SWX3220(config)#policy-map policy1
SWX3220(config-pmap)#class class1
SWX3220(config-pmap-c)#police twin-rate 48 96 12 12 yellow-action remark red-action
drop
SWX3220(config-pmap-c)#remark-map yellow ip-dscp 10
SWX3220(config-pmap-c)#exit
SWX3220(config-pmap)#exit
SWX3220(config)#interface port1.1
SWX3220(config-if)#service-policy input policy1
```

9.2.28 Set remarking of individual policers

[Syntax]

remark-map *color type value*
no remark-map

[Parameter]

color : Bandwidth class to remark

Setting value	Description
yellow	Make remarking settings for bandwidth class Yellow
red	Make remarking settings for bandwidth class Red

type : Type of remarking

Setting value	Description
cos	CoS remarking
ip-precedence	TOS precedence remarking
ip-dscp	DSCP remarking

value : <0 - 7>

CoS or TOS precedence remarking value

: <0 - 63>

DSCP remarking value

[Input mode]

policy map class mode

[Description]

Specifies remarking operations for bandwidth classes Yellow and Red that were classified by individual policers. In addition, reassign the egress queue according to the egress queue ID table that corresponds to the trust mode.

For remarking, you can select either CoS value, TOS precedence, or DSCP value.

If this is executed with the "no" syntax, the remarking setting is deleted.

In order to perform remarking, you must specify this command and additionally use the **police** command (policy map class mode)) to specify "remark" as the action for the corresponding bandwidth class.

[Note]

In order to execute this command, QoS must be enabled.

Remarking can be used in conjunction with pre-marking and specifying the egress queue.

Up to four user-defined values may be used for pre-marking/remarking to a DSCP value not recommended in the RFC. The following table shows the DSCP values that are recommended in the RFC.

PHB	DSCP value	RFC
default	0	2474
Class Selector	0, 8, 16, 24, 32, 40, 48, 56	2474
Assured Forwarding	10, 12, 14, 18, 20, 22, 26, 28, 30, 34, 36, 38	2597
Expedited Forwarding(EF)	46	2598

[Example]

Make the following settings for received frames of LAN port #1@

- Permit traffic from the 10.1.0.0 network
- Categorize bandwidth classes as CIR:48kbps, CBS:12kbyte, and EBS:12kbyte
- Green: forward, Yellow: rewrite DSCP value to 10, Red: discard

[Traffic class definition]

```
SWX3220(config)#access-list 1 permit any 10.1.0.0 0.0.255.255 any
SWX3220(config)#class-map class1
SWX3220(config-cmap)#match access-list 1
SWX3220(config-cmap)#exit
```

[Policy settings]

```
SWX3220(config)#policy-map policy1
SWX3220(config-pmap)#class class1
SWX3220(config-pmap-c)#police 48 12 12 yellow-action remark red-action drop
SWX3220(config-pmap-c)#remark-map yellow ip-dscp 10
SWX3220(config-pmap-c)#exit
SWX3220(config-pmap)#exit
SWX3220(config)#interface port1.1
SWX3220(config-if)#service-policy input policy1
```

9.2.29 Generate aggregate policer

[Syntax]

aggregate-police *name*
no aggregate-police *name*

[Parameter]

name	:	Name of aggregate policer (maximum 20 characters; uppercase and lowercase are distinguished)

[Input mode]

global configuration mode

[Description]

Generates an aggregate policer. If the policer has already been generated, this command edits its content.

When the command succeeds, you transition to aggregate policer mode, where you can edit the content of the aggregate policer.

If this command is executed with the "no" syntax, the aggregate policer is deleted.

In the following case, the content of the aggregate policer cannot be changed (you will not transition to aggregate policer mode).

- A policy map that includes a class map specified by the aggregate policer is applied to LAN/SFP port and logical interface.

In the following case, the aggregate policer cannot be deleted.

- The **police-aggregate** command was used to set the aggregate policer to a traffic class

[Note]

In order to execute this command, QoS must be enabled.

Metering cannot be performed on the following logical interfaces. A policy map that includes metering (policer) settings (police-type commands) must not be applied.

- On the SWX3200-52GT, logical interfaces that group ports 1 - 24, 49, 50 with ports 25 - 48, 51, 52
- Logical interfaces that are grouped across member switches constituting a stack

[Example]

Generate aggregate policer "AGP-01".

```
SWX3220(config)#aggregate-police AGP-01
SWX3220(config-agg-policer)#
```

9.2.30 Set aggregate policer (single rate)

[Syntax]

police [single-rate] *CIR CBS EBS* **yellow-action** *action* **red-action** *action*
no police

[Keyword]

single-rate	:	Use single-rate policer

[Parameter]

CIR	:	<1 - 102300000> Traffic rate (kbps)
CBS	:	<11 - 2097120> Burst size of conformant token bucket (kbyte)
EBS	:	<11 - 2097120> Burst size of excess token bucket (kbyte)
action	:	Operation for packets categorized by bandwidth class

Setting value	Operation
transmit	Forward
drop	Discard
remark	Remarking (CoS/TOS/DSCP)

[Input mode]

aggregate policer mode

[Description]

Specifies a single rate policer as an aggregate policer.

If this is executed with the "no" syntax, metering/policing/remarking processing is deleted.

Metering on the SWX3220 is implemented as a single-rate three-color marker (RFC2697), and the following processing can be specified for the categorized bandwidth classes.

- Green : Only forward (cannot be specified)
- Yellow : Choose forward, discard, or remark
- Red : : Choose discard or remark

  However, remarking can be specified for either Yellow or Red, not both.

Detailed remarking settings are made using the **remark-map** command (aggregate policer mode). Regardless of whether *action* is set to "remark," remarking is disabled if there are no detailed remarking settings for that bandwidth class. In this case, the default settings (Yellow: forward, Red: discard) are applied.

[Note]

In order to execute this command, QoS must be enabled.

Metering cannot be performed on the following logical interfaces. A policy map that includes metering (policer) settings (police-type commands) must not be applied.

- On the SWX3200-52GT, logical interfaces that group ports 1 - 24, 49, 50 with ports 25 - 48, 51, 52
- Logical interfaces that are grouped across member switches constituting a stack

[Example]

Create an aggregate policer "AGP-01".

- Executing metering by SrTCM with CIR:48kbps, CBS:12kbyte, and EBS:12kbyte
- Yellow: rewrite DSCP value to 10, Red: discard

[Aggregate policer creating]

```
SWX3220(config)#aggregate-police AGP-01
SWX3220(config-agg-policer)#police single-rate 48 12 12 yellow-action remark red-
action drop
SWX3220(config-agg-policer)#remark-map yellow ip-dscp 10
SWX3220(config-agg-policer)#exit
```

9.2.31 Set aggregate policer (twin rate)

[Syntax]

police twin-rate *CIR PIR CBS PBS* **yellow-action** *action* **red-action** *action*
no police

[Keyword]

twin-rate : Use twin rate policers

[Parameter]

CIR : <1 - 102300000>

Traffic rate (kbps)

PIR : <1 - 102300000>

Peak traffic rate (kbps). A value less than CIR cannot be specified.

CBS : <11 - 2097120>

Burst size of conformant token bucket (kbyte)

PBS : <11 - 2097120>

Burst size of peak token bucket (kbyte)

action : Operation for packets categorized by bandwidth class

Setting value	Operation
transmit	Forward
drop	Discard
remark	Remarking (CoS/TOS/DSCP)

[Input mode]

aggregate policer mode

[Description]

Specifies a twin rate policer as an aggregate policer.

If this is executed with the "no" syntax, metering/policing/remarking processing is deleted.

Metering on the SWX3220 is implemented as a single-rate three-color marker (RFC2697), and the following processing can be specified for the categorized bandwidth classes.

- Green : Only forward (cannot be specified)
- Yellow : Choose forward, discard, or remark
- Red : Choose discard or remark

  However, remarking can be specified for either Yellow or Red, not both.

Detailed remarking settings are made using the **remark-map** command (aggregate policer mode). Regardless of whether *action* is set to "remark," remarking is disabled if there are no detailed remarking settings for that bandwidth class. In this case, the default settings (Yellow: forward, Red: discard) are applied.

[Note]

In order to execute this command, QoS must be enabled.

Metering cannot be performed on the following logical interfaces. A policy map that includes metering (policer) settings (police-type commands) must not be applied.

- On the SWX3200-52GT, logical interfaces that group ports 1 - 24, 49, 50 with ports 25 - 48, 51, 52
- Logical interfaces that are grouped across member switches constituting a stack

[Example]

Create an aggregate policer "AGP-01".

- Executing metering by TrTCM with CIR:48kbps, PIR:96kbps, CBS:12kbyte, and EBS:12kbyte
- Yellow: rewrite DSCP value to 10, Red: discard

[Aggregate policer creating]

```
SWX3220(config)#aggregate-police AGP-01
SWX3220(config-agg-policer)#police twin-rate 48 96 12 12 yellow-action remark red-
action drop
SWX3220(config-agg-policer)#remark-map yellow ip-dscp 10
SWX3220(config-agg-policer)#exit
```

9.2.32 Set remarking of aggregate policers

[Syntax]

remark-map *color type value*
no remark-map

[Parameter]

color : Bandwidth class to remark

Setting value	Description
yellow	Make remarking settings for bandwidth class Yellow
red	Make remarking settings for bandwidth class Red

type : Type of remarking

Setting value	Description
cos	CoS remarking
ip-precedence	TOS precedence remarking
ip-dscp	DSCP remarking

value : <0 - 7>

CoS or TOS precedence remarking value

: <0 - 63>

DSCP remarking value

[Input mode]

aggregate policer mode

[Description]

Specifies remarking operations for bandwidth classes Yellow and Red that were classified by aggregate policers. In addition, reassign the egress queue according to the egress queue ID table that corresponds to the trust mode.

For remarking, you can select either CoS value, TOS precedence, or DSCP value.

If this is executed with the "no" syntax, the remarking setting is deleted.

In order to perform remarking, you must specify this command and additionally use the **police** command (aggregate policer mode) to specify "remark" as the action for the corresponding bandwidth class.

[Note]

In order to execute this command, QoS must be enabled.

Remarking can be used in conjunction with pre-marking and specifying the egress queue.

Up to four user-defined values may be used for pre-marking/remarking to a DSCP value not recommended in the RFC. The following table shows the DSCP values that are recommended in the RFC.

PHB	DSCP value	RFC
default	0	2474
Class Selector	0, 8, 16, 24, 32, 40, 48, 56	2474
Assured Forwarding	10, 12, 14, 18, 20, 22, 26, 28, 30, 34, 36, 38	2597
Expedited Forwarding(EF)	46	2598

[Example]

Make the following settings for aggregate policer "AGP-01".

- Executing metering by TrTCM with CIR:48kbps, PIR:96kbps, CBS:12kbyte, and PBS:12kbyte
- Yellow: rewrite DSCP value to 10, Red: discard

[Aggregate policer creating]

```
SWX3220(config)#aggregate-police AGP-01
SWX3220(config-agg-policer)#police twin-rate 48 96 12 12 yellow-action remark red-
action drop
SWX3220(config-agg-policer)#remark-map yellow ip-dscp 10
SWX3220(config-agg-policer)#exit
```

9.2.33 Show aggregate policers

[Syntax]

show aggregate-police [*name*]

[Parameter]

name	:	Aggregate policer name. If this is omitted, the command applies to all aggregate policers.

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the contents of an aggregate policer. The contents shown are the same as in the police section shown by the **show class-map** command.

[Note]

In order to execute this command, QoS must be enabled.

[Example]

Show the contents of aggregate policer "AGP-01".

```
SWX3220#show aggregate-police AGP-01

      Aggregator-Police Name: AGP-01
          Mode: TrTCM
          average rate (48 Kbits/sec)
          peak rate (96 Kbits/sec)
          burst size (12 KBytes)
          peak burst size (16 KBytes)
          yellow-action (Transmit)
          red-action (Drop)
```

9.2.34 Apply aggregate policer

[Syntax]

police-aggregate *name*
no police-aggregate *name*

[Parameter]

name	:	Aggregate policer to apply

[Input mode]

policy map class mode

[Description]

Specifies an aggregate policer for a traffic class.

If this is executed with the "no" syntax, the aggregate policer settings for the traffic class are removed.

This cannot be used in conjunction with an individual policer (the **police single-rate and police twin-rate** commands of policy map class mode).

[Note]

In order to execute this command, QoS must be enabled.

Metering cannot be performed on the following logical interfaces. A policy map that includes metering (policer) settings (police-type commands) must not be applied.

- On the SWX3200-52GT, logical interfaces that group ports 1 - 24, 49, 50 with ports 25 - 48, 51, 52
- Logical interfaces that are grouped across member switches constituting a stack

[Example]

Apply aggregate policer "AGP-01" to the two traffic classes "class1" and "class2" of policy map "policy1."

- Executing metering by SrTCM with CIR:48kbps, CBS:12kbyte, and EBS:12kbyte
- Yellow: rewrite DSCP value to 10, Red: discard

[Create an aggregate policer]

```
SWX3220(config)#aggregate-police AGP-01
SWX3220(config-agg-policer)#police single-rate 48 12 12 yellow-action remark red-
```

```
action drop
SWX3220(config-agg-policer)#remark-map yellow ip-dscp 10
SWX3220(config-agg-policer)#exit
```

[Set policy]

```
SWX3220(config)#policy-map policy1
SWX3220(config-pmap)#class class1
SWX3220(config-pmap-c)#police-aggregate AGP-01
SWX3220(config-pmap-c)#exit
SWX3220(config-pmap)#class class2
SWX3220(config-pmap-c)#police-aggregate AGP-01
SWX3220(config-pmap-c)#exit
SWX3220(config-pmap)#exit
SWX3220(config)#interface port1.1
SWX3220(config-if)#service-policy input policy1
```

9.2.35 Show metering counters

[Syntax]

show qos metering-counters [*ifname*]

[Parameter]

ifname	:	LAN/SFP port name or logical interface name. If this is omitted, the command applies to all ports.

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the metering totals for all policers (individual policers / aggregate policers) on the specified LAN/SFP port or logical interface.

The following totals are shown.

Item	Description
Green Bytes	Number of bytes categorized as bandwidth class Green
Yellow Bytes	Number of bytes categorized as bandwidth class Yellow
Red Bytes	Number of bytes categorized as bandwidth class Red

The count starts when the policy map is applied to the LAN/SFP port or logical interface.

[Note]

In order to execute this command, QoS must be enabled.

[Example]

Show the metering totals for LAN port #1.

```
SWX3220#show qos metering-counters port1.1
Interface: port1.1(policy1)

  ****** Individual ******
  Class-map        : class1
      Green Bytes  : 178345
      Yellow Bytes : 0
      Red Bytes    : 0

  ****** Aggregate *******
  Aggregate-policer: AGP-01
  Class-map        : class2
                     class3
      Green Bytes  : 28672
      Yellow Bytes : 2048
      Red Bytes    : 51552
```

9.2.36 Clear metering counters

[Syntax]

clear qos metering-counters [*ifname*]

[Parameter]

ifname	:	LAN/SFP port name or logical interface name. If this is omitted, the command applies to all ports.

[Input mode]

privileged EXEC mode

[Description]

Clears the metering totals for all policers (individual policers / aggregate policers) on the specified LAN/SFP port or logical interface.

[Note]

In order to execute this command, QoS must be enabled.

[Example]

Clear the metering totals for LAN port #1.

```
SWX3220#clear qos metering-counter port1.1
```

9.2.37 Set egress queue (CoS-Queue)

[Syntax]

set cos-queue *value*
no set cos-queue

[Parameter]

value	:	<0 - 7> CoS value corresponding to egress queue

[Input mode]

policy map class mode

[Description]

Assigns an egress queue to the classified traffic class.

Use the CoS value to specify the egress queue; the egress queue that is assigned is based on the "CoS-egress queue ID conversion table."

If this is executed with the "no" syntax, the specification of egress queue based on traffic class is removed.

[Note]

In order to execute this command, QoS must be enabled.

Egress queue specification cannot be used in conjunction with pre-marking.

Egress queue specification based on CoS is only for CoS trust mode. If a policy map contains even one class map that includes this command, that policy map cannot be applied to a port that uses DSCP trust mode.

[Example]

Make the following settings for received frames of LAN port #1

- Permit traffic from the 10.1.0.0 network
- Change the classified traffic class to egress queue 3 (CoS:3)

[Traffic class definition]

```
SWX3220(config)#access-list 1 permit any 10.1.0.0 0.0.255.255 any
SWX3220(config)#class-map class1
SWX3220(config-cmap)#match access-list 1
SWX3220(config-cmap)#exit
```

[Policy settings]

```
SWX3220(config)#policy-map policy1
SWX3220(config-pmap)#class class1
SWX3220(config-pmap-c)#set cos-queue 3
SWX3220(config-pmap-c)#exit
SWX3220(config-pmap)#exit
SWX3220(config)#interface port1.1
SWX3220(config-if)#service-policy input policy1
```

9.2.38 Set egress queue (DSCP-Queue)

[Syntax]

set ip-dscp-queue *value*
no set ip-dscp-queue

[Parameter]

value : <0 - 63>

DSCP value corresponding to egress queue

[Input mode]

policy map class mode

[Description]

Assigns an egress queue to the classified traffic class.

Use the DSCP value to specify the egress queue; the egress queue that is assigned is based on the "DSCP-egress queue ID conversion table."

If this is executed with the "no" syntax, the specification of egress queue based on traffic class is removed.

[Note]

In order to execute this command, QoS must be enabled.

Egress queue specification cannot be used in conjunction with pre-marking.

Egress queue specification based on DSCP is only for DSCP trust mode. If a policy map contains even one class map that includes this command, that policy map cannot be applied to a port that uses DSCP trust mode.

[Example]

Make the following settings for received frames of LAN port #1

- Permit traffic from the 10.1.0.0 network
- Change the classified traffic class to egress queue 3 (DSCP:24)

[Traffic class definition]

```
SWX3220(config)#access-list 1 permit any 10.1.0.0 0.0.255.255 any
SWX3220(config)#class-map class1
SWX3220(config-cmap)#match access-list 1
SWX3220(config-cmap)#exit
```

[Policy settings]

```
SWX3220(config)#policy-map policy1
SWX3220(config-pmap)#class class1
SWX3220(config-pmap-c)#set ip-dscp-queue 24
SWX3220(config-pmap-c)#exit
SWX3220(config-pmap)#exit
SWX3220(config)#interface port1.1
SWX3220(config-if)#service-policy input policy1
```

9.2.39 Show policy map information

[Syntax]

show policy-map [*name*]

[Parameter]

name : Policy map name. If this is omitted, all policy map information is shown.

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows information for the specified policy map. The following content is shown.

Item	Description
Policy-Map Name	Policy map name
State	Application status of the policy map (attached/detached)

Item	Description
Class-Map Name	Class map information. For details, refer to the **show class-map** command.
Match	Classification conditions - Match Access-List (Access list ID) - Match ethertype (Ethernet Type) - Match vlan (VLAN ID) - Match vlan-range (VLAN ID) - Match CoS (CoS value) - Match IP precedence (TOS precedence) - Match IP DSCP (DSCP value)
Set	Pre-marking setting, egress queue setting - Set CoS (Pre-marking setting : CoS value) - Set IP precedence (Pre-marking setting : TOS precedence) - Set IP DSCP (Pre-marking setting : DSCP value) - Set CoS-Queue (Specify egress queue : CoS - Set IP-DSCP-Queue (Specify egress queue : DSCP)
Police	Metering/policing/remarking setting * For details, refer to the following

Details of metering, policing, and remarking settings are as follows.

Item		Description
Aggregator-Police Name		Name of aggregate policer (only if specified)
Mode		Metering algorithm (SrTCM/TrTCM)
Shown only for SrTCM	average rate	Traffic rate (kbits/sec)
	burst size	Burst size of conformant token bucket (kBytes)
	excess burst size	Burst size of excess token bucket (kBytes)
Shown only for TrTCM	average rate	Traffic rate (kbits/sec)
	peak rate	Peak traffic rate (kbits/sec)
	burst size	Burst size of conformant token bucket (kBytes)
	peak burst size	Burst size of peak token bucket (kBytes)
yellow-action		Action for bandwidth class Yellow (transmit/drop/remark)
red-action		Action for bandwidth class Red (drop/remark)

- Of the various items in the "Match" and the "Set", only the single item that has been specified is shown.
- The "Match", the "Set", and the "Police" are not shown if the corresponding command (match, set, police) has not been specified.

[Note]

In order to execute this command, QoS must be enabled.

[Example]

Show information for policy map "policy1".

```
SWX3220#show policy-map policy1
```

```
  Policy-Map Name: policy1
    State: attached

    Class-Map Name: class1
      Qos-Access-List Name: 1
      Police: Mode: SrTCM
              average rate (48 Kbits/sec)
              burst size (12 KBytes)
              excess burst size (12 KBytes)
              yellow-action (Remark [DSCP:10])
              red-action (Drop)
```

9.2.40 Show map status

[Syntax]

show qos map-status *type* [*name*]

[Parameter]

type : Type of map to show

Setting value	Description
policy	Show policy map status information
class	Show class map status information

name : The name of the policy map (or class map) to show. If this is omitted, all policy maps (or class maps)

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows policy map or class map status information.

By using this command, you can obtain information about the combination of policy maps or class maps, such as the LAN/SFP ports and logical interfaces to which a policy map is applied, or the policy maps to which a class map is registered.

The following content is displayed.

policy-map

Item	Display information
input port	List of LAN/SFP ports and logical interfaces to which the policy map is applied
edit/erase	Whether **policy-map/no policy-map** can be executed
attach limitation	Whether attachment is possible for each trust mode

class-map

Item	Display information
policy-map asociation	List of policy maps to which the class map is associated
edit/erase	Whether **class-map/no class-map** can be executed
attach limitation	Whether attachment is possible for each trust mode

Use the **show policy-map** and **show class-map** commands to check the settings of the policy map or class map.

[Note]

In order to execute this command, QoS must be enabled.

[Example]

Show the status of policy map "policy1".

```
SWX3220#show qos map-status policy policy1
policy1 status
  input port            : port1.3

  edit/erase            : Disable
```

```
  attach limitation
    CoS trust mode           : Enable
    DSCP trust mode          : Enable
    Port-Priority trust mode : Disable
```

Show the status of class map "class1".

```
SWX3220#show qos map-status class class1
class1 status
  policy-map association : policy1 (Detached)

  edit/erase             : Disable

  attach limitation
    CoS trust mode           : Enable
    DSCP trust mode          : Enable
    Port-Priority trust mode : Disable
```

9.2.41 Set egress queue scheduling

[Syntax]

qos wrr-weight *queue-id weight*
no qos wrr-weight *queue-id*

[Parameter]

queue-id	:	<0-7>
		Egress queue ID
weight	:	<1-32>
		Weight of WRR

[Initial value]

no qos wrr-weight 0

no qos wrr-weight 1

no qos wrr-weight 2

no qos wrr-weight 3

no qos wrr-weight 4

no qos wrr-weight 5

no qos wrr-weight 6

no qos wrr-weight 7

[Input mode]

global configuration mode

[Description]

Specifies the WRR (weighted round robin) weight for the egress queue.

The scheduling method setting is common to all LAN/SFP ports and logical interfaces.

If this is executed with the "no" syntax, the egress queue uses the strict priority (SP) method.

[Note]

In order to execute this command, QoS must be enabled.

[Example]

Set egress queues #7 and #6 to the SP method (7 has priority), and set #5, #4, #3, #2, #1, and #0 to the WRR method (5:5:5:2:1:1).

```
SWX3220(config)#no qos wrr-weight 7
SWX3220(config)#no qos wrr-weight 6
SWX3220(config)#qos wrr-weight 5 5
SWX3220(config)#qos wrr-weight 4 5
SWX3220(config)#qos wrr-weight 3 5
SWX3220(config)#qos wrr-weight 2 2
```

```
SWX3220(config)#qos wrr-weight 1 1
SWX3220(config)#qos wrr-weight 0 1
```

9.2.42 Set traffic shaping (individual port)

[Syntax]

traffic-shape rate kbps *CIR* **burst** *BC*
no traffic-shape rate

[Parameter]

CIR : Traffic rate (kbps). Due to rounding, the actual value applied may differ from the input value (See [Note])

Model	Input range
SWX3220-16MT, SWX3220-16TMs	<18-10000000>
SWX3220-30MC, SWX3220-30TCs	<50-100000000>

BC : Burst size (kbyte). Specified in 4 kbyte units. (See [Note])

Model	Input range
SWX3220-16MT, SWX3220-16TMs	<16-16000>
SWX3220-30MC, SWX3220-30TCs	<16-4000>

[Initial value]

no traffic-shape rate

[Input mode]

interface mode

[Description]

Specifies shaping for the port.

If this command is executed with the "no" syntax, the port shaping setting is disabled.

[Note]

In order to execute this command, QoS must be enabled.

Due to the rounding of traffic rates, the actual value applied may differ from the input value.

For SWX3220-16MT and SWX3220-16TMs, set the burst size to at least 10 times the maximum MRU value (the largest MRU value among all interfaces).

If the burst size is not set properly, frames will not be transmitted from ports that are configured for shaping.

[Example]

Reduce transmission from LAN port #1 down to CIR:30016 kbps, Bc:1876000 bytes.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#traffic-shape rate kbps 30016 burst 1876
```

9.2.43 Sets traffic shaping (per queue)

[Syntax]

traffic-shape queue *queue-id* **rate kbps** *CIR* **burst** *BC*
no traffic-shape queue *queue-id* **rate**

[Parameter]

queue-id : <0-7>

Egress queue ID

CIR : Traffic rate (kbps). Due to rounding, the actual value applied may differ from the input value (See [Note])

Model	Input range
SWX3220-16MT, SWX3220-16TMs	<18-10000000>
SWX3220-30MC, SWX3220-30TCs	<50-100000000>

BC : Burst size (kbyte). Specified in 4 kbyte units. (See [Note])

Model	Input range
SWX3220-16MT, SWX3220-16TMs	<16-16000>
SWX3220-30MC, SWX3220-30TCs	<16-4000>

[Initial value]

no traffic-shpe queue 0 rate

no traffic-shpe queue 1 rate

no traffic-shpe queue 2 rate

no traffic-shpe queue 3 rate

no traffic-shpe queue 4 rate

no traffic-shpe queue 5 rate

no traffic-shpe queue 6 rate

no traffic-shpe queue 7 rate

[Input mode]

interface mode

[Description]

Specifies shaping for the transmission queue of the port.

If this command is executed with the "no" syntax, the egress queue shaping setting is disabled.

[Note]

In order to execute this command, QoS must be enabled.

Due to the rounding of traffic rates, the actual value applied may differ from the input value.

For SWX3220-16MT and SWX3220-16TMs, set the burst size to at least 10 times the maximum MRU value (the largest MRU value among all interfaces).

If the burst size is not set properly, frames will not be transmitted from ports that are configured for shaping.

[Example]

This filters the transmission from LAN port # 1 queue #0 down to CIR: 10 Mbps, Bc: 64000 bytes.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#traffic-shape queue 0 rate kbps 10000 burst 64
```

9.3 Flow control

9.3.1 Set flow control (IEEE 802.3x PAUSE send/receive) (system)

[Syntax]

flowcontrol *type*
no flowcontrol

[Parameter]

type : Flow control operation

Setting value	Description
enable	Enables flow control
disable	Disables flow control

[Initial value]

flowcontrol disable

[Input mode]

global configuration mode

[Description]

Enables flow control for the entire system (IEEE 802.3x PAUSE frames send/receive).

If this is executed with the "no" syntax, flow control is disabled.

[Note]

If the QoS function is enabled, it is not possible to enable flow control for the system.

If flow control is enabled, the tail drop function is automatically disabled. However, this limitation does not apply if the stack function is enabled.

On the SWX3220-16MT and SWX3220-16TMs, the following limitations apply.

- Flow control for each interface operates only if the flow control settings of the system and of the interface are each enabled.

[Example]

Enable flow control for system.

```
SWX3220(config)#flowcontrol enable
```

9.3.2 Set flow control (IEEE 802.3x PAUSE send/receive) (interface)

[Syntax]

flowcontrol *type*
no flowcontrol

[Parameter]

type : Flow control operation

Setting value	Description
auto	Enable flow control auto negotiation
both	Enable transmission/reception of Pause frames
disable	Disable flow control

[Initial value]

flowcontrol disable

[Input mode]

interface mode

[Description]

Enables flow control for the LAN/SFP port (IEEE 802.3x PAUSE frames send/receive).

If this is executed with the "no" syntax, flow control is disabled.

[Note]

This command can be specified only for LAN/SFP port.

This will not operate if flow control is disabled for the system.

Sending and receiving of PAUSE frames are enabled or disabled as a set.

The period of pause time requested when the SWX3220 transmits a PAUSE frame is 0xFFFF (65535).

The following limitations apply.

- SWX3220-16MT, SWX3220-16TMs
  - Auto-negotiation cannot be used on boards to which an SFP+ module is connected.
  - If the following conditions apply, auto negotiation and Pause frame transmission are unsupported. (Pause frame reception only is supported)
    - If the stack function is enabled and flow control is enabled
- SWX3220-30MC, SWX3220-30TCs

- "flowcontrol auto" cannot be specified for a SFP+/SFP28/QSFP28 port.
- If the following conditions apply, auto negotiation and Pause frame transmission are unsupported. (Pause frame reception only is supported)
  - If the stack function is enabled and flow control is enabled

[Example]

Enable flow control for LAN port #1.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#flowcontrol both
```

Disable flow control for LAN port #1.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#no flowcontrol
```

9.3.3 Show flow control operating status

[Syntax]

show flowcontrol [inteface *ifname*]

[Keyword]

interface	:	Specifies the interface to show

[Parameter]

ifname	:	Name of LAN/SFP port. If this is omitted, the command applies to all interfaces. Interface to show

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows information related to flow control (enabled/disabled, number of PAUSE frames sent/received).

[Note]

The number of PAUSE frames sent and received are shown only if flow control is enabled on the corresponding port.

The number of PAUSE frames sent and received is cleared when you execute the **clear frame-counters** command.

[Example]

Show flow control information for LAN port #1.

```
SWX3220#show flowcontrol port1.1
Port        FlowControl       RxPause TxPause
---------   -----------       ------- -------
port1.1     Both                 4337       0
```

Show flow control information for all ports.

```
SWX3220#show flowcontrol
System flow-control: Enable
Port        FlowControl       RxPause TxPause
---------   -----------       ------- -------
port1.1     Both                 4337       0
port1.2     Disable                 -       -
port1.3     Both                    0    1732
port1.4     Disable                 -       -
port1.5     Disable                 -       -
port1.6     Disable                 -       -
port1.7     Disable                 -       -
port1.8     Disable                 -       -
```

9.4 Storm control

9.4.1 Set storm control

[Syntax]

storm-control *type* [*type*..] **level** *level*
no storm-control

[Parameter]

type : Storm control type

Storm control type	Description
broadcast	Enables broadcast storm control
multicast	Enables multicast storm control
unicast	Enables control for unicast frames with unknown address

level : <0.00-100.00>

Specifies the threshold value as a percentage of the bandwidth
The threshold value can be specified to the second decimal place

[Initial value]

no storm-control

[Input mode]

interface mode

[Description]

Applies reception restrictions to a LAN/SFP port, enabling broadcast storm control, multicast storm control, and control of unicast frames with unknown address.

Incoming frames that exceed the threshold value are discarded. However, no reception restrictions are applied if the threshold value is 100%. The threshold value is common to all frames, and cannot be specified individually.

[Example]

Enable broadcast storm control and multicast storm control for LAN port #1, and set the threshold value to 30%.

```
SWX3220(config)#interface port1.1
SWX3220(config-if)#storm-control broadcast multicast level 30
```

9.4.2 Show storm control reception upper limit

[Syntax]

show storm-control [*ifname*]

[Parameter]

ifname : LAN/SFP port interface name

Interface to show

[Initial value]

none

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the upper limit value for frame reception.

If the interface name is omitted, all interfaces are shown.

[Example]

Show the setting status of all interfaces.

```
SWX3220#show storm-control
Port      BcastLevel    McastLevel    UcastLevel
port1.1     30.00%        30.00%       100.00%
port1.2     20.00%        20.00%        20.00%
port1.3    100.00%       100.00%       100.00%
port1.4    100.00%       100.00%       100.00%
port1.5     50.00%        50.00%       100.00%
port1.6    100.00%       100.00%       100.00%
port1.7    100.00%       100.00%        30.00%
port1.8    100.00%       100.00%        30.00%
```

Chapter 10

Application

10.1 DHCP server

10.1.1 Set the DHCP server function (system)

[Syntax]

dhcp-server *switch*
no dhcp-server

[Parameter]

switch : Behavior DHCP server function

Setting value	Description
enable	Enable the DHCP server function
disable	Disable the DHCP server function

[Initial value]

dhcp-server disable

[Input mode]

global configuration mode

[Description]

Configures the operations of the DHCP server function for the entire system.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

To enable the DHCP server function, you must enable the DHCP server function for the interface in addition to using this command.

[Example]

Enable the DHCP server function for the entire system.

```
SWX3220(config)#dhcp-server enable
```

Disable the DHCP server function for the entire system.

```
SWX3220(config)#dhcp-server disable
```

10.1.2 Set the DHCP server function (interface)

[Syntax]

dhcp-server *switch*
no dhcp-server

[Parameter]

switch : Behavior DHCP server function

Setting value	Description
enable	Enable the DHCP server function
disable	Disable the DHCP server function

[Initial value]

dhcp-server disable

[Input mode]

interface mode

[Description]

Configures the operations for the DHCP server of the applicable interface.

This can only be set for VLAN interface.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

To enable the DHCP server function, you must enable the DHCP server function for the entire system in addition to using this command.

Information distributed by the DHCP server function such as IP addresses is set in the DHCP pool.

The DHCP pool is configured using the **dhcp pool** command. For VLAN interface, the IPv4 address must be specified.

For this command, up to 32 for VLAN interface can be set.

[Example]

Enable the DHCP server function on VLAN #1.

```
SWX3220(config)#interface vlan1
SWX3220(config-if)#dhcp-server enable
```

Disable the DHCP server function on VLAN #1.

```
SWX3220(config)#interface vlan1
SWX3220(config-if)#dhcp-server disable
```

10.1.3 DHCP server operation type settings

[Syntax]

server-type *type*
no server-type

[Parameter]

type : DHCP server operation type

Operation mode	Explanation
normal	Ordinary DHCP server
auth-web	DHCP server for Web authentication

[Initial value]

server-type normal

[Input mode]

DHCP mode

[Description]

This sets the operation mode for the applicable DHCP pool.

When “auth-web” is specified for TYPE, DHCPNAK is sent to clients that send DHCP requests in which the IP address and VLAN do not match.

If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

This sets the operation type of the DHCP pool “pool_auth” to the DHCP server for Web authentication.

```
SWX3220(config)#dhcp pool pool_auth
SWX3220(config-dhcp)#server-type auth-web
```

10.1.4 Set DHCP pool

[Syntax]

dhcp pool *pool_name*

no dhcp pool *pool_name*

[Parameter]

pool_name	:	DHCP pool name Single-byte alphanumeric characters and single-byte symbols(31 characters or less)

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Moves to DHCP mode to configure the DHCP pool settings.

In DHCP mode, this configures the settings for the DHCP pool name specified by this command.

If this command is executed with the "no" syntax, the setting value is deleted.

[Note]

Use the **exit** command to return to global configuration mode from DHCP mode, and use the **end** command to return to privileged EXEC mode.

After creating the DHCP pool, you must first specify the network containing DHCP clients using the **network** command.

The number of DHCP pools that can be set is 64.

[Example]

This creates a DHCP pool called "pool_vlan1", and moves to DHCP mode.

```
SWX3220(config)#dhcp pool pool_vlan1
SWX3220(config-dhcp)#
```

10.1.5 Set network interface

[Syntax]

network *ip_address*/*mask*
network *ip_address netmask*
no network

[Parameter]

ip_address	:	A.B.C.D IP address
mask	:	<1-31> Number of mask bits
netmask	:	A.B.C.D Address format of the net mask

[Initial value]

none

[Input mode]

DHCP mode

[Description]

Sets the network interface in the applicable DHCP pool.

If this command is executed with the "no" syntax, the setting value is deleted.

When the DHCP client is on the same network as the VLAN interface that enables the DHCP server function, this specifies the network for the IP address that is configured in the VLAN interface.

When accepting a request from a DHCP client via the DHCP relay agent, this specifies the network that the client belongs to.

[Note]

Multiple pools with the same network part cannot be set.

The "Subnet Mask" DHCP option (option code 1) notified to the client uses the value for this command.

[Example]

Set the 192.168.100.0/24 network part in the applicable "pool_vlan1" DHCP pool.

```
SWX3220(config)#dhcp pool pool_vlan1
SWX3220(config-dhcp)#network 192.168.100.0/24
```

10.1.6 Set range of IP addresses to be assigned(DHCP)

[Syntax]

range *start_ip_address* [*end_ip_address*]
no range [*start_ip_address* [*end_ip_address*]]

[Parameter]

start_ip_address	:	A.B.C.D The first IP address amongst all assigned IP addresses
end_ip_address	:	A.B.C.D The last IP address amongst all assigned IP addresses If only one address was assigned, this can be omitted

[Initial value]

none

[Input mode]

DHCP mode

[Description]

Sets the IP address range to assign for the applicable DHCP pool.

The addresses to assign must be within the **network** specified by the network command.

Up to eight address ranges can be set.

You cannot include the same IP address in multiple DHCP pools.

You cannot include the same IP address in multiple ranges.

You cannot include a network address or a broadcast address within an IP address range.

You cannot use IP addresses that duplicate those which were specified using the **range** command in DHCP pool class mode.

You cannot include the same IP address that is specified within the range of IP addresses using the **range** command in DHCP pool class mode.

If this command is executed with the "no" syntax by specifying a parameter, the setting value with the specified parameter will be deleted.

If this command is executed with the "no" syntax without specifying a parameter, all setting values that are set in the applicable DHCP pool will be deleted.

[Note]

If the total number of ranges set using the **range** command for all pools and all pool classes exceeds 8192, this command will result in an error.

[Example]

Set the IP address range of 192.168.100.2 to 192.168.100.191/24 for a DHCP pool called "pool_vlan1".

```
SWX3220(config)#dhcp pool pool_vlan1
SWX3220(config-dhcp)#range 192.168.100.2 192.168.100.191
```

10.1.7 Setting the IP address to assign to a specific client

[Syntax]

bind host *ip_address mac_address*
no bind host [*ip_address*]

[Parameter]

ip_address	:	A.B.C.D IP address to assign to a specific client
mac_address	:	HHHH.HHHH.HHHH MAC address of cliant

[Initial value]

none

[Input mode]

DHCP mode

[Description]

Sets the IP address to assign to a client in the applicable DHCP pool that has a specific MAC address.

The addresses to assign must be within the network specified by the **network** command.

The maximum **bind host** command setting is the 4096 for the total number of **bind host** commands for all pools.

The same IP address cannot be specified for multiple MAC addresses within a single pool.

Multiple IP addresses cannot be specified for a single MAC addresses within a single pool.

You cannot include a network address or a broadcast address within an IP address range.

If this command is executed with the "no" syntax by specifying a parameter, the setting value with the specified parameter will be deleted.

If this command is executed with the "no" syntax without specifying a parameter, all setting values that are set in the applicable DHCP pool will be deleted.

[Example]

This sets the command to assign the IP address of 192.168.100.100 to the client with a MAC address of 00a0.deae.b893.

```
SWX3220(config-dhcp)#bind host 192.168.100.100 00a0.deae.b893
```

10.1.8 Set lease time(DHCP)

[Syntax]

lease *day hour min* [*sec*]
no lease

[Parameter]

day	:	<0-120> Days
hour	:	<0-23> Hours
min	:	<0-59> Minutes
sec	:	<0-59> Secconds (If sec is omitted, 0 is specified)

[Initial value]

lease 1 0 0

(A day)

[Input mode]

DHCP mode

[Description]

Sets the IP address lease time for the applicable DHCP pool.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

The minimum value is 20 seconds. (lease 0 0 0 20).

[Example]

Set the lease time to 6 hours.

```
SWX3220(config-dhcp)#lease 0 6 0
```

10.1.9 Settings for duplication checks of leased IP addresses

[Syntax]

probe *switch*
no probe

[Parameter]

switch : Operations for duplication checks of leased IP addresses

Setting value	Description
enable	Enables duplication checks
disable	Disables duplication checks

[Initial value]

probe enable

[Input mode]

DHCP mode

[Description]

Sets duplication checks of leased IP addresses for the applicable DHCP pool.

If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

Enable duplication checks.

```
SWX3220(config-dhcp)#probe enable
```

Disable duplication checks.

```
SWX3220(config-dhcp)#probe disable
```

10.1.10 Timeout duration settings for duplication checks of leased IP addresses

[Syntax]

probe timeout *timeout*
no probe timeout

[Parameter]

timeout : <1-5>

Time to wait for a reply to transmitted packets (seconds)

[Initial value]

probe timeout 1

[Input mode]

DHCP mode

[Description]

Sets the timeout duration for duplication checks of leased IP addresses for the applicable DHCP pool.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

PING is used to check.

[Example]

Set the timeout duration to 2 seconds.

```
SWX3220(config-dhcp)#probe timeout 2
```

10.1.11 Default gateway address notification setting(DHCP)

[Syntax]

default-router *ip_address*
no default-router [*ip_address*]

[Parameter]

ip_address	:	A.B.C.D IP address

[Initial value]

none

[Input mode]

DHCP mode

[Description]

Sets the IP address to notify as a default gateway from the applicable DHCP pool.

The specified address must be within the network specified by the **network** command.

Up to eight addresses can be set.

If this command is executed with the "no" syntax by specifying a parameter, the setting value with the specified parameter will be deleted.

If this command is executed with the "no" syntax without specifying a parameter, all setting values that are set in the applicable DHCP pool will be deleted.

[Note]

The "Router Option" DHCP option (option code 3) notified to the client uses the value for this command.

[Example]

This sets the notified default gateway address to 192.168.100.1.

```
SWX3220(config-dhcp)#default-router 192.168.100.1
```

10.1.12 DNS server settings for notification(DHCP)

[Syntax]

dns-server *ip_address*
no dns-server [*ip_address*]

[Parameter]

ip_address	:	A.B.C.D IP address

[Initial value]

none

[Input mode]

DHCP mode

[Description]

Configures the IP address to notify as a DNS for the applicable DHCP pool.

Up to eight addresses can be set.

If this command is executed with the "no" syntax by specifying a parameter, the setting value with the specified parameter will be deleted.

If this command is executed with the "no" syntax without specifying a parameter, all setting values that are set in the applicable DHCP pool will be deleted.

[Note]

The "Domain Name Server Option" DHCP option (option code 6) notified to the client uses the value for this command.

[Example]

Sets 192.168.100.1 for the DNS to notify.

```
SWX3220(config-dhcp)#dns-server 192.168.100.1
```

10.1.13 Domain name settings for notification(DHCP)

[Syntax]

domain-name *domain_name*
no domain-name

[Parameter]

domain_name	:	Domain name Up to 253 single-byte alphanumeric characters, including dots and hyphens

[Initial value]

none

[Input mode]

DHCP mode

[Description]

Sets the domain name for the applicable DHCP pool.

If this command is executed with the "no" syntax, the setting value is deleted.

[Note]

The "Domain Name" DHCP option (option code 15) notified to the client uses the value for this command.

The length of the portion of the domain name separated by a dot (.) (the label) must be at least one character and no more than 63 characters.

If the first character of the domain name is a dot (.) then this command produces an error.

[Example]

Sets the domain name to be notified as yamaha.example.com.

```
SWX3220(config-dhcp)#domain-name yamaha.example.com
```

10.1.14 Set boot file name

[Syntax]

bootfile *boot_file_name*
no bootfile

[Parameter]

boot_file_name	:	Boot file name Single-byte alphanumeric characters and single-byte symbols (127 characters or less)

[Initial value]

none

[Input mode]

DHCP mode

[Description]

Sets the boot file name for the applicable DHCP pool.

If this command is executed with the "no" syntax, the setting value is deleted.

[Note]

Use the **next-server** command for addresses on servers when the boot file is located.

[Example]

This sets the boot file name as "execfile".

```
SWX3220(config-dhcp)#bootfile execfile
```

10.1.15 Settings for the server on which the boot file is located

[Syntax]

next-server *ip_address*
no next-server

[Parameter]

ip_address : A.B.C.D
IP address

[Initial value]

none

[Input mode]

DHCP mode

[Description]

Configures the server on which the boot file is located for the applicable DHCP pool.

If this command is executed with the "no" syntax, the setting value is deleted.

[Example]

Set 192.168.100.1 on the server on which the boot file is located.4

```
SWX3220(config-dhcp)#next-server 192.168.100.1
```

10.1.16 Set user-defined DHCP pptions(DHCP)

[Syntax]

option *option value*
no option [*option*]

[Parameter]

option : Option

Setting value	Description
<1-255>	Option number
Mnemonic	Character string recognized as a mnemonic

value : Option value

[Initial value]

none

[Input mode]

DHCP mode

[Description]

Sets the user-defined option value for the applicable DHCP pool.

Up to 32 values can be set.

If this command is executed with the "no" syntax by specifying a parameter, the setting value with the specified parameter will be deleted.

If this command is executed with the "no" syntax without specifying a parameter, all setting values that are set in the applicable DHCP pool will be deleted.

The types of values that are available are listed below. The option number determines which values can be used. For example, ‘router’, ‘dns’ and , ‘wins server’ are an array of IP addresses, and ‘hostname’ and ‘domain’ are text strings.

1-octet integer	0..255
2-octet integer	0..65535
Array of 2-octet integers	Series of 2-octet integers delimited by commas (Max eight)
4-octet integer	0..4294967295
IP address	IP address
Array of IP addresses	IP addresses delimited by commas (Max eight)
Text string	Text string (Single-byte alphanumeric characters and single-byte symbols, max 127 characters)
Switches	"on", "off", "1", or "0"

The available options are shown below.

Option number / Mnemonics that can be used with a command	Option type
1/subnet mask	IP address
2/time_offset	4-octet integer
3/router	Array of IP addresses
4/time_server	Array of IP addresses
5/name_server	Array of IP addresses
6/dns	Array of IP addresses
7/log_server	Array of IP addresses
8/cookie_server	Array of IP addresses
9/lpr_server	Array of IP addresses
10/impress_server	Array of IP addresses
11/resource_location_server	Array of IP addresses
12/hostname	Text string
13/boot_file_size	2-octet integer
14/merit_dump_file	Text string
15/domain	Text string
16/swap_server	IP address
17/root_path	Text string
18/extensions_pathname	Text string
19/ip_forwarding	Switches
20/non_local_source_routing	Switches
21/policy_filter	Array of IP addresses *An even number of IP addresses must be set, consisting of a combination of IP address and mask
22/maximum_datagram_reassembly	2-octet integer
23/default_ip_ttl	1-octet integer
24/path_mtu_aging_timeout	4-octet integer
25/path_mtu_plateau_table	Array of 2-octet integers
26/interface_mtu	2-octet integer

Option number / Mnemonics that can be used with a command	Option type
27/all_subnets_are_local	Switches
28/broadcast_address	IP address
29/perform_mask_discovery	Switches
30/mask_supplier	Switches
31/perform_router_discovery	Switches
32/router_solicitation_address	IP address
33/static_route	Array of IP addresses :An even number of IP addresses must be set, consisting of a combination of destination address and router address
34/trailer_encapsulation	Switches
35/arp_cache_timeout	4-octet integer
36/ethernet_encapsulation	Switches
37/tcp_default_ttl	1-octet integer
38/tcp_keepalive_interval	4-octet integer
39/tcp_keepalive_garbage	Switches
40/nis_domain	Text string
41/nis_server	Array of IP addresses
42/ntp_server	Array of IP addresses
44/wins_server	Array of IP addresses
45/nbt_dd_server	Array of IP addresses
46/nbt_node_type	1-octet integer
47/nbt_scope	Text string
48/x_font_server	Array of IP addresses
49/x_display_manager	Array of IP addresses
62/netware_domain_name	Text string
64/nis+_domain	Text string
65/nis+_server	Array of IP address
66/tftp_server_name	Text string
67/boot_file_name	Text string
68/mobile_ip_home_agent	Array of IP addresses
69/smtp_server	Array of IP address
70/pop3_server	Array of IP addresses
71/nntp_server	Array of IP addresses
72/default_www_server	Array of IP addresses
73/default_finger_server	Array of IP addresses
74/default_irc_server	Array of IP addresses
75/streettalk_server	Array of IP addresses
76/streettalk_directory_assistance_server	Array of IP addresses
85/nds_server	Array of IP addresses
86/nds_tree_name	Text string

Option number / Mnemonics that can be used with a command	Option type
87/nds_context	Text string

[Note]

The DHCP option notified to the client uses the value for this command.

If the client does not request the relevant option, the relevant option will not actually be transmitted.

When re-registering for option numbers that have already been set, the settings will be overwritten.

[Example]

192.168.100.240 will be set in the "Time Server" DHCP option (option code 4).

```
SWX3220(config-dhcp)#option time_server 192.168.100.240
```

10.1.17 DHCP class settings

[Syntax]

dhcp class *class_name*
no dhcp class *class_name*

[Parameter]

class_name : DHCP class name

Up to 31 single-byte alphanumeric characters and symbols, other than the characters ?"|> and single-byte spaces

[Initial value]

None

[Input mode]

global configuration mode

[Description]

Switches to DHCP class mode to configure the DHCP class settings.

In DHCP class mode, this configures the settings for the DHCP class name specified by this command.

If this command is executed with the "no" syntax, the setting value is deleted.

[Note]

Use the **exit** command to return to global configuration mode from DHCP class mode, and use the **end** command to return to privileged EXEC mode.

The number of DHCP pools that can be set is 16.

[Example]

This creates a DHCP class called "class_customer1", and switches to DHCP class mode.

```
SWX3220(config)#dhcp class class_customer1
SWX3220(config-dhcp-class)#
```

10.1.18 Remote-id settings

[Syntax]

remote-id *remote-id*
no remote-id [*remote-id*]

[Parameter]

remote-id : Hexadecimal value up to 65 bytes; bytes separated by colons

[Initial value]

None

[Input mode]

DHCP class mode

[Description]

Sets the remote-id used for DHCP Option 82 for the applicable DHCP class.

The maximum number of settings for the **remote-id** command is 128, which is the total of all DHCP class **remote-id** commands.

If this command is executed with the "no" syntax by specifying a parameter, the setting value with the specified parameter will be deleted.

If this command is executed with the "no" syntax without specifying a parameter, all remote-id setting values in the applicable DHCP class will be deleted.

[Example]

This sets remote-id "00:06:ac:44:f2:00:00:01" for the DHCP class "class_customer1".

```
SWX3220(config)#dhcp class class_customer1
SWX3220(config-dhcp-class)#remote-id 00:06:ac:44:f2:00:00:01
```

10.1.19 circuit-id settings

[Syntax]

circuit-id *circuit-id*
no circuit-id [*circuit-id*]

[Parameter]

circuit-id	:	Hexadecimal value up to 65 bytes; bytes separated by colons

[Initial value]

None

[Input mode]

DHCP class mode

[Description]

Sets circuit-id used for DHCP Option 82 as the applicable DHCP class.

The maximum number of settings for the **circuit-id** command is, 128, which is the total of all DHCP class **circuit-id** commands.

If this command is executed with the "no" syntax by specifying a parameter, the setting value with the specified parameter will be deleted.

If this command is executed with the "no" syntax without specifying a parameter, all setting values for circuit-id in the applicable DHCP class will be deleted.

[Example]

Sets circuit-id "01:06:00:01:00:00:13:8d" for the DHCP class "class_customer1".

```
SWX3220(config)#dhcp class class_customer1
SWX3220(config-dhcp-class)#circuit-id 01:06:00:01:00:00:13:8d
```

10.1.20 subscriber-id settings

[Syntax]

subscriber-id *subscriber-id*
no subscriber-id [*subscriber-id*]

[Parameter]

subscriber-id	:	Single-byte alphanumeric characters, and symbols other than the single-byte characters "?", "|" and ">" (50 characters or less)

[Initial value]

None

[Input mode]

DHCP class mode

[Description]

Sets the subscriber-id used for DHCP Option 82 for the applicable DHCP class.

The maximum number of settings for the **subscriber-id** command is 128, which is the total of all DHCP class **subscriber-id** commands.

If this command is executed with the "no" syntax by specifying a parameter, the setting value with the specified parameter will be deleted.

If this command is executed with the "no" syntax without specifying a parameter, all setting values for subscriber-id in the applicable DHCP class will be deleted.

[Example]

Sets subscriber-id "subscriber_id_1" for the DHCP class "class_customer1".

```
SWX3220(config)#dhcp class class_customer1
SWX3220(config-dhcp-class)#subscriber-id subscriber_id_1
```

10.1.21 DHCP pool class settings

[Syntax]

dhcp pool class *class_name*
no dhcp pool class *class_name*

[Parameter]

class_name	:	DHCP class name Up to 31 single-byte alphanumeric characters and symbols, other than the characters ?"|> and single-byte spaces

[Initial value]

None

[Input mode]

DHCP mode

[Description]

Switches to DHCP pool class mode to configure the DHCP pool class settings.

You must use the **dhcp class** command to create the DHCP class name beforehand.

If the contents of Option 82 are the same as the applied class id, the settings in the DHCP pool class are used on the DHCP server.

The maximum number of DHCP pool classes that can be set is 16.

If this command is executed with the "no" syntax, the setting value is deleted.

[Note]

Use the exit command to return to DHCP mode from DHCP pool class mode, and use the end command to return to privileged EXEC mode.

The DHCP class name is specified as the class name in the **dhcp class** command. If the class name being used by this command is deleted, this command is also deleted.

[Example]

This switches to DHCP pool class mode.

```
SWX3220(config)#dhcp pool pool1
SWX3220(config-dhcp)#dhcp pool class class_customer1
SWX3220(config-dhcp-pool-class)#
```

10.1.22 Range of IP addresses to assign (DHCP pool class).

[Syntax]

range *start_ip_address* [*end_ip_address*]
no range [*start_ip_address* [*end_ip_address*]]

[Parameter]

start_ip_address	:	A.B.C.D The first IP address amongst all assigned IP addresses
end_ip_address	:	A.B.C.D The last IP address amongst all assigned IP addresses If only one address was assigned, this can be omitted

[Initial value]

None

[Input mode]

DHCP pool class mode

[Description]

Sets the IP address range to assign for the applicable DHCP pool.

The addresses to assign must be within the network specified by the **network** command.

Up to eight address ranges can be set.

You cannot include the same IP address in multiple DHCP pools.

You cannot include the same IP address in multiple ranges.

You cannot include a network address or a broadcast address within an IP address range.

You cannot use IP addresses that duplicate those which were specified using the **range** command in DHCP mode.

You cannot include the same IP address that is specified within the range of IP addresses using the **range** command in DHCP mode.

If this command is executed with the "no" syntax by specifying a parameter, the setting value with the specified parameter will be deleted.

If this command is executed with the "no" syntax without specifying a parameter, all setting values that are set in the applicable DHCP pool will be deleted.

[Note]

If the total number of ranges set using the **range** command for all pool classes and all pools exceeds 8192, this command will result in an error.

[Example]

This sets the IP address range of "192.168.100.10 to 192.168.100.20/24" for a DHCP pool called "pool1".

```
SWX3220(config)#dhcp pool pool1
SWX3220(config-dhcp)#dhcp pool class class_customer1
SWX3220(config-dhcp-pool-class)#range 192.168.100.10 192.168.100.20
```

10.1.23 Lease time settings (DHCP pool class)

[Syntax]

lease *day hour min* [*sec*]
no lease

[Parameter]

day	:	<0-120> Day
hour	:	<0-23> Hour
min	:	<0-59> Minute
sec	:	<0-59> Seconds (if omitted, this is 0)

[Initial value]

lease 1 0 0

(One day)

[Input mode]

DHCP pool class mode

[Description]

Sets the IP address lease time for the applicable DHCP pool.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

The minimum value is 20 sec. (lease 0 0 0 20).

[Example]

This sets the lease time to 6 hours.

```
SWX3220(config)#dhcp pool pool1
SWX3220(config-dhcp)#dhcp pool class class_customer1
SWX3220(config-dhcp-pool-class)##lease 0 6 0
```

10.1.24 Default gateway address notification setting (DHCP pool class)

[Syntax]

default-router *ip_address*
no default-router [*ip_address*]

[Parameter]

ip_address	:	A.B.C.D IP address

[Initial value]

None

[Input mode]

DHCP pool class mode

[Description]

Sets the IP address to notify as a default gateway from the applicable DHCP pool.

The specified address must be an address within the network specified by the DHCP mode **network** command.

Up to eight addresses can be set.

If this command is executed with the "no" syntax by specifying a parameter, the setting value with the specified parameter will be deleted.

If this command is executed with the "no" syntax without specifying a parameter, all setting values that are set in the applicable DHCP pool will be deleted.

[Note]

The "Router Option" DHCP option (option code 3) notified to the client uses the value for this command.

If this command is not set, the "Router Option" DHCP option (option code 3) notified to the client uses the value for the DHCP mode **default-router** command.

[Example]

This sets the notified default gateway address to 192.168.100.1.

```
SWX3220(config)#dhcp pool pool1
SWX3220(config-dhcp)#dhcp pool class class_customer1
SWX3220(config-dhcp-pool-class)#default-router 192.168.100.1
```

10.1.25 DNS server settings for notification (DHCP pool class)

[Syntax]

dns-server *ip_address*
no dns-server [*ip_address*]

[Parameter]

ip_address : A.B.C.D

IP address

[Initial value]

None

[Input mode]

DHCP pool class mode

[Description]

Configures the IP address to notify as a DNS server for the applicable DHCP pool class.

Up to eight addresses can be set.

If this command is executed with the "no" syntax by specifying a parameter, the setting value with the specified parameter will be deleted.

If this command is executed with the "no" syntax without specifying a parameter, all setting values that are set in the applicable DHCP pool will be deleted.

[Note]

The "Domain Name Server Option" DHCP option (option code 6) notified to the client uses the value for this command.

If this command is not set, the "Domain Name Server Option" DHCP option (option code 6) notified to the client uses the value for the DHCP mode **dns-server** command.

[Example]

Sets 192.168.100.1 for the DNS server to notify.

```
SWX3220(config)#dhcp pool pool1
SWX3220(config-dhcp)#dhcp pool class class_customer1
SWX3220(config-dhcp-pool-class)#dns-server 192.168.100.1
```

10.1.26 Domain name settings for notification (DHCP pool class)

[Syntax]

domain-name *domain_name*
no domain-name

[Parameter]

domain_name : Domain name

Up to 253 single-byte alphanumeric characters, including dots and hyphens

[Initial value]

None

[Input mode]

DHCP pool class mode

[Description]

Sets the domain name for the applicable DHCP pool class.

If this command is executed with the "no" syntax, the setting value is deleted.

[Note]

The "Domain Name" DHCP option (option code 15) notified to the client uses the value for this command.

If this command is not set, the "Domain Name" DHCP option (option code 15) notified to the client uses the value for the DHCP mode **domain-name** command.

The length of the portion of the domain name separated by a dot (.) (the label) must be at least one character and no more than 63 characters.

If the first character of the domain name is a dot (.) then this command produces an error.

[Example]

This sets the domain name to be notified as yamaha.example.com.

```
SWX3220(config)#dhcp pool pool1
SWX3220(config-dhcp)#dhcp pool class class_customer1
SWX3220(config-dhcp-pool-class)#domain-name yamaha.example.com
```

10.1.27 Show information of DHCP pool

[Syntax]

show dhcp pool [*pool_name*]

[Parameter]

pool_name	:	Pool name Pool name to show

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows information of DHCP pool.

When POOL_NAME is specified, only the information for the specified POOL_NAME will be shown.

The following items are shown.

- DHCP pool na,e
- Network address
- IP address assigned as static
- Range of IP addresses assigned dynamically
- Lease time
- Sub netmask
- Duplication check
- Total number of dynamically assigned IP addresses, and quantity of each
- DHCP class names applied to a pool, and DHCP class settings
- Range of IP addresses dynamically assigned within a DHCP class to a pool
- Lease time in a DHCP class assigned to a pool

[Note]

If network is not enabled for the DHCP pool, this will not be shown.

"Total number of dynamically assigned IP addresses, and quantity of each" is only displayed when the DHCP server settings are enabled.

Large amounts of lease information may take time to display.

[Example]

Show the current pool status.

```
SWX3220#show dhcp pool
Pool: p1
  network: 192.168.100.0/24
  address ranges:
    addr: 192.168.100.2 to 192.168.100.191
  static host addresses:
  lease <days:hours:minutes:seconds> <120:23:59:59>
  sub netmask: 255.255.255.0
  Probe:
    Status: Enabled
    Timeout: 1
  Dynamic addresses:
    Total:     189
    Leased:    1
  DHCP class: class_customer1
    remote-id: 00:06:ac:44:f2:00:00:01
```

```
    circuit-id: 01:06:00:01:00:00:13:8d
    subscriber-id: subscriber_id_1
    address ranges:
      addr: 192.168.100.10 to 192.168.100.20
    lease <days:hours:minutes:seconds> <1:0:0:0>
```

10.1.28 Show IP address assignment information for DHCP clientsDHCP

[Syntax]

show dhcp binding [*pool_name*]

[Parameter]

pool_name	:	Pool name Pool name to show

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows IP address assignment information for DHCP clients.

When POOL_NAME is specified, only the information for the specified POOL_NAME will be shown.

The following items are shown.

- DHCP pool name
- Network address
- Assigned IP addresses
- MAC address of the assigned client
- Type (dynamic assignment or static assignment)
- Lease finish time
- HostName

[Note]

IP addresses set as static assignments will always be displayed with this command.

Large amounts of lease information may take time to display.

When a notification is received via DHCP HostName option from a client, the HostName is displayed for dynamically-distributed addresses. If a notification has not been received via DHCP HostName option from a client, “-” is displayed. Up to 64 characters can be shown for HostName.

[Example]

Show the current pool status.

```
SWX3220#show dhcp binding
Pool p1 Network 192.168.100.0/24
DHCP Client Entries
IP Address       MacAddr         Type     Expiry               HostName
-------------------------------------------------------------------------------
192.168.100.100  0000.5e00.5300  Dynamic  2020/07/31 14:30:16  Example
192.168.100.101  0000.5e00.5301  Dynamic  2020/07/31 14:28:36  -
192.168.100.120  0000.5e00.5302  Static   -                    -
```

10.1.29 Show DHCP server status

[Syntax]

show dhcp server

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows tje DHCP server status.

The following items are shown.

- DHCP server boot status
- The interface on which the DHCP server is running. Will display when the server is running.
- DHCP server function enable/disable for the entire system
- DHCP server function interface settings

- DHCP server function pool settings

[Example]

Show the current DHCP server status.

```
SWX3220#show dhcp server
DHCP server is running
  running interface list : vlan1 vlan2 vlan3
DHCP server system setting : enable
DHCP server interface setting list : vlan1 vlan2 vlan3
Pool list : p1 p2 p3
```

10.1.30 Delete lease information on DHCP server

[Syntax]

clear dhcp-server lease

[Input mode]

privileged EXEC mode

[Description]

Deletes the lease information (IP address assignment information) on the DHCP server.

[Note]

The DHCP server must be stopped when executing this command.

Use the **show dhcp server** command to check the DHCP boot status.

[Example]

This deletes the lease information.

```
SWX3220#clear dhcp-server lease
```

10.2 DHCPv6 server

10.2.1 DHCPv6 server function settings (system)

[Syntax]

dhcpv6-server *switch*
no dhcpv6-server

[Parameter]

switch : DHCPv6 server function operation

Setting value	Description
enable	Enables the DHCPv6 server function.
disable	Disables the DHCPv6 server function.

[Initial value]

dhcpv6-server disable

[Input mode]

global configuration mode

[Description]

Configures the operations of the DHCPv6 server function for the entire system.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

To enable the DHCPv6 server function, you must configure the pool by using the **dhcpv6-server** command on VLAN interface as well, in addition to using this command.

This command cannot be used if the stack function is enabled.

[Example]

This enables the DHCPv6 server function for the entire system.

```
SWX3220(config)#dhcpv6-server enable
```

This disables the DHCPv6 server function for the entire system.

```
SWX3220(config)#dhcpv6-server disable
```

10.2.2 Set DHCPv6 server function (interface)

[Syntax]

dhcpv6-server *pool_name*
no dhcpv6-server

[Parameter]

pool_name	:	DHCPv6 pool name Single-byte alphanumeric characters and single-byte symbols (31 characters or less)

[Initial value]

None

[Input mode]

interface mode

[Description]

Configures the operations for the DHCPv6 server of the applicable interface.

This can only be set for VLAN interface.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

To enable the DHCPv6 server function, you must enable the DHCPv6 server function for the entire system in addition to using this command.

Information distributed by the DHCPv6 server function is set in the DHCPv6 pool.

The DHCPv6 pool that you specify using this command is set using the **dhcpv6 pool** command.

For VLAN interface, the global IPv6 address must be specified using the **ipv6 address** command.

If all VLAN interface global IPv6 addresses that were set with this command have been deleted, this command is also deleted.

This command can be specified for a maximum of 32 VLAN interface.

This cannot be set for VLAN interface that has already been set using the **ipv6 address autoconfig**, **ipv6 address dhcp** or **ipv6 dhcp client pd** commands.

This command cannot be used if the stack function is enabled.

[Example]

This enables the pool name "pool_vlan1" DHCPv6 server function for VLAN #1.

```
SWX3220(config)#interface vlan1
SWX3220(config-if)#dhcpv6-server pool_vlan1
```

This disables the DHCPv6 server function on VLAN #1.

```
SWX3220(config)#interface vlan1
SWX3220(config-if)#no dhcpv6-server
```

10.2.3 DHCPv6 pool settings

[Syntax]

dhcpv6 pool *pool_name*
no dhcpv6 pool *pool_name*

[Parameter]

pool_name	:	DHCPv6 pool name Single-byte alphanumeric characters and single-byte symbols (31 characters or less)

[Initial value]

None

[Input mode]

global configuration mode

[Description]

Switches to DHCPv6 mode to configure the DHCPv6 pool settings.

In DHCPv6 mode, this configures the settings for the DHCPv6 pool name specified by this command.

If this command is executed with the "no" syntax, the setting value is deleted.

You cannot delete by using the **dhcpv6-server** command for the interface if the pool is in use.

You must first delete the configuration of the **dhcpv6-server** command for the interface.

[Note]

Use the **exit** command to return to global configuration mode from DHCPv6 mode, and use the **end** command to return to privileged EXEC mode.

The number of DHCPv6 pools that can be set is 64.

This command cannot be used if the stack function is enabled.

[Example]

This creates a DHCPv6 pool called "pool_vlan1", and switches to DHCPv6 mode.

```
SWX3220(config)#dhcpv6 pool pool_vlan1
SWX3220(config-dhcp6)#
```

10.2.4 Set the range of IPv6 addresses assigned dynamically (DHCPv6)

[Syntax]

range *start_ipv6_address end_ipv6_address/prefix_len* [lifetime *valid preferred*]
range *pd_prefixname start_pd_ipv6_address end_pd_ipv6_address/prefix_len* [lifetime *valid preferred*]
no range
no range *start_ipv6_address end_ipv6_address/prefix_len*
no range *pd_prefixname start_ipv6_address end_ipv6_address/prefix_len*

[Parameter]

start_ipv6_address : X:X::X:X

The first IPv6 address amongst all assigned IPv6 addresses

end_IPv6_address : X:X::X:X

The last IPv6 address amongst all assigned IPv6 addresses

The address must have the same subnet prefix as *start_ipv6_address*

prefix_len : <1-128>

Prefix length of assigned IPv6 address

valid : <60-315360000>

Official time enabled (in seconds) for the IPv6 address.

Must be the same as or greater than the *preferred* parameter value

(if omitted, this is 2592000 seconds (30 days))

preferred : <60-315360000>

Recommended (preferred) time enabled (in seconds) for the IPv6 address.

Must be the same as or less than the *valid* parameter value

(if omitted, this is 604800 seconds (7 days))

pd_prefixname : Prefix name set on the DHCPv6-PD client (ipv6 dhcp client pd command)

Up to 32 single-byte alphanumeric characters, including dots, hyphens and underscores

start_pd_IPv6_address : X:X::X:X

The first IPv6 address amongst all assigned IPv6 addresses

Sets the lower level (remaining) portion for the prefix obtained from a DHCPv6-PD client

"0" must be specified for the prefix obtained from DHCPv6-PD client

end_pd_IPv6_address : X:X::X:X

The last IPv6 address amongst all assigned IPv6 addresses

Sets the lower level (remaining) portion for the prefix obtained from a DHCPv6-PD client

"0" must be specified for the prefix obtained from DHCPv6-PD client

The address must have the same subnet prefix as *start_pd_ipv6_address*

[Initial value]

None

[Input mode]

DHCPv6 mode

[Description]

Sets the IPv6 address range to assign for the applicable DHCPv6 pool.

Up to eight ranges can be set for one pool.

This command cannot be set if the **prefix-delegation** command has been set first on the applicable DHCPv6 pool.

You cannot use the **range** command on a DHCPv6 pool to set a command that has a duplicated subnet prefix.

You cannot use the **range** command, **prefix-delegation** command or **link-address** command on a DHCPv6 pool to set a command that has a duplicated subnet prefix.

If this command is executed with the "no" syntax by specifying a parameter, the setting value with the specified parameter will be deleted.

If this command is executed with the "no" syntax without specifying a parameter, all setting values that are set in the applicable DHCPv6 pool are deleted.

[Note]

When both *valid* and *preferred* are equal to the default value, *valid* and *preferred* are not shown when config is shown.

If either *valid* or *preferred* are not equal to the default value, both *valid* and *preferred* are shown in the config.

If the total number of ranges set in all pools and all pool classes for the **range** command (DHCPv6 mode) and the **prefix-delegation** command is greater than 8192, this command results in an error.

For example, if the settings have been configured as shown below, the current range number total is 384 (128 + 256).

```
dhcpv6 pool pool_vlan1
 range 2001:db8:1::dd00 2001:db8:1::dd7f/64
dhcpv6 pool pool_vlan2
 prefix-delegation 2001:db8:2:1000::/56 64
```

When using a syntax that specifies *pd_prefixname* and the prefix information cannot be obtained, the IPv6 address is not generated.

An IPv6 address is also not generated for IPv6 addresses that cannot be used for setting this command.

The *prefix_len* prefix length is a necessary parameter for the DHCPv6 server to distinguishing between *range* IPv6 networks, but the prefix length of *prefix_len* is not used for assigning IPv6 addresses.

When there is no prefix length for an assigned address, the DHCPv6 client determines which prefix length is used.

This command cannot be used if the stack function is enabled.

[Example]

This sets the IPv6 address range of "2001:db8:1::dd00 - 2001:db8:1::dd7f" with a prefix length of 64 for DHCPv6 pool "pool_vlan1".

```
SWX3220(config)#dhcpv6 pool pool_vlan1
SWX3220(config-dhcp6)#range 2001:db8:1::dd00 2001:db8:1::dd7f/64
```

This uses the prefix obtained from a DHCPv6-PD client to set the IPv6 address range for DHCPv6 "pool_vlan1".

In this example, we assume that "2001:db8:1:aa00::/56" is obtained with the prefix name "PD_VLAN2", and that the DHCPv6-PD client is VLAN2.

In this case, the IPv6 address range for the following commands is "2001:db8:1:aa10::dd00 - 2001:db8:1:aa10::dd7f".

```
SWX3220(config)#dhcpv6 pool pool_vlan1
SWX3220(config-dhcp6)#range PD_VLAN2 ::10:0:0:0:dd00 ::10:0:0:0:dd7f/64
```

10.2.5 Set a prefix to dynamically assign to a PD client

[Syntax]

prefix-delegation *ipv6_address*/*prefix_len alloc_prefix_len* [lifetime *valid preferred*] [exclude-local-prefix]
prefix-delegation *pd_prefixname pd_ipv6_address*/*prefix_len alloc_prefix_len* [lifetime *valid preferred*] [exclude-local-prefix]
no prefix-delegation

[Keyword]

exclude-local-prefix	:	Excludes the subnet prefix assigned to the IPv6 global address of a VLAN from an assigned prefix

[Parameter]

ipv6_address	:	X:X::X:X Original IPv6 address to assign to PD client
prefix_len	:	<1-127> Prefix length of original IPv6 address to be assigned to PD client
alloc_prefix_len	:	<3-127> Length of prefix assigned to PD client Must be greater than the *prefix_len* value
valid	:	<60-315360000> Official time enabled (in seconds) for the prefix. Must be the same as or greater than the *preferred* parameter value (if omitted, this is 2592000 seconds (30 days))
preferred	:	<60-315360000> Recommended time enabled (in seconds) for the prefix. Must be the same as or less than the *valid* parameter value (if omitted, this is 604800 seconds (7 days))
pd_prefixname	:	Prefix name set on the DHCPv6-PD client (ipv6 dhcp client pd command) Up to 32 single-byte alphanumeric characters, including dots, hyphens and underscores
pd_IPv6_address	:	X:X::X:X Original IPv6 address to assign to PD client Sets the lower level (remaining) portion for the prefix obtained from a DHCPv6-PD client "0" must be specified for the prefix obtained from DHCPv6-PD client

[Initial value]

None

[Input mode]

DHCPv6 mode

[Description]

Sets a prefix to dynamically assign to a PD client for the applicable DHCPv6 pool.

One command can be set for one pool.

When a new command is set, the previous settings are overwritten.

This specifies an IPv6 address prefix that can be assigned to *ipv6_address*/*prefix_len*.

The prefix is assigned from amongst these with the prefix length specified in *alloc_prefix_len*.

This command cannot be set if the **range** command has been set first on the applicable DHCPv6 pool.

You cannot use the **range** command, **prefix-delegation** command or **link-address** command on a DHCPv6 pool to set a command that has a duplicated subnet prefix.

If this command is executed with the "no" syntax, the setting value is deleted.

[Note]

When both *valid* and *preferred* are equal to the default value, *valid* and *preferred* are not shown when config is shown.

If either *valid* or *preferred* are not equal to the default value, both *valid* and *preferred* are shown in the config.

If the total number of ranges for the **range** command (DHCPv6 mode) and **prefix-delegation** command set for all pools exceeds 8,192, this command results in an error.

For example, if the settings have been configured as shown below, the current range number total is 384 (128 + 256).

```
dhcpv6 pool pool_vlan1
 range 2001:db8:1::dd00 2001:db8:1::dd7f/64
dhcpv6 pool pool_vlan2
 prefix-delegation 2001:db8:2:1000::/56 64
```

When using a syntax that specifies *pd_prefixname* and the prefix information cannot be obtained, the IPv6 address is not generated.

An IPv6 address is also not generated for IPv6 addresses that cannot be used for setting this command.

This command cannot be used if the stack function is enabled.

[Example]

This dynamically assigns the "2001:db8::/48 - 2001:db8:ff::/48" prefix to the DHCPv6 pool "pool_vlan1".

```
SWX3220(config)#dhcpv6 pool pool_vlan1
SWX3220(config-dhcp6)#prefix-delegation 2001:db8::/40 48
```

Uses the prefix obtained from a DHCPv6-PD client to set a prefix that's dynamically assigned to DHCPv6 pool "pool_vlan1".

In this example, we assume that "2001:db8:1:aa00::/56" is obtained with the prefix name "PD_VLAN2", and that the DHCPv6-PD client is VLAN2.

From here, reassignment take places within the /64 range, from the "2001:db8:1:aa10::/60" subnet prefix.

The prefix dynamically assigned with the following commands is "2001:db8:1:aa10::/64 - 2001:db8:1:aa1f::/64".

```
SWX3220(config)#dhcpv6 pool pool_vlan1
SWX3220(config-dhcp6)#prefix-delegation PD_VLAN2 0:0:0:10::/60 64
```

10.2.6 DNS server settings for notification (DHCPv6)

[Syntax]

dns-server *ipv6_address*
dns-server pd *pd_prefixname*
no dns-server *ipv6_address*
no dns-server

[Keyword]

pd	:	Use the DNS server address acquired by the DHCPv6-PD client

[Parameter]

ipv6_address	:	X:X::X:X IPv6 address
pd_prefixname	:	Prefix name set on the DHCPv6-PD client (ipv6 dhcp client pd command) Up to 32 single-byte alphanumeric characters, including dots, hyphens and underscores

[Initial value]

None

[Input mode]

DHCPv6 mode

[Description]

Configures the IP address to notify as a DNS server for the applicable DHCPv6 pool.

Up to eight addresses can be set for *ipv6_address*.

When using the **dns-server** pd *pd_prefixname* syntax, the DNS server acquired from the DHCPv6-PD client is used as the DNS server to notify.

Only one of this syntax can be configured. When this syntax is used, you cannot use the **dns-server** *ipv6_address*, **no dns-server** *ipv6_address* syntax.

When using the **dns-server** *ipv6_address* syntax, you cannot use the **dns-server** pd *pd_prefixname* syntax.

If this command is executed with the "no" syntax by specifying a parameter, the setting value with the specified parameter will be deleted.

If this command is executed with the "no" syntax without specifying a parameter, all setting values that are set in the applicable DHCPv6 pool are deleted.

[Note]

The DHCPv6 option "DNS Recursive Name Server" (option code 23) notified to the client uses this command's value.

When using a syntax that specifies *pd_prefixname* and the prefix information cannot be obtained, the IPv6 address is not generated.

An IPv6 address is also not generated for IPv6 addresses, which cannot be used for setting this command.

This command cannot be used if the stack function is enabled.

[Example]

Sets 2001:db8:1::1 for the DNS server to notify.

```
SWX3220(config-dhcp6)#dns-server 2001:db8:1::1
```

10.2.7 Setting the domain name for resolving names to be notified (DHCPv6)

[Syntax]

domain-name *domain_name*
domain-name pd *pd_prefixname*
no domain-name *domain_name*
no domain-name

[Keyword]

pd	:	Use domain name acquired by the DHCPv6-PD client

[Parameter]

domain_name	:	Domain name Up to 253 single-byte alphanumeric characters, including dots and hyphens
pd_prefixname	:	Prefix name set on the DHCPv6-PD client (ipv6 dhcp client pd command) Up to 32 single-byte alphanumeric characters, including dots, hyphens and underscores

[Initial value]

None

[Input mode]

DHCPv6 mode

[Description]

Sets the domain name to notify for the applicable DHCPv6 pool (the domain name that is used for resolving names).

Up to eight names can be set for *domain_name*.

When using the **domain-name** pd *pd_prefixname* syntax, the domain name acquired from the DHCPv6-PD client is used as the domain name to notify.

Only one of this syntax can be configured. When this syntax is used, you cannot use the **domain-name** *domain_name*, **no domain-name** *domain_name* syntax.

When using the **domain-name** *domain_name* syntax, you cannot use the **domain-name** pd *pd_prefixname* syntax.

If this command is executed with the "no" syntax by specifying a parameter, the setting value with the specified parameter will be deleted.

If this command is executed with the "no" syntax without specifying a parameter, all setting values that are set in the applicable DHCPv6 pool are deleted.

[Note]

The "Domain Search List" DHCPv6 option (option code 24) notified to the client uses the value for this command.

The length of the portion of the domain name separated by a dot (.) (the label) must be at least one character and no more than 63 characters.

If the first character of the domain name is a dot (.), this command produces an error.

When using a syntax that specifies *pd_prefixname* and the prefix information cannot be obtained, the domain name is not generated.

A domain name is also not generated for domain names that cannot be used for setting this command.

This command cannot be used if the stack function is enabled.

[Example]

This sets the domain name to be notified as yamaha.example.com.

```
SWX3220(config-dhcp6)#domain-name yamaha.example.com
```

10.2.8 Set user-defined DHCPv6 option (DHCPv6)

[Syntax]

option *option value*
no option *option*
no option

[Parameter]

option : Option

Setting value	Description
<1-34>	Option number
Mnemonic	Character string recognized as a mnemonic

value : Option value (within 256 characters)

[Initial value]

None

[Input mode]

DHCPv6 mode

[Description]

Sets the user-defined option value for the applicable DHCPv6 pool.

If this command is executed with the "no" syntax by specifying a parameter, the setting value with the specified parameter will be deleted.

If this command is executed with the "no" syntax without specifying a parameter, all setting values that are set in the applicable DHCPv6 pool are deleted.

Below are the following types of option values. The option number determines which value can be used.

For example, text string arrays can be used for 'sip_servers_domain_name_list', and IPv6 address arrays can be used for 'sip_servers_ipv6_address_list'.

4-octet integer	0..4294967295
IPv6 address array	List of IPv6 addresses (maximum of 8), separated by commas
Text string array	List of text strings (maximum of 8; single-byte alphanumeric characters and single-byte symbols, maximum 253 characters), separated by commas

The available options are shown below.

Mnemonics that can be used with option numbers/ commands	Option type
21/sip_servers_domain_name_list	Text string array

Mnemonics that can be used with option numbers/ commands	Option type
22/sip_servers_ipv6_address_list	IPv6 address array
27/nis_servers	IPv6 address array
28/nis+_servers	IPv6 address array
29/nis_domain_name	Text string array
30/nis+_domain_name	Text string array
31/sntp_servers	IPv6 address array
32/information_refresh_time	4-octet integer
33/bcmcs_controller_domain_name_list	Text string array
34/bcmcs_controller_ipv6_address	IPv6 address array

[Note]

The DHCPv6 option notified to the client uses the value for this command.

If the client does not request the relevant option, the relevant option will not actually be transmitted.

When re-registering for option numbers that have already been set, the settings will be overwritten.

For specifying the domain name, the characters that can be used for the option numbers 21, 29, 30 and 33 are the same as for the **domain-name** command.

Although multiple option numbers can be specified for the array format by separating the numbers with commas, the length of the entire option value array cannot be more than 256 characters.

This command cannot be used if the stack function is enabled.

[Example]

This sets "2001:db8:1::1" and "2001:db8:1::2" for the DHCPv6 option "SIP Servers IPv6 Address List" (option code 22).

```
SWX3220(config-dhcp6)#option sip_servers_ipv6_address_list
2001:db8:1::1,2001:db8:1::2
```

10.2.9 Set subnet prefix for identifying the link address field

[Syntax]

link-address *network*
no link-address

[Parameter]

network : X:X::X:X/M

IPv6 address and prefix used for identifying the link address field <1-128>

[Initial value]

None

[Input mode]

DHCPv6 mode

[Description]

Sets the subnet prefix used to identify the link address field for the applicable DHCPv6 pool.

When the subnet prefix for the link address field of this command and of the DHCPv6 relay forwarding message match in comparison to the stateless DHCPv6 message that was relayed by the DHCPv6 relay agent, an option can be distributed from the pool set for this command.

One command can be set for one pool.

When a new command is set, the previous settings are overwritten.

You cannot use the **range** command, **prefix-delegation**command or **link-addres** command on a DHCPv6 pool to set a command that has a duplicated subnet prefix.

If this command is executed with the "no" syntax, the setting value is deleted.

[Note]

You can only set this command when you want to receive stateless DHCPv6 via a relay agent.

When using a stateful DHCPv6 (**range** command) or DHCPv6-PD (**prefix-delegation** command) via a relay agent, this command is unnecessary.

This command cannot be used if the stack function is enabled.

[Example]

Set "2001:db8:2b::/64" as the subnet prefix for identifying the link address field.

```
SWX3220(config-dhcp6)#link-address 2001:db8:2b::/64
```

10.2.10 Show DHCPv6 pool information

[Syntax]

show dhcpv6 pool [*pool_name*]

[Parameter]

pool_name	:	DHCPv6 pool name Pool name shown

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

Shows the DHCPv6 pool information.

Items that have not been set are not shown.

When *pool_name* is specified, only the information for the specified *pool_name* is shown.

The following items are shown.

- DHCPv6 pool name
- Range of IPv6 addresses assigned dynamically, or the prefix dynamically assigned to the PD client
  - The prefix name that is used, if set on a DHCPv6-PD client
- Time enabled
- DNS server
  - The prefix name that is used, if set on a DHCPv6-PD client
- Domain name
  - The prefix name that is used, if set on a DHCPv6-PD client
- Option settings
- link-address

[Note]

This command cannot be used if the stack function is enabled.

[Example]

This shows the DHCPv6 pool information.

```
SWX3220#show dhcpv6 pool
DHCPv6 Pool: p1
  Address Range: 2001:db8:1::dd00 to 2001:db8:1::dd7f/64
       Lifetime: 2592000(valid), 604800(preferred)

DHCPv6 Pool: p2
  PD Prefix  : 2001:db8:2::/56-64
     Lifetime: 2592000(valid), 604800(preferred)
  DNS Server: 2001:db8:1::2
  Domain Name: example.co.jp
  Option Code : 22
         Value: 10::10
  Option Code : 31
         Value: 20::20

DHCPv6 Pool: p3
  DNS Server: 2001:db8:1::2
```

```
  Domain Name: example.co.jp
  Link-Address: 2001:db8:2b::/64

DHCPv6 Pool: p4
  Address Range: 2001:db8:1:af10::dd00 to 2001:db8:1:af10::dd7f/64
       Lifetime: 2592000(valid), 604800(preferred)
        PD Name: RANGE_EXAMPLE
  DNS Server: 2001:db8:1:bb10::100
  DNS Server: 2001:db8:1:bb10::200
     PD Name: DNS_EXAMPLE
  Domain Name: example.co.jp.
      PD Name: DOMAIN_EXAMPLE
```

10.2.11 Displaying IPv6 address assignment information for DHCPv6 clients

[Syntax]

show dhcpv6 binding [pool *pool_name*]
show dhcpv6 binding summary

[Keyword]

summary	:	Shows the number of IPv6 address assignments for each pool

[Parameter]

pool_name	:	Pool name Pool name shown

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

Shows the IPv6 address assignment information for the DHCPv6 client.

If "summary" is not specified, the following items are shown.

When *pool_name* is specified, only the information for the specified *pool_name* is shown.

- DHCPv6 pool name
- Currently assigned IPv6 addresses, or currently assigned prefixes
- Currently assigned client IAID
- Currently assigned client DUID
- Lease finish time

When "summary" is specified , this shows the number of IPv6 address assignments for each pool.

[Note]

Large amounts of lease information may take time to display.

This command cannot be used if the stack function is enabled.

[Example]

This shows the IPv6 address assignment information.

```
SWX3220#show dhcpv6 binding
Pool : pool01
  Address     : 2001:db8:1:aa10::dd40
  client IAID : 0f28924a
  client DUID : 000100010000000000a0de000000
  expires     : 2023/03/01 15:31:10

Pool : pool02
  Prefix      : 2001:db8:8:aa1f::/64
  client IAID : 0bb4b52f
  client DUID : 000100010000000000a0de000000
  expires     : 2023/03/01 15:32:47
```

This shows the number of IPv6 address assignments for each pool.

```
SWX3220#show dhcpv6 binding summary
Pool Name                        Number of Leased Addresses
-------------------------------------------------------------
pool01                           1
```

```
pool02                          1
Total in all Pools:             2
```

10.2.12 Show DHCPv6 server status

[Syntax]

show dhcpv6 server

[Input mode]

unprivileged EXEC mode、privileged EXEC mode

[Description]

Shows the status of the DHCPv6 server.

The following items are shown.

- DHCPv6 server boot status
- The interface on which the DHCPv6 server is running. This is shown when the server is running.
- The DHCPv6 server DUID. Shown when the server is running
- Enable/disable DHCPv6 server function for the entire system
- Interface settings for the DHCPv6 server function
- Pool settings for the DHCPv6 server function

[Note]

This command cannot be used if the stack function is enabled.

[Example]

This shows the current status of the DHCPv6 server.

```
SWX3220#show dhcpv6 server
DHCPv6 server is running
  running interface list : vlan1
  DHCPv6 Server DUID : 000100010000000000a0de000000
DHCPv6 server system setting : enable
DHCPv6 server interface setting list : vlan1
DHCPv6 Pool list : p1
```

10.2.13 Delete DHCPv6 server lease information

[Syntax]

clear dhcpv6-server lease

[Input mode]

privileged EXEC mode

[Description]

Deletes the DHCPv6 server lease information (IPv6 address assignment information).

[Note]

This command cannot be used if the stack function is enabled.

[Example]

This deletes the lease information.

```
SWX3220#clear dhcpv6-server lease
```

10.3 DHCP relay

10.3.1 Set the DHCP relay agent function

[Syntax]

dhcp-relay *switch*
no dhcp-relay

[Parameter]

switch	:	DHCP relay agent operations

Setting value	Description
enable	Enable the DHCP relay agent function
disable	Disable the DHCP relay agent function

[Initial value]

dhcp-relay disable

[Input mode]

global configuration mode

[Description]

Configures the operations of the DHCP relay agent function that affect the entire system.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

To enable the DHCP relay agent function, the DHCP forwarding address for the DHCP relay agent function must be specified on the interface, in addition to this command.

[Example]

Enable the DHCP relay agent function for the entire system.

```
SWX3220(config)#dhcp-relay enable
```

Disable the DHCP relay agent function for the entire system.

```
SWX3220(config)#dhcp-relay disable
```

10.3.2 Configuring the forwarding address for the DHCP relay agent function

[Syntax]

dhcp-relay server-address *server*
no dhcp-relay server-address *server*

[Parameter]

server : A.B.C.D

IPv4 address of forwarding DHCP server

[Initial value]

none

[Input mode]

interface mode

[Description]

Specifies the forwarding address for the DHCP relay agent function on the applicable interface.

This can only be set for VLAN interface.

The DHCP packets received on the configured VLAN interface will be forwarded to the specified IPv4 address.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

For VLAN interface, the IPv4 address must be specified.

For this command, up to 32 for the VLAN interface can be set.

Up to five can be set for one VLAN interface with this command.

[Example]

DHCP packets received by VLAN #1 will be forwarded to 192.168.200.1.

```
SWX3220(config)#interface vlan1
SWX3220(config-if)#dhcp-relay server-address 192.168.200.1
```

10.3.3 Configuring the broadcast forward for the DHCP relay agent function

[Syntax]

dhcp-relay broadcast *switch*
no dhcp-relay broadcast

[Parameter]

switch : Broadcast forward operation

Setting value	Description
enable	Enable broadcast forward
disable	Disable broadcast forward

[Initial value]

dhcp-relay broadcast disable

[Input mode]

global configuration mode

[Description]

Configure the broadcast forward for the DHCP relay agent function.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

In the following cases, DHCP packets will be forwarded to the broadcast address.

- This command is enabled.
- The broadcast address is specified using the **dhcp-relay server-address** command.

[Example]

Enables broadcast forward.

```
SWX3220(config)#dhcp-relay broadcast enable
```

10.3.4 Show status of DHCP relay agent

[Syntax]

show dhcp relay

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the status of the DHCP relay agent.

The following items are shown.

- DHCP relay agent boot status
- The interface on which the DHCP relay agent has been started. Displays when the relay agent has been started
- DHCP relay agent function enable/disable for the entire system
- Broadcast forward settings
- Forwarding address settings

[Example]

```
SWX3220#show dhcp relay
DHCP relay is running
  running interface list : vlan1
DHCP relay system setting : enable
DHCP relay broadcast setting : disable
Server address list :
  vlan1 : 192.168.200.1
```

10.4 DNS relay

10.4.1 Set DNS relay function (system)

[Syntax]

dns-forwarding *switch*
no dns-forwarding

[Parameter]

switch : DNS relay function operation

Setting value	Description
enable	Enable the DNS relay function
disable	Disable the DNS relay function

[Initial value]

dns-forwarding disable

[Input mode]

global configuration mode

[Description]

Configures the operation of the DNS relay function for the entire system.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

To enable the DNS relay function, the forwarding address for the DNS relay function must be specified on the interface, in addition to this command.

[Example]

Enable the DNS relay function for the entire system.

```
SWX3220(config)#dns-forwarding enable
```

Disable the DNS relay function for the entire system.

```
SWX3220(config)#dns-forwarding disable
```

10.4.2 Set DNS relay function (interface)

[Syntax]

dns-forwarding *switch*
no dns-forwarding

[Parameter]

switch : DNS relay function operation

Setting value	Description
enable	Enable the DNS relay function
disable	Disable the DNS relay function

[Initial value]

dns-forwarding disable

[Input mode]

interface mode

[Description]

Specifies the forwarding address for the DNS relay function on the applicable interface.

This can only be set for VLAN interface.

DNS packets received at a VLAN interface for which this is enabled are forwarded to the address specified by the **dns-forwarding name-server** command.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

To enable the DNS relay function, you must enable the DNS relay function for the entire system in addition to using this command.

For VLAN interface, the IPv4 address must be specified.

[Example]

Enable the DNS relay function for VLAN #1.

```
SWX3220(config)#interface vlan1
SWX3220(config-if)#dns-forwarding enable
```

Disable the DNS relay function for VLAN #1.

```
SWX3220(config)#interface vlan1
SWX3220(config-if)#dns-forwarding disable
```

10.4.3 Set DNS relay function forwarding address

[Syntax]

dns-forwarding name-server *server* [*domain_name*]
no dns-forwarding name-server *server* [*domain_name*]

[Parameter]

server	:	A.B.C.D IPv4 address of DNS server
domain_name	:	Domain name Single-byte alphanumeric characters, dot '.', and hyphen '-' (253 characters or less)

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Sets the forwarding address of the DNS relay function.

Up to eight servers can be specified.

If you specify a domain name, queries for that domain name are forwarded only to the specified server.

If this command is executed with the "no" syntax, the specified server is deleted from the forwarding destination addresses of the DNS relay function.

[Note]

The domain name is referenced as the best match for the latter portion.

For example, if rtpro.yamaha.co.jp is specified as 192.168.100.2, and yamaha.co.jp is specified as 192.168.100.3, then rtpro.yamaha.co.jp is forwarded to 192.168.100.2 and network.yamaha.co.jp is forwarded to 192.168.100.3.

The length of the portion of the domain name separated by dots (.) (the label) must be at least one character and no more than 63 characters.

If the first character of the domain name is a dot (.) then this command produces an error.

[Example]

Add 192.168.100.1 as a forwarding address for the DNS relay function.

```
SWX3220(config)#dns-forwarding name-server 192.168.100.1
```

Of the DNS relay function's forwarding destination addresses, make queries to the "swr.example.com" domain be forwarded to 192.168.100.100.

```
SWX3220(config)#dns-forwarding name-server 192.168.100.100 swr.example.com
```

10.4.4 Set maximum TTL for DNS relay function cache entries

[Syntax]

dns-forwarding cache max-ttl *time*
no dns-forwarding cache max-ttl

[Parameter]

time	:	<60-3600>
		seconds

[Initial value]

dns-forwarding cache max-ttl 1800

[Input mode]

global configuration mode

[Description]

Sets the maximum TTL for DNS relay function cache entries.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

If the TTL as notified from the forwarding-destination server exceeds the value specified by this command, the setting value of this command is used as the TTL for cache entries.

[Example]

Set the maximum TTL for DNS relay function cache entries to 3600 seconds.

```
SWX3220(config)#dns-forwarding cache max-ttl 3600
```

10.4.5 Clear DNS relay function cache entries

[Syntax]

clear dns-forwarding cache

[Input mode]

privileged EXEC mode

[Description]

Clears the DNS relay function cache entries.

[Example]

Clear the cache entries.

```
SWX3220#clear dns-forwarding cache
```

10.4.6 Set DNS relay function static record

[Syntax]

dns-forwarding static-host *host address* [*time*]
no dns-forwarding static-host *host address*

[Parameter]

host	:	Host name
		Single-byte alphanumeric characters, dot '.', and hyphen '-' (253 characters or less)
address	:	A.B.C.D
		IPv4 address of host
time	:	<1-2147483647>
		TTL (seconds) for static records (if omitted: 1800)

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Sets the DNS relay function's static records.

When a DNS client requests a host name or address specified by this command, a response is returned using the setting value of this command, without forwarding the packet to the server.

If this command is executed with the "no" syntax, the specified static record is deleted.

[Note]

Up to 16 instances of this command can be set.

If this command is specified, the "A" record and "PTR" record for the specified host name and address are statically maintained.

The length of the portion of the host name separated by dots (.) (the label) must be at least one character and no more than 63 characters.

If the first character of the host name is a dot (.) then this command produces an error.

[Example]

Set the DNS relay function's static records. Specify "swr.example.com" as "192.168.100.100".

```
SWX3220(config)#dns-forwarding static-host swr.example.com 192.168.100.100
```

10.4.7 Show status of DNS relay

[Syntax]

show dns-forwarding

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Shows the status of the DNS relay.

The following items are shown.

- DNS relay boot status
- The interface on which the DNS relay has been started. Displays when the DNS relay has been started
- DNS relay function enable/disable for the entire system
- Forwarding address settings
- Static record settings

[Example]

Shows the DNS relay status.

```
SWX3220#show dns-forwarding
DNS forwarding is running
  running interface list : vlan1
DNS forwarding system setting : enable
DNS forwarding interface setting list : vlan1
Server address list :
  192.168.200.1
  192.168.100.100  swr.example.com
Static host list :
  yamaha.swr.com  192.168.100.200
```

10.4.8 Show cache of DNS relay

[Syntax]

show dns-forwarding cache

[Input mode]

unprivileged EXEC mode, privileged EXEC mode

[Description]

Show the cache of the DNS relay.

The following items are shown.

- Maximum TTL for cache entries
- Number of entries shown
- Record type
- TTL
- Host name
- Record information

[Note]

Up to 1000 cache entries are shown.

If there are more than 1000 cache entries, the most recent 1000 cache entries are shown.

[Example]

Show the cache status for DNS relay.

```
SWX3220#show dns-forwarding cache
DNS forwarding max TTL : 1800
Summary: 3 entry

 TYPE        TTL     HOST (RECORD INFO)
-------------------------------------------------------------------
 A           10      swx01.example.com (192.168.100.100)
 A           103     swx02.example.com (192.168.100.101)
 AAAA        250     swx03.example.com
```

10.5 Local RADIUS server

10.5.1 Local RADIUS server function settings

[Syntax]

radius-server local enable [*port*]
radius-server local disable
no radius-server local

[Parameter]

port : <1024-65535>

UDP port number used for authentication (the default value of 1812 is used when this is omitted)

[Initial value]

radius-server local disable

[Input mode]

global configuration mode

[Description]

Enables/disables the settings for the local RADIUS server function.

You can also change the authentication UDP port number.

If this command is executed with the "no" syntax, the setting returns to the default.

[Note]

To use the local RADIUS server functions, you must first use the **crypto pki generate ca** command to generate a route certificate authority.

[Example]

Enables the local RADIUS server function.

```
SWX3220(config)#radius-server local enable
```

10.5.2 Set access interface

[Syntax]

radius-server local interface *interface*
no radius-server local interface

[Parameter]

interface : VLAN interface name

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Sets the VLAN interface that allows access to the local RADIUS server.

Up to seven access interfaces can be specified.

If the command is executed with the "no" syntax, the specified interface is deleted.

[Example]

Allows access to the RADIUS client (NAS) connected to VLAN #1 and VLAN #100.

```
SWX3220(config)#radius-server local interface vlan1
SWX3220(config)#radius-server local interface vlan100
```

10.5.3 Generate a route certificate authority

[Syntax]

crypto pki generate ca [*ca-name*]
no crypto pki generate ca

[Parameter]

ca-name : Certificate authority name

Characters that can be inputted for the certificate authority name

- Within 3–32 characters
- Single-byte alphanumeric characters and symbols other than the characters \ [ ] " ? and spaces
- Cannot specify “DEFAULT”

[Initial value]

none

[Input mode]

global configuration mode

[Description]

Generates a route certificate authority to issue a client certificate.

“YAMAHA_SWITCH” will be used when the certificate authority is omitted.

If this command is executed with the "no" syntax, the specified route certificate authority is deleted.

[Note]

If a route certificate authority has not been generated, the functions of the local RADIUS server cannot be used.

When setting a different route certificate authority name when a route certificate authority has already been generated, the route certificate authority will be overwritten.

When the route certificate authority is deleted or overwritten, all client certificates already issued will become invalid.

Even if a route certificate authority exists, it cannot be used as such unless the **crypto pki generate ca** settings have not been made.

[Example]

This generates a route certificate authority with the name “MY RADIUS”.

```
SWX3220(config)#crypto pki generate ca MYRADIUS
```

10.5.4 RADIUS configuration mode

[Syntax]

radius-server local-profile

[Input mode]

global configuration mode

[Description]

Switches to the RADIUS configuration mode.

This mode is used to configure the operating specifications for the local RADIUS server function.

[Example]

Switches to the RADIUS configuration mode.

```
SWX3220(config)#radius-server local-profile
SWX3220(config-radius)#
```

10.5.5 Authentication method settings

[Syntax]

authentication *mode* [*mode*...]
no authentication

[Parameter]

mode : Authentication method

Setting value	Description
pap	PAP authentication method
peap	PEAP authentication method
eap-md5	EAP-MD5 authentication method
eap-tls	EAP-TLS authentication method
eap-ttls	EAP-TTLS authentication method

[Initial value]

authentication pap peap eap-md5 eap-tls eap-ttls

[Input mode]

RADIUS configuration mode

[Description]

Specifies the authentication method used for the local RADIUS server.

If this command is executed with the "no" syntax, the setting is returned to its default, and all authentication methods will be enabled.

[Note]

As an internal authentication method for PEAP and EAP-TTLS, this supports MSCHAPv2 and MD5.

The authentication method must be set to “eap-md5” when using MD5.

[Example]

This restricts the authentication method to PEAP and EAP-MD5.

```
SWX3220(config)#radius-server local-profile
SWX3220(config-radius)#authentication peap eap-md5
```

10.5.6 RADIUS client (NAS) settings

[Syntax]

nas *host* key *secret*
no nas *host*

[Keyword]

key : Sets the password used for communicating with the RADIUS client (NAS)

[Parameter]

host : IP address, or IP network address

Setting value	Description
IPv4 address (A.B.C.D)	Range from 0.0.0.1 to 223.255.255.255, except for 127.0.0.1
IPv4 network address (A.B.C.D/M)	The network mask range is from 8 to 32, and the IP address host part will be “0”
IPv6 address (A:B:C::D)	Out of all unicast addresses, the exceptions are unspecified addresses (::/128), default root addresses (::/0) and loopback addresses (::1/128)
IPv6 network address (A:B:C::D/M)	The prefix length is 1–128

secret : Shared password

(128 characters or less, single-byte alphanumeric characters and symbols other than the characters \ [ ] " ? and spaces)

[Initial value]

nas 127.0.0.1 key secret_local

[Input mode]

RADIUS configuration mode

[Description]

Adds a RADIUS client (NAS) to the RADIUS client list.

The maximum number of registered entries is 100.

If this command is executed with the "no" syntax, the specified RADIUS client setting is deleted.

[Note]

RADIUS client (NAS) information configured using this command will not display in running-config or startup-config.

Also, this is different from the regular settings command, in that it will be saved as setting data when this command is executed.

Information for the RADIUS client (NAS) that was set can be checked using the **show radius-server local nas** command.

The following settings must be made when specifying a local RADIUS server using the port authentication function of this device.

```
SWX3220(config)#radius-server host 127.0.0.1 key secret_local
```

[Example]

Add the RADIUS client (NAS) at IP address 192.168.100.101, with a shared password of "abcde”.

```
SWX3220(config)#radius-server local-profile
SWX3220(config-radius)#nas 192.168.100.101 key abcde
```

10.5.7 Authenticated user settings

[Syntax]

user *userid password* [vlan *vlan-id*] [mac *mac-address*] [ssid *ssid*] [name *name*] [mail *mail-address*] [auth *type*] [expire *date*]

no user *userid*

[Keyword]

vlan : Set the VLAN for dynamic VLAN

mac : Specify the terminal’s MAC address when you want to specify an authentication terminal

ssid : Specify the SSID when you want to specify a connected SSID

name : Specify the user name

mail : Set the e-mail addresses to which client certificates will be distributed

auth : Set the authentication method type

expire : Set the term of validity for the client certificate (this is enabled only when the authentication method is EAP-TLS)

[Parameter]

userid : User ID

(within 3–32 characters; cannot specify “DEFAULT”)

Authentication method	Characters that can be inputted
EAP-MD5, EAP-TTLS, PEAP, PAP	Single-byte alphanumeric characters and symbols other than the characters \ [ ] " ? and spaces
EAP-TLS	Single-byte alphanumeric characters and symbols other than the characters \ [ ] " ? and spaces

password : Password

(32 characters or less, single-byte alphanumeric characters and symbols other than the characters \ [ ] " ? and spaces)

vlan-id : <1-4094>

VLAN number for dynamic VLAN

mac-address : hhhh.hhhh.hhhh (h is hexadecimal)

MAC address for terminal (user) to authenticate

ssid : SSID connection point

(32 characters or less, single-byte alphanumeric characters and symbols other than the characters \ [ ] " ? and spaces)

name : User name

(32 characters or less, single-byte alphanumeric characters and symbols other than the characters " ? and spaces

mail-address : Mail address

(256 characters or less, single-byte alphanumeric characters and _ - . @)

type : Type of authentication method

Setting value	Description
pap	PAP authentication method (this type uses the user ID and password)
peap	PEAP, EAP-MD5, EAP-TTLS authentication method (this type uses the user ID and password)
eap-tls	EAP-TLS authentication method (this type uses the user ID and password)

When abbreviating, use “eap-tls”

date : Date (“2037/12/31” is used when omitted)

(YYYY/MM/DD from current date to 2037/12/31)

[Initial value]

none

[Input mode]

RADIUS configuration mode

[Description]

This registers the user to be authenticated with the RADIUS server.

The maximum number of registered entries is 2000.

If this command is executed with the "no" syntax, the specified user is deleted.

When the authentication method is EAP-TLS, client certificates need to be issued by executing the **certificate user** command.

Client certificates must be reissued for users for whom the term of validity has been changed on their password or client certificate.

When deleting a user whose client certificate has already been issued, the client certificate will automatically be processed for revocation.

[Note]

Information configured using this command will not display in running-config or startup-config.

Also, this is different from the regular settings command, in that it will be saved as setting data when this command is executed.

User information that was set can be checked using the **show radius-server local user** command.

MAC addresses specified using the “mac” keyword are used when the RADIUS client (NAS) notifies its Calling-Station-Id.

SSID specified using the “ssid” keyword are used when the RADIUS client (NAS) notifies its Calling-Station-Id.

[Example]

This registers the authenticated user.

```
SWX3220(config)#radius-server local-profile
SWX3220(config-radius)#user yamaha secretpassword mac 00a0.de00.0001 auth peap name
YamahaTaro
```

10.5.8 Reauthentication interval setting

[Syntax]

reauth interval *time*
no reauth interval

[Parameter]

time	:	<3600,43200,86400,604800> Reauthentication interval (no. of seconds)

[Initial value]

reauth interval 3600

[Input mode]

RADIUS configuration mode

[Description]

Sets the reauthentication interval that is notified to the RADIUS client (NAS).

The RADIUS client (NAS) determines whether the reauthentication interval will be used.

If this command is executed with the "no" syntax, the setting returns to the default.

[Example]

This sets the reauthentication interval to 604800 seconds.

```
SWX3220(config)#radius-server local-profile
SWX3220(config-radius)#reauth interval 604800
```

10.5.9 Apply setting data to local RADIUS server

[Syntax]

radius-server local refresh

[Input mode]

privileged EXEC mode

[Description]

This applies the current settings to the local RADIUS server.

If the RADIUS-related settings have been modified, this command must be executed to update the data of the local RADIUS server.

[Note]

When this command is executed, operations will be temporarily halted and restarted afterwards, so that the data can be applied to the local RADIUS server.

[Example]

Applies the current settings to the local RADIUS server.

```
SWX3220#radius-server local refresh
```

10.5.10 Issuing a client certificate

[Syntax]

certificate [mail] **user** [*userid*]

[Keyword]

mail : This issues a client certificate and sends the certificate to the user via e-mail attachment.

[Parameter]

userid : User ID

(within 3–32 characters; cannot specify “DEFAULT”)

Authentication method	Characters that can be inputted
EAP-MD5, EAP-TTLS, PEAP, PAP	Single-byte alphanumeric characters and symbols other than the characters \ [ ] " ? and spaces
EAP-TLS	Single-byte alphanumeric characters and symbols other than the characters \ [ ] / : * | < > " ? and spaces

[Input mode]

privileged EXEC mode

[Description]

This issues client certificates to users for which the EAP-TLS certification method is specified.

If the user ID is omitted, client certificates will be sent for all users who meet the following conditions.

- Users to whom a client certificate has never been issued
- Users whose passwords or client certificate’s term of validity has been changed
- Users whose authentication method has been changed to EAP-TLS

This automatically revokes the client certificates for users whose authentication methods have been changed from EAP-TLS to a method other than EAP-TLS.

When the “mail” keyword is specified, this sends a client certificate to the e-mail address set using the **user** command.

The e-mail subject and body text follow the e-mail settings template (**mail send certificate** command) used when the certificate was sent.

E-mails cannot be sent if an e-mail address has not been set.

[Note]

Up to two client certificates may be issued per user. If two or more client certificates are issued, the older ones will be revoked.

As bulk issuance of client certificates takes time, this is performed in the background, and other commands may be executed while the certificates are being issued.

However, note that the following commands may not be executed due to restrictions.

- crypto pki generate ca
- no crypto pki generate ca
- nas
- user
- certificate user
- certificate mail user
- certificate revoke
- certificate export sd
- copy radius-server local

[Example]

Bulk issuance of client certificates.

```
SWX3220#certificate user
```

10.5.11 Aborting the issue of a client certificate

[Syntax]

certificate abort

[Input mode]

privileged EXEC mode

[Description]

This aborts the bulk issuance of client certificates.

The issuance of client certificates can be restarted by executing the **certificate user** command once more.

[Example]

Aborts the bulk issuance of client certificates.

```
SWX3220#certificate abort
```

10.5.12 Revoking client certificates

[Syntax]

certificate revoke user *userid*
certificate revoke id *certificate-id*

[Keyword]

user	:	Revoking client certificates for specified users
id	:	Revoking client certificates for specified client certificate IDs

[Parameter]

userid : User ID

(within 3–32 characters; cannot specify “DEFAULT”)

Authentication method	Characters that can be inputted
EAP-MD5, EAP-TTLS, PEAP, PAP	Single-byte alphanumeric characters and symbols other than the characters \ [ ] " ? and spaces
EAP-TLS	Single-byte alphanumeric characters and symbols other than the characters \ [ ] / : * | < > " ? and spaces

certificate-id : Client certificate ID

Combination of “user ID” and “serial number”

[Input mode]

privileged EXEC mode

[Description]

This revokes client certificates for specified users or client certificate IDs.

In the event that a client certificate is revoked, the authorization using that certificate will fail.

[Note]

Client certificate IDs (certificate-id) can be checked using the **show radius-server local certificate list** command.

[Example]

This revokes the client certificate for user ID “Taro”.

```
SWX3220#certificate revoke user Taro
```

This revokes the client certificate for client certificate ID “Taro-DF598EE9B44D22CC”.

```
SWX3220#certificate revoke id Taro-DF598EE9B44D22CC
```

10.5.13 Exporting client certificates (copying to SD card)

[Syntax]

certificate export sd all [**compress**]

certificate export sd user *userid* [**compress**]

[Keyword]

all	:	Exporting client certificates for all users
user	:	Exporting client certificates for specified users
compress	:	Compress into a ZIP file

[Parameter]

userid : User ID

(within 3–32 characters; cannot specify “DEFAULT”)

Authentication method	Characters that can be inputted
EAP-MD5, EAP-TTLS, PEAP, PAP	Single-byte alphanumeric characters and symbols other than the characters \ [ ] " ? and spaces
EAP-TLS	Single-byte alphanumeric characters and symbols other than the characters \ [ ] / : * | < > " ? and spaces

[Input mode]

privileged EXEC mode

[Description]

This exports the client certificates to an SD card.

The certificates will be exported to the /swx3220/certification/ folder on the SD card.

If specified using “compress,” the client certificates will be compressed to a ZIP file and then exported.

Export target	Contents
all	Compress all client certificates as “certificate_all.zip”
user	Compress client certificates for specified users as “certificate_<specified ID>.zip”

[Note]

Only the newest client certificate (1) can be exported.

[Example]

This exports the client certificate for the user ID “Yamaha” to an SD card.

```
SWX3220#certificate export sd user Yamaha
```

10.5.14 Exporting of client certificates (sending via e-mail)

[Syntax]

certificate export mail all compress
certificate export mail user *userid* **compress**

[Keyword]

all	:	Send client certificates for all users via e-mail
user	:	Send client certificates for specified users via e-mail
compress	:	Compress into a ZIP file

[Parameter]

userid : User ID

(within 3–32 characters; cannot specify “DEFAULT”)

Authentication method	Characters that can be inputted:
EAP-MD5, EAP-TTLS, PEAP, PAP	Single-byte alphanumeric characters and symbols other than the characters \ [ ] " ? and spaces
EAP-TLS	Single-byte alphanumeric characters and symbols other than the characters \ [ ] / : * | < > " ? and spaces

[Input mode]

privileged EXEC mode

[Description]

Sends client certificates to each user via e-mail attachment.

Client certificates to be sent are ZIP files, compressed using the passwords for each user.

E-mail cannot be sent to users whose e-mail addresses have not been set.

To send e-mail, the e-mail destination server and e-mail recipient name must be configured in the e-mail template, and an e-mail template ID for use when sending the e-mail must be set using the **mail send certificate** command.

[Note]

Only the newest client certificate (1) can be sent via e-mail.

[Example]

This sends a client certificate via e-mail to the user with the “Yamaha” user ID.

```
SWX3220#certificate export mail user Yamaha
```

10.5.15 Copying RADIUS data

[Syntax]

copy radius-server local *src_config_num dst_config_num*

[Parameter]

src_config_num : Copy source configuration number

Setting value	Description
<0-1>	Configuration #0-#1
sd	Configuration on the SD card

dst_config_num : Copy destination configuration number

Setting value	Description
<0-1>	Configuration #0-#1
sd	Configuration on the SD card

[Input mode]

privileged EXEC mode

[Description]

This copies the entire set of data in connection with the local RADIUS server.

- Route certificate authority
- Client certificates issued
- User data
- Management file

When you need to copy all settings including the command settings, you can use the **copy startup-config** command to copy.

[Note]

If an SD card that is not mounted is specified, an error will occur.

[Example]

This copies the config #0 RADIUS data to the SD card.

```
SWX3220#copy radius-server local 0 sd
Succeeded to copy Radius configuration
```

10.5.16 Show RADIUS client (NAS) status

[Syntax]

show radius-server local nas *host*

[Parameter]

host : IP address or IP network address

Setting value	Description
IPv4 address (A.B.C.D)	Range from 0.0.0.1 to 223.255.255.255, except for 127.0.0.1
IPv4 network address (A.B.C.D/M)	The network mask range is from 8 to 32, and the IP address host part will be “0”
IPv6 address (A:B:C::D)	Out of all unicast addresses, the exceptions are unspecified addresses (::/128), default root addresses (::/0) and loopback addresses (::1/128)
IPv6 network address (A:B:C::D/M)	The prefix length is 1–128

[Input mode]

privileged EXEC mode

[Description]

Shows a list of RADIUS clients (NAS).

[Example]

Shows the RADIUS clients (NAS) with an IP address of “192.168.100.0/24”.

```
SWX3220#show radius-server local nas 192.168.100.0/24
host                                    key
-------------------------------------------------------------------------------
-------------------
192.168.100.0/24                        abcde
```

10.5.17 Show authenticated user information

[Syntax]

show radius-server local user [detail *userid*]

[Keyword]

detail : Show detailed information for the specified user

[Parameter]

userid : User ID

(within 3–32 characters; cannot specify “DEFAULT”)

Authentication method	Characters that can be inputted
EAP-MD5, EAP-TTLS, PEAP, PAP	Single-byte alphanumeric characters and symbols other than the characters \ [ ] " ? and spaces
EAP-TLS	Single-byte alphanumeric characters and symbols other than the characters \ [ ] / : * | < > " ? and spaces

[Input mode]

privileged EXEC mode

[Description]

This shows the user information.

[Example]

Shows the user information list.

```
SWX3220#show radius-server local user
Total     1

userid                           name                             vlan mode
-------------------------------------------------------------------------------
00a0de001080                     YamahaTaro                          1 eap-md5
```

Shows user information for user ID “00a0de000001”.

```
SWX3220#show radius-server local user detail 00a0de000001
Total     1

userid      : 00a0de000001
password    : secretpassword
mode        : eap-tls
vlan        : 10
MAC         : 00a0.de00.0001
SSID        :
name        : YamahaTaro
mail-address: test.com
expire date : 2037/12/31
certificated: Not
```

10.5.18 Client certificate issuance status display

[Syntax]

show radius-server local certificate status

[Input mode]

privileged EXEC mode

[Description]

Shows the issuance status for client certificates.

Issuance status	Contents
done	Client certificate issuance completed, or not issued
processing	Now issuing client certificate
aborted	Issuance of client certificate aborted by executing “certificate abort” or other command

[Example]

Shows the issuance status for client certificates.

```
SWX3220#show radius-server local certificate status
certificate process: done.
```

10.5.19 Client certificate list display

[Syntax]

show radius-server local certificate list [**detail** *userid*]

[Keyword]

detail : Output the list of details

[Parameter]

userid : User ID

(within 3–32 characters; cannot specify “DEFAULT”)

Authentication method	Characters that can be inputted
EAP-MD5, EAP-TTLS, PEAP, PAP	Single-byte alphanumeric characters and symbols other than the characters \ [ ] " ? and spaces
EAP-TLS	Single-byte alphanumeric characters and symbols other than the characters \ [ ] / : * | < > " ? and spaces

[Input mode]

privileged EXEC mode

[Description]

This shows the list of client certificates that have been issued.

Specifying *userid* will show detailed information for that user.

[Example]

This displays client certificates that have been issued for specific users.

```
SWX3220#show radius-server local certificate list detail Yamaha

userid                          certificate number
enddate
------------------------------------------------------------------------------------
--------
Yamaha                          Yamaha-DF598EE9B44D22CC
2018/12/31
                                Yamaha-DF598EE9B44D22CD
2019/12/31
```

10.5.20 Revoked client certificate list display

[Syntax]

show radius-server local certificate revoke

[Input mode]

privileged EXEC mode

[Description]

This shows a list of client certificates that have been processed for revocation.

Reason for revocation	Contents
revoked	Manual revocation
expired	Revocation due to expired term of validity

[Example]

Displays the list of revoked client certificates.

```
SWX3220#show radius-server local certificate revoke

userid                          certificate number
reason
------------------------------------------------------------------------------------
--------
Yamaha                          Yamaha-DF598EE9B44D22CC
expired
                                Yamaha-DF598EE9B44D22CD
revoked
```

Index

A

aaa authentication auth-mac 215
aaa authentication auth-web 215
aaa authentication dot1x 214
accept-lifetime 453
access-group (IPv4) 531
access-group (IPv6) 533
access-group (MAC) 536
access-list (IPv4) 529
access-list (IPv6) 532
access-list (MAC) 534
access-list description (IPv4) 531
access-list description (IPv6) 533
access-list description (MAC) 535
action 169
address-family ipv6 322
advertisement-interval 459
agent-watch down-count 149
agent-watch interval 148
aggregate-address (BGP IPv4) 360
aggregate-address (BGP IPv6) 361
aggregate-police 561
area authentication 396
area default-cost (OSPFv2) 397
area default-cost (OSPFv3) 412
area filter-list 397
area nssa (OSPFv2) 398
area nssa (OSPFv3) 413
area range (OSPFv2) 399
area range (OSPFv3) 414
area stub (OSPFv2) 400
area stub (OSPFv3) 415
area virtual-link (OSPFv2) 401
area virtual-link (OSPFv3) 416
arp 293
arp-ageing-timeout 293
arp-ageing-timeout request 294
auth clear-state time (global configuration mode) 232
auth clear-state time (interface mode) 233
auth dynamic-vlan-creation 221
auth guest-vlan 222
auth host-mode 220
auth no-response-authorized 228
auth order 220
auth radius attribute nas-identifier 227
auth reauthentication 221
auth timeout quiet-period 222
auth timeout reauth-period 223
auth timeout server-timeout 223
auth timeout supp-timeout 224
auth-mac auth-user 218
auth-mac enable 217
auth-mac static 218
auth-web enable 219
auth-web redirect-url 231
authentication 616
auto-cost reference-bandwidth (OSPFv2) 402
auto-cost reference-bandwidth (OSPFv3) 416
auto-ip 289
auto-summary 361

B

backup system 183
banner motd 42
baudrate select 82
beep buzzer 173
bgp aggregate-nexthop-check 365
bgp always-compare-med 357
bgp bestpath as-path ignore 357
bgp bestpath compare-confed-aspath 358
bgp bestpath compare-originator-id 358
bgp bestpath compare-routerid 358
bgp bestpath med 359
bgp bestpath med remove-recv-med 359
bgp bestpath med remove-send-med 359
bgp client-to-client reflection (BGP IPv4) 366
bgp client-to-client reflection (BGP IPv6) 366
bgp cluster-id 367
bgp confederation identifier 367
bgp confederation peers 368
bgp default ipv4-unicast 323
bgp default local-preference 356
bgp deterministic-med 360
bgp enforce-first-as 356
bgp fast-external-failover 324
bgp log 394
bgp log-neighbor-changes 324
bgp nexthop-trigger 365
bgp nexthop-trigger delay 366
bgp router-id 323
bgp scan-time 325
bind host 580
boot auto-apply 49
boot prioritize sd 49
bootfile 584
buzzer 171
buzzer trigger 172

C

cable-diagnostics tdr execute interface 60
capability opaque 403
certificate abort 621
certificate export mail 622
certificate export sd 621
certificate revoke 621
certificate user 620
channel-group mode 205
circuit-failover 460
circuit-id 589
class 548
class-map 547
clear access-list counters 537
clear arp-cache 293
clear auth state 232
clear auth statistics 231
clear boot list 48
clear cable-diagnostics tdr 60
clear counters 200
clear dhcp-server lease 596
clear dhcpv6-server lease 607
clear dns-forwarding cache 612
clear ip bgp 392
clear ip dhcp snooping binding 284
clear ip dhcp snooping statistics 285
clear ip igmp 528
clear ip igmp snooping 491
clear ip mroute 478
clear ip ospf 430
clear ip pim sparse-mode 517
clear ip prefix-list 393
clear ip rip route 455
clear ip rip statistics 456
clear ip route 292

clear ipv6 bgp 392
clear ipv6 dhcp client 305
clear ipv6 mld snooping 497
clear ipv6 neighbors 310
clear ipv6 ospf 435
clear ipv6 prefix-list 394
clear ipv6 rip route 456
clear ipv6 route 309
clear lacp counters 210
clear lldp counters 146
clear logging 87
clear mac-address-table dynamic 240
clear qos metering-counters 566
clear spanning-tree detected protocols 265
clear ssh host 126
clear ssh-server host key 123
clear system-diagnostics on-demand 59
clear test cable-diagnostics tdr 60
cli-command 170
clock set 61
clock summer-time date 63
clock summer-time recurring 63
clock timezone 61
cold start 180
compatible rfc1583 403
config-auto-set enable 156
copy auth-web custom-file 233
copy radius-server local 623
copy running-config startup-config 43
copy startup-config 46
copy tech-support sd 56
crypto pki generate ca 615

D

db-summary-opt (OSPFv2) 403
db-summary-opt (OSPFv3) 417
default-information originate (OSPFv2) 404
default-information originate (OSPFv3) 417
default-information originate (RIP) 442
default-metric (OSPFv2) 404
default-metric (OSPFv3) 418
default-metric (RIP) 443
default-router (DHCP mode) 583
default-router (DHCP pool class mode) 592
description 186
description (route-map) 466
description (schedule) 169
dhcp class 588
dhcp pool 578
dhcp pool class 590
dhcp-relay 607
dhcp-relay broadcast 609
dhcp-relay server-address 608
dhcp-server (global configuration mode) 577
dhcp-server (interface mode) 577
dhcpv6 pool 597
dhcpv6-server (global configuration mode) 596
dhcpv6-server (interface mode) 597
distance (BGP IPv4) 325
distance (BGP IPv6) 326
distance (OSPFv2) 405
distance (OSPFv3) 418
distance (RIP) 443
distribute-list (OSPFv2) 405
distribute-list (OSPFv3) 419
distribute-list (RIP) 443
dns-client 319
dns-client domain-list 320
dns-client domain-name 320
dns-client name-server 319
dns-forwarding (global configuration mode) 610
dns-forwarding (interface mode) 610
dns-forwarding cache max-ttl 612
dns-forwarding name-server 611
dns-forwarding static-host 612
dns-server (DHCP mode) 583
dns-server (DHCP pool class mode) 593
dns-server (DHCPv6 mode) 601
domain-name (DHCP mode) 584
domain-name (DHCP pool class mode) 593
domain-name (DHCPv6 mode) 602
dot1x control-direction 216
dot1x max-auth-req 217
dot1x port-control 215

E

eee 191
enable password 38
erase auth-web custom-file 234
erase startup-config 46
errdisable auto-recovery 237
event-watch disable 155
event-watch interval 156
exec-timeout 80
exit-address-family 322

F

fec 188
find switch start 182
find switch stop 183
firmware-update execute 160
firmware-update http-proxy 159
firmware-update reload-method 163
firmware-update reload-time 162
firmware-update revision-down enable 161
firmware-update sd execute 162
firmware-update timeout 160
firmware-update url 158
flowcontrol (global configuration mode) 573
flowcontrol (interface mode) 574

H

host 406
host (OSPFv3) 419
hostname 179
http-proxy 119
http-proxy timeout 119
http-server 115
http-server access 117
http-server interface 116
http-server language 118
http-server login-timeout 118
http-server secure 115

I

instance 266
instance priority 267
instance vlan 266
interface reset 198
ip address 286
ip address dhcp 287
ip as-path access-list 326
ip community-list 327
ip dhcp snooping (global configuration mode) 276
ip dhcp snooping (interface mode) 277
ip dhcp snooping information option 279
ip dhcp snooping information option allow-untrusted 280
ip dhcp snooping information option format remote-id 280

ip dhcp snooping information option format-type circuit-id 280
ip dhcp snooping limit rate 282
ip dhcp snooping logging 282
ip dhcp snooping subscriber-id 281
ip dhcp snooping trust 278
ip dhcp snooping verify mac-address 278
ip directed-broadcast 295
ip forwarding (global configuration mode) 294
ip forwarding (interface mode) 295
ip igmp 517
ip igmp access-group 522
ip igmp check source-address 521
ip igmp immediate-leave 521
ip igmp last-member-query-count 519
ip igmp last-member-query-interval 519
ip igmp limit 522
ip igmp mroute-proxy 525
ip igmp proxy-service 525
ip igmp querier-timeout 520
ip igmp query-interval 518
ip igmp query-max-response-time 518
ip igmp robustness-variable 520
ip igmp snooping 482
ip igmp snooping check ra 485
ip igmp snooping check tos 486
ip igmp snooping check ttl 485
ip igmp snooping fast-leave 482
ip igmp snooping mrouter interface 483
ip igmp snooping mrouter-port data-suppression 489
ip igmp snooping querier 484
ip igmp snooping query-interval 484
ip igmp snooping report-forward 488
ip igmp snooping report-suppression 487
ip igmp snooping version 486
ip igmp ssm-map 523
ip igmp ssm-map static 524
ip igmp static-group 523
ip igmp version 517
ip mroute 475
ip multicast route-limit 475
ip multicast-routing 474
ip ospf authentication 422
ip ospf authentication-key 423
ip ospf cost 423
ip ospf database-filter 423
ip ospf dead-interval 424
ip ospf disable all 424
ip ospf hello-interval 424
ip ospf message-digest-key 425
ip ospf network (ospfv2) 425
ip ospf priority 426
ip ospf retransmit-interval 426
ip ospf transmit-delay 426
ip pim 498
ip pim accept-register 504
ip pim bsr-border 503
ip pim bsr-candidate 503
ip pim crp-fixed-prefix 502
ip pim dr-priority 500
ip pim exclude-genid 500
ip pim graft-retransmit 509
ip pim hello-holdtime 499
ip pim hello-interval 498
ip pim ignore-rp-set-priority 503
ip pim jp-timer 506
ip pim neighbor-filter 499
ip pim propagation-delay 509
ip pim register-checksum 505
ip pim register-rate-limit 505
ip pim register-rp-reachability 510
ip pim register-source 504
ip pim register-suppression 506
ip pim rp-address 501
ip pim rp-candidate 501
ip pim rp-register-kat 507
ip pim spt-disable 507
ip pim ssm 508
ip pim state-refresh origination-interval 508
ip pim unicast-bsm 510
ip policy route-map 470
ip rip authentication key-chain 447
ip rip authentication mode 447
ip rip authentication string 448
ip rip metric-zero-accept 448
ip rip poison-reverse 450
ip rip receive version 449
ip rip receive-packet 448
ip rip send version 449
ip rip send-packet 449
ip rip split-horizon 450
ip route 289
ip-prefix-list 328
ipv6 298
ipv6 address 299
ipv6 address autoconfig 299
ipv6 address dhcp 300
ipv6 address pd 301
ipv6 dhcp client nd-prefix 306
ipv6 dhcp client pd 302
ipv6 forwarding 317
ipv6 mld snooping 491
ipv6 mld snooping fast-leave 492
ipv6 mld snooping mrouter interface 493
ipv6 mld snooping querier 493
ipv6 mld snooping query-interval 494
ipv6 mld snooping report-suppression 495
ipv6 mld snooping version 494
ipv6 nd accept-ra-default-routes 303
ipv6 nd current-hoplimit 313
ipv6 nd link-mtu 316
ipv6 nd managed-config-flag 313
ipv6 nd minimum-ra-interval 312
ipv6 nd other-config-flag 314
ipv6 nd prefix 311
ipv6 nd ra-interval 312
ipv6 nd ra-lifetime 314
ipv6 nd reachable-time 315
ipv6 nd retransmission-time 315
ipv6 nd send-ra 310
ipv6 neighbor 309
ipv6 ospf cost 427
ipv6 ospf dead-interval 427
ipv6 ospf hello-interval 427
ipv6 ospf network (ospfv3) 428
ipv6 ospf priority 428
ipv6 ospf retransmit-interval 429
ipv6 ospf transmit-delay 430
ipv6 policy route-map 470
ipv6 rip metric-offset 451
ipv6 rip poison-reverse 451
ipv6 rip split-horizon 451
ipv6 route 306
ipv6 router ospf area 429
ipv6 router rip 452
ipv6-prefix-list 328

K

key 452
key chain 452
key-string 453

L

l2-mcast flood 481
l2-mcast snooping tcn-query 481
l2-unknown-mcast (global configuration mode) 479
l2-unknown-mcast (interface mode) 479
l2-unknown-mcast forward link-local 480
l2ms configuration 147
l2ms enable 147
l2ms filter enable 150
l2ms reset 151
l2ms role 147
lacp multi-speed 209
lacp port-priority 214
lacp system-priority 208
lacp timeout 209
lease (DHCP mode) 581
lease (DHCP pool class mode) 591
led-mode default 181
line con 79
line vty 80
link-address 604
lldp auto-setting 135
lldp interface enable 142
lldp run 133
lldp system-description 134
lldp system-name 134
lldp-agent 135
logging backup sd 87
logging event 86
logging facility 84
logging format 83
logging host 83
logging stdout info 85
logging trap debug 84
logging trap error 85
logging trap informational 85
loop-detect (global configuration mode) 272
loop-detect (interface mode) 273
loop-detect blocking 274
loop-detect blocking interval 275
loop-detect reset 275

M

mac-address-table ageing-time 239
mac-address-table learning 239
mac-address-table static 240
mail certificate expire-notify 132
mail notify trigger 128
mail send certificate 131
mail send certificate-notify 132
mail server smtp host 126
mail server smtp name 127
mail template 129
management interface 82
match access-list (QoS) 549
match access-list (VLAN) 538
match access-list @acl-id 467
match acess-list (BGP IPv4) 369
match acess-list (BGP IPv6) 370
match as-path 368
match community 368
match cos 549
match ethertype 551
match ip next-hop 369
match ip-dscp 550
match ip-precedence 550
match ipv6 next-hop 370
match metric 371
match origin 371
match vlan 551
match vlan-range 552
max-concurrent-dd (OSPFv2) 407
max-concurrent-dd (OSPFv3) 420
maximum-paths 290
mdix auto 191
mirror interface 193
mount sd 180
mru 190
mtu 296
multicast 474
multiple-vlan group name 253
multiple-vlan transfer ympi 254
mute buzzer 173

N

nas 616
negotiation 188
neighbor (RIP) 444
neighbor activate (BGP IPv4) 330
neighbor activate (BGP IPv6) 330
neighbor advertisement-interval 331
neighbor allowas-in (BGP IPv4) 331
neighbor allowas-in (BGP IPv6) 332
neighbor as-origination-interval 332
neighbor attribute-unchanged (BGP IPv4) 333
neighbor attribute-unchanged (BGP IPv6) 334
neighbor capability orf prefix-list (BGP IPv4) 334
neighbor capability orf prefix-list (BGP IPv6) 335
neighbor capability route-refresh 335
neighbor capability-negotiate 339
neighbor default-originate (BGP IPv4) 336
neighbor default-originate (BGP IPv6) 336
neighbor description 337
neighbor disallow-infinite-holdtime 337
neighbor distribute-list (BGP IPv4) 338
neighbor distribute-list (BGP IPv6) 338
neighbor ebgp-multihop 340
neighbor filter-list (BGP IPv4) 340
neighbor filter-list (BGP IPv6) 341
neighbor interface 341
neighbor maximum-prefix (BGP IPv4) 342
neighbor maximum-prefix (BGP IPv6) 342
neighbor next-hop-self (BGP IPv4) 343
neighbor next-hop-self (BGP IPv6) 343
neighbor override-capability 344
neighbor passive 345
neighbor password 345
neighbor peer-group 345
neighbor peer-group (BGP IPv4) 346
neighbor peer-group (BGP IPv6) 346
neighbor prefix-list (BGP IPv4) 347
neighbor prefix-list (BGP IPv6) 347
neighbor remote-as 348
neighbor remove-private-as (BGP IPv4) 348
neighbor remove-private-as (BGP IPv6) 349
neighbor route-map (BGP IPv4) 349
neighbor route-map (BGP IPv6) 350
neighbor route-reflector-client (BGP IPv4) 351
neighbor route-reflector-client (BGP IPv6) 351
neighbor send-community (BGP IPv4) 352
neighbor send-community (BGP IPv6) 352
neighbor shutdown 353
neighbor soft-reconfiguration inbound (BGP IPv4) 353
neighbor soft-reconfiguration inbound (BGP IPv6) 354
neighbor timers 354
neighbor weight (BGP IPv4) 355
neighbor weight (BGP IPv6) 356
network (BGP IPv4) 362
network (BGP IPv6) 362
network (RIP) 444
network synchronization (BGP IPv4) 363

network synchronization (BGP IPv6) 363
network(DHCP) 579
network(OSPF) 407
next-server 585
ntpdate interval 66
ntpdate oneshot 66
ntpdate server 65

O

offset-list 445
option (DHCP mode) 585
option (DHCPv6 mode) 603
ospf router-id 408
overflow database 408
overflow database external 409

P

pass-through eap 235
passive-interface (OSPFv2) 409
passive-interface (OSPFv3) 420
passive-interface (RIP) 445
password-encryption 38
pbr enable 471
ping 297
ping6 317
police single-rate (aggregate policer mode) 561
police single-rate (policy map class mode) 557
police twin-rate (aggregate policer mode) 562
police twin-rate (policy map class mode) 558
police-aggregate 565
policy-map 553
port-channel load-balance 211
port-security enable 235
port-security mac-address 236
port-security violation 236
preempt-mode 461
prefix-delegation 600
priority 461
private-vlan 243
private-vlan association 244
proav profile-type 184
probe 582
probe timeout 582
ptp (global configuration mode) 67
ptp (interface mode) 67
ptp announce interval 71
ptp announce timeout-interval 72
ptp delay-req interval 73
ptp domain 70
ptp mode 68
ptp priority1 70
ptp priority2 71
ptp sync interval 72
ptp transport protocol 69
ptp vlan 74

Q

qos cos 541
qos cos-queue 545
qos dscp-queue 546
qos enable 540
qos port-priority-queue 546
qos queue sent-from-cpu 547
qos trust 541
qos wrr-weight 571

R

radius-server deadtime 227
radius-server host 225
radius-server key 227
radius-server local enable 614
radius-server local interface 614
radius-server local refresh 619
radius-server local-profile 615
radius-server retransmit 226
radius-server timeout 226
range (DHCP mode) 580
range (DHCP pool class mode) 590
range (DHCPv6 mode) 598
reauth interval 619
redistribute (BGP IPv4) 363
redistribute (BGP IPv6) 364
redistribute (OSPFv2) 410
redistribute (OSPFv3) 420
redistribute (RIP) 446
region 267
reload 179
remark-map (aggregate policer mode) 563
remark-map (policy map class mode) 559
remote-id 588
remote-login 166
restart 179
restore system 184
revision 268
rmon 98
rmon alarm 101
rmon clear counters 105
rmon event 100
rmon history 99
rmon statistics 98
route-map 466
router bgp 322
router ipv6 ospf 395
router ipv6 rip 442
router ipv6 vrrp 458
router ospf 395
router rip 442
router vrrp 458
router-id (OSPFv3) 421

S

save 43
save logging 86
schedule 167
schedule template 169
script 171
send from 129
send notify wait-time 131
send server 129
send subject 130
send to 130
send-lifetime 454
server-type 578
service terminal-length 81
service-policy 554
set aggregator as 372
set as-path prepend 372
set atomic-aggregate 373
set comm-list delete 373
set community 373
set cos 555
set cos-queue 567
set interface null 469
set ip next-hop (BGP) 374
set ip next-hop (PBR) 468
set ip-dscp 556

set ip-dscp-queue 568
set ip-precedence 555
set ipv6 next-hop (BGP) 375
set ipv6 next-hop (PBR) 468
set lldp 136
set local-preference 375
set management-address-tlv 136
set metric 375
set msg-tx-hold 140
set origin 376
set originator-id 376
set timer msg-fast-tx 139
set timer msg-tx-interval 139
set timer reinit-delay 140
set too-many-neighbors limit 141
set tx-fast-init 141
set weight 377
sflow 106
sflow agent 106
sflow collector 107
sflow collector max-datagram-size 107
sflow max-header-size 108
sflow polling-interval 108
sflow sampling-rate 108
sfp-monitor rx-power 202
show access-group 537
show access-list 537
show aggregate-police 565
show arp 292
show auth statistics 230
show auth status 228
show auth supplicant 230
show bgp nexthop-tracking 377
show bgp nexthop-tree-detailed 377
show boot 48
show boot prioritize sd 50
show buzzer 174
show cable-diagnostics tdr 60
show class-map 552
show clock 64
show config(show running-config) 44
show config(show startup-config) 45
show ddm status 201
show dhcp binding 595
show dhcp lease 288
show dhcp pool 594
show dhcp relay 609
show dhcp server 595
show dhcpv6 binding 606
show dhcpv6 pool 605
show dhcpv6 server 607
show dipsw 182
show disk-usage 52
show dns-client 321
show dns-forwarding 613
show dns-forwarding cache 613
show eee capabilities interface 192
show eee status interface 192
show environment 50
show errdisable 238
show error port-led 181
show etherchannel 206
show etherchannel status 212
show fan history 57
show firmware-update 161
show flowcontrol 575
show frame-counter 199
show http-proxy 119
show http-server 116
show interface 194
show interface brief 197
show interface negotiation 189
show inventory 50
show ip as-path-access-list 378
show ip bgp 379
show ip bgp community 380
show ip bgp community-list 381
show ip bgp filter-list 381
show ip bgp inconsistent-as 382
show ip bgp neighbors 383
show ip bgp neighbors advertised-routes 384
show ip bgp neighbors hold-time 385
show ip bgp neighbors keepalive 386
show ip bgp neighbors keepalive-interval 386
show ip bgp neighbors notification 386
show ip bgp neighbors open 387
show ip bgp neighbors rcvd-msgs 387
show ip bgp neighbors received prefix-filter 387
show ip bgp neighbors received-routes 388
show ip bgp neighbors routes 389
show ip bgp neighbors sent-msgs 390
show ip bgp neighbors update 390
show ip bgp scan 390
show ip bgp summary 391
show ip dhcp snooping 283
show ip dhcp snooping binding 284
show ip dhcp snooping interface 283
show ip dhcp snooping statistics 284
show ip forwarding 295
show ip igmp groups 526
show ip igmp interface 526
show ip igmp proxy 527
show ip igmp snooping groups 490
show ip igmp snooping interface 490
show ip igmp snooping mrouter 489
show ip igmp ssm-map 527
show ip interface 287
show ip mroute 476
show ip mvif 477
show ip ospf 430
show ip ospf border-routers 431
show ip ospf database 431
show ip ospf database asbr-summary 431
show ip ospf database external 432
show ip ospf database network 432
show ip ospf database nssa-external 433
show ip ospf database router 433
show ip ospf database summary 433
show ip ospf interface 434
show ip ospf neighbor 434
show ip ospf route 435
show ip ospf virtual-links [brief] 435
show ip pim bsr-router 516
show ip pim interface 510
show ip pim mroute 512
show ip pim neighbor 514
show ip pim nexthop 514
show ip pim rp mapping 515
show ip pim rp-hash 516
show ip prefix-list 378
show ip protocols ospf 435
show ip protocols rip 456
show ip rip 457
show ip rip interface 457
show ip rip statistics 458
show ip route 290
show ip route database 291
show ip route pbr 472
show ip route summary 291
show ip rpf 478
show ipv6 bgp 379
show ipv6 bgp community 380
show ipv6 bgp community-list 381
show ipv6 bgp filter-list 382

show ipv6 bgp inconsistent-as 382
show ipv6 bgp neighbors 383
show ipv6 bgp neighbors advertised-routes 385
show ipv6 bgp neighbors received-routes 388
show ipv6 bgp neighbors routes 389
show ipv6 bgp summary 391
show ipv6 dhcp interface 304
show ipv6 forwarding 317
show ipv6 interface 304
show ipv6 mld snooping groups 496
show ipv6 mld snooping interface 496
show ipv6 mld snooping mrouter 495
show ipv6 nd ra 316
show ipv6 neighbors 310
show ipv6 ospf 436
show ipv6 ospf border-routers 436
show ipv6 ospf database 436
show ipv6 ospf database external 437
show ipv6 ospf database inter-prefix 437
show ipv6 ospf database inter-router 438
show ipv6 ospf database intra-prefix 438
show ipv6 ospf database link 439
show ipv6 ospf database network 439
show ipv6 ospf database router 440
show ipv6 ospf interface 440
show ipv6 ospf neighbor 441
show ipv6 ospf route 441
show ipv6 ospf virtual-links 441
show ipv6 prefix-list 378
show ipv6 protocols ospf 442
show ipv6 protocols rip 456
show ipv6 rip 457
show ipv6 rip interface 457
show ipv6 route 307
show ipv6 route database 308
show ipv6 route pbr 473
show ipv6 route summary 308
show l2ms 151
show l2ms agent-config 153
show lacp sys-id 208
show lacp-counter 210
show led-mode 181
show lldp interface 142
show lldp neighbors 145
show logging 87
show loop-detect 275
show mac-address-table 241
show mac-address-table count 242
show mail information 133
show memory 52
show mirror 194
show ntpdate 66
show policy-map 568
show port-security status 236
show power-supply 57
show process 52
show ptp 75
show ptp data 76
show ptp interface 75
show ptp port-data 77
show ptp statistics 78
show qos 543
show qos interface 543
show qos map-status 570
show qos metering-counters 566
show qos queue-counters 544
show radius-server 231
show radius-server local certificate list 625
show radius-server local certificate revoke 626
show radius-server local certificate status 625
show radius-server local nas 624
show radius-server local user 624
show rmon 103
show rmon alarm 105
show rmon event 104
show rmon history 104
show rmon statistics 103
show route-map 472
show running-config 44
show sflow 109
show sflow sampling 109
show snmp community 96
show snmp group 97
show snmp user 97
show snmp view 96
show spanning-tree 262
show spanning-tree mst 270
show spanning-tree mst config 270
show spanning-tree mst instance 271
show spanning-tree statistics 264
show ssh-server 120
show ssh-server host key 123
show stack 165
show startup-config 45
show static-channel-group 204
show storm-control 576
show system-diagnostics 58
show tech-support 53
show telnet-server 111
show test cable-diagnostics tdr 60
show tftp-server 114
show tx-queue-monitor 203
show users 41
show vlan 254
show vlan access-map 540
show vlan filter 540
show vlan multiple-vlan 255
show vlan private-vlan 255
show vrrp 463
show vrrp ipv6 464
show vrrp ipv6 statistics 465
show vrrp statistics 464
show y-unos 178
show yno 176
shutdown 186
snapshot delete 158
snapshot enable 157
snapshot save 158
snapshot trap terminal 157
snmp-server access 95
snmp-server community 92
snmp-server contact 91
snmp-server enable trap 90
snmp-server group 93
snmp-server host 88
snmp-server location 91
snmp-server startup-trap-delay 89
snmp-server user 94
snmp-server view 92
spanning-tree 258
spanning-tree bpdu-filter 259
spanning-tree bpdu-guard 259
spanning-tree edgeport 261
spanning-tree forward-time 256
spanning-tree instance 268
spanning-tree instance path-cost 269
spanning-tree instance priority 269
spanning-tree link-type 258
spanning-tree max-age 257
spanning-tree mst configuration 265
spanning-tree path-cost 260
spanning-tree priority (global configuration mode) 257
spanning-tree priority (interface mode) 261
spanning-tree shutdown 256

speed-duplex 186
ssh 125
ssh-client 125
ssh-server 120
ssh-server access 121
ssh-server client alive 124
ssh-server host key generate 122
ssh-server interface 121
stack 163
stack renumber 164
stack subnet 166
startup-config description 47
startup-config select 47
static-channel-group 204
storm-control 575
subscriber-id 589
summary-address (OSPFv2) 410
summary-address (OSPFv3) 422
switchport access vlan 246
switchport mode access 245
switchport mode private-vlan 249
switchport mode trunk 246
switchport multiple-vlan group 252
switchport private-vlan host-association 249
switchport private-vlan mapping 250
switchport trunk allowed vlan 247
switchport trunk native vlan 248
switchport voice cos 252
switchport voice dscp 252
switchport voice vlan 251
sync-e input-source 79
synchronization (BGP IPv4) 364
synchronization (BGP IPv6) 365
system-diagnostics on-demand execute 59

T

telnet 112
telnet-client 113
telnet-server 110
telnet-server access 112
telnet-server interface 111
terminal length 81
terminal-watch enable 149
terminal-watch interval 150
test cable-diagnostics tdr interface 60
tftp-server 113
tftp-server interface 114
timers basic 446
timers bgp 329
timers lsa arrival 411
timers spf exp 411
timers throttle lsa all 412
tlv-select basic-mgmt 137
tlv-select ieee-8021-org-specific 137
tlv-select ieee-8023-org-specific 138
tlv-select med 138
traceroute 298
traceroute6 318
traffic-shape queue rate 572
traffic-shape rate 572
tx-queue-monitor usage-rate (global configuration mode) 202
tx-queue-monitor usage-rate (interface mode) 203

U

unmount sd 180
unmute buzzer 174
unregister yno 176
user 617
username 39
username privilege 40

V

version 447
virtual-ip 462
virtual-ipv6 462
virtual-router 460
vlan 243
vlan access-map 538
vlan database 242
vlan filter 539

W

wireless-terminal-watch interval 155
write 43

Y

y-unos enable 177
yno enable 174
yno https-proxy 176
yno keepalive 175